

Izbrana poglavja iz matematike

Obsegi

- (1) Zapiši tabeli za seštevanje in množenje v Galoisovem obsegu $GF(4)$.

Rešitev: Teorija obsegov nam pove, da za vsako praštevilo p in vsako naravno število n obstaja do izomorfizma natanko določen končni obseg s p^n elementi. Označimo ga z $GF(p^n)$ in mu rečemo Galoisov obseg. Če je $n = 1$, se obseg $GF(p)$ ujema z obsegom $\mathbb{Z}_p$ ostankov pri deljenju s praštevilom p .

Za $n > 1$ konstruiramo Galoisov obseg $GF(p^n) \cong \mathbb{Z}_p[x]/(u)$ na naslednji način:

- Izberemo nerazcepen polinom u stopnje n v kolobarju $\mathbb{Z}_p[x]$.
- Elementi $GF(p^n)$ so polinomi stopnje največ $n - 1$ v $\mathbb{Z}_p[x]$, ki jih lahko interpretiramo tudi kot ostanke pri deljenju s polinomom $u(x)$.
- Seštevanje je definirano kot seštevanje polinomov.
- Produkt dveh polinomov dobimo tako, da najprej izračunamo njun produkt v $\mathbb{Z}_p[x]$, nato pa vzamemo ostanek pri deljenju s polinomom $u(x)$.

Edini nerazcepen kvadratni polinom v $\mathbb{Z}_2[x]$ je polinom $u(x) = x^2 + x + 1$, zato je

$$GF(4) = \{0, 1, x, 1 + x\},$$

operaciji seštevanja in množenja pa lahko predstavimo s tabelama:

+	0	1	x	$1 + x$	·	0	1	x	$1 + x$
0	0	1	x	$1 + x$	0	0	0	0	0
1	1	0	$1 + x$	x	1	0	1	x	$1 + x$
x	x	$1 + x$	0	1	x	0	x	$1 + x$	1
$1 + x$	$1 + x$	x	1	0	$1 + x$	0	$1 + x$	1	x

Množica vseh elementov obsega zmeraj tvori grupo za seštevanje, ki je v našem primeru izomorfna grupi $\mathbb{Z}_2 \times \mathbb{Z}_2$. Grupa obrnljivih elementov Galoisovega obsega $GF(2^2)$ pa je izomorfna grupi $\mathbb{Z}_3$. Bolj splošno velja, da je grupa obrnljivih elementov končnega obsega vedno izomorfna ciklični grupi. $\square$

- (2) Naj bo obseg $GF(8)$ definiran z nerazcepnim polinomom $u(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$. Opiši grupi $(GF(8), +)$ in $(GF(8)^*, \cdot)$.

Rešitev: Sedaj je

$$GF(8) = \{0, 1, x, x + 1, x^2, x^2 + x, x^2 + 1, x^2 + x + 1\}.$$

Na te polinome lahko gledamo tudi kot na vektorski prostor nad $\mathbb{Z}_2$ z bazo $\{1, x, x^2\}$, zato imamo izomorfizem

$$(GF(8), +) \cong \mathbb{Z}_2^3.$$

Množica neničelnih elementov obsega $GF(p^n)$, ki jo označimo z $GF(p^n)^*$, zmeraj tvori grupo za množenje, ki je izomorfna grupi $\mathbb{Z}_{p^n-1}$. Generatorjem te grupe rečemo primitivni

elementi Galoisovega obsega. V primeru obsega $\text{GF}(8)$ je $\text{GF}(8)^* \cong \mathbb{Z}_7$, zato je vsak nekonstanten polinom primitiven element. Če vzamemo na primer element x , so njegove potence:

$$\begin{aligned}x^1 &= x, \\x^2 &= x^2, \\x^3 &= x + 1, \\x^4 &= x^2 + x, \\x^5 &= x^2 + x + 1, \\x^6 &= x^2 + 1, \\x^7 &= 1.\end{aligned}$$

□

(3) Obseg $\text{GF}(2^8)$ definiramo z nerazcepnim polinomom $u(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbb{Z}_8[x]$.

(a) Izračunaj produkt polinomov $a(x) = x^6 + x^2 + 1$ in $b(x) = x^7 + x^6 + x^2 + 1$ v $\text{GF}(2^8)$.

(b) Izračunaj inverz polinoma $q(x) = x^5 + x + 1$ v $\text{GF}(2^8)$.

Rešitev: (a) Najprej izračunajmo produkt polinomov a in b v kolobarju $\mathbb{Z}_8[x]$

$$a(x)b(x) = (x^6 + x^2 + 1)(x^7 + x^6 + x^2 + 1) = x^{13} + x^{12} + x^9 + x^7 + x^4 + 1.$$

Pri deljenju polinoma $x^{13} + x^{12} + x^9 + x^7 + x^4 + 1$ s polinomom $u(x)$ dobimo kvocient $x^5 + x^4$ in ostanek $x^6 + 1$. V obsegu $\text{GF}(2^8)$ torej velja

$$a(x) \cdot b(x) = x^6 + 1.$$

(b) Inverz polinomov v Galoisovih obsegih iščemo s pomočjo posplošenega Evklidovega algoritma. Če namreč velja

$$su + tq = 1,$$

je polinom t inverz polinoma q v Galoisovem obsegu, ki ga definira nerazcepní polinom u . V našem primeru dobimo:

r_i	s_i	t_i	k_i
$x^8 + x^4 + x^3 + x + 1$	1	0	
$x^5 + x + 1$	0	1	
$x + 1$	1	x^3	x^3
1	$x^4 + x^3 + x^2 + x$	$x^7 + x^6 + x^5 + x^4 + 1$	$x^4 + x^3 + x^2 + x$

Ta tabela temelji na izračunih:

$$x^8 + x^4 + x^3 + x + 1 = x^3 \cdot (x^5 + x + 1) + x + 1,$$

$$x^5 + x + 1 = (x^4 + x^3 + x^2 + x) \cdot (x + 1) + 1,$$

iz nje pa lahko preberemo, da velja

$$q(x)^{-1} = x^7 + x^6 + x^5 + x^4 + 1.$$

□

(4) Pokaži, da so naslednja števila algebrailčna in nato izračunaj njihove minimalne polinome:

- (a) $a = 1 + \sqrt[3]{5}$,
- (b) $a = \sqrt{2} + \sqrt{3}$,
- (c) $a = \sqrt{1 + \sqrt{2}}$.

Rešitev: Kompleksna števila lahko razdelimo na naslednji dve podmnožici:

- število $a \in \mathbb{C}$ je *algebrailčno* nad $\mathbb{Q}$, če obstaja polinom $p \in \mathbb{Q}[x]$, da je $p(a) = 0$,
- število $a \in \mathbb{C}$ je *transcendentno* nad $\mathbb{Q}$, če ni algebrailčno.

Množico algebrailčnih števil torej poleg racionalnih števil tvorijo še ničle polinomskih enačb z racionalnimi koeficienti. Tipični primeri so števila, ki jih dobimo iz racionalnih števil s seštevanjem, odštevanjem, množenjem, deljenjem in korenjenjem. Vendar pa obstajajo ničle polinomskih enačb stopnje vsaj 5, ki jih ne moremo izraziti na ta način.

Za vsako algebrailčno število a obstaja enolično določen, nerazcepen, monični polinom $g_a \in \mathbb{Q}[x]$, da je $g_a(a) = 0$. Rečemo mu *minimalni polinom* algebrailčnega števila a .

(a) Pišimo $a = 1 + \sqrt[3]{5}$. Potem je $a - 1 = \sqrt[3]{5}$. S potenciranjem te enačbe dobimo zvezo

$$a^3 - 3a^2 + 3a - 6 = 0.$$

Če definiramo $g_a(x) = x^3 - 3x^2 + 3x - 6$, je torej $g_a(a) = 0$. Polinom g_a je moničen in nerazcepen v $\mathbb{Q}[x]$ po Eisensteinovem kriteriju. Torej je g_a minimalni polinom števila $a = 1 + \sqrt[3]{5}$.

(b) V primeru števila $a = \sqrt{2} + \sqrt{3}$ pridemo po dvakratnem kvadriranju do zveze

$$a^4 - 10a^2 + 1 = 0,$$

zato definirajmo polinom $g_a(x) = x^4 - 10x^2 + 1$. Preverimo lahko, da g_a nima racionalnih ničel. Če bi bil razcepen, bi torej moral biti produkt dveh kvadratnih faktorjev

$$x^4 - 10x^2 + 1 = (x^2 + bx + c)(x^2 + dx + e) = x^4 + (b+d)x^3 + (c+e+bd)x^2 + (eb+cd)x + ce,$$

kjer lahko po Gaussovi lemi predpostavimo, da so $b, c, d, e \in \mathbb{Z}$. Od tod dobimo sistem enačb:

$$\begin{aligned} b + d &= 0, \\ c + e + bd &= -10, \\ eb + cd &= 0, \\ ce &= 1. \end{aligned}$$

Iz prve enačbe dobimo $d = -b$, iz zadnje pa, da je $c = e = 1$ ali pa $c = e = -1$. Ko to vstavimo v drugo enačbo, dobimo $-b^2 = -12$ ali pa $-b^2 = -8$, kar pa ne gre. Od tod sklepamo, da je polinom g_a minimalni polinom števila $a = \sqrt{2} + \sqrt{3}$.

(c) V primeru števila $a = \sqrt{1 + \sqrt{2}}$ lahko podobno kot pri prejšnjem primeru pokažemo, da je algebrailčno in da ima minimalni polinom

$$g_a(x) = x^4 - 2x^2 - 1.$$

□

- (5) (a) Izračunaj stopnjo in bazo razširitve $\mathbb{Q}(\sqrt[3]{2})$ nad $\mathbb{Q}$. Nato izračunaj inverz števila $2 + \sqrt[3]{2} + \sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})$.
- (b) Izračunaj stopnjo in bazo razširitve $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ nad $\mathbb{Q}$ in pokaži, da je enostavna.

Rešitev: Naj bo a poljubno kompleksno število. Potem označimo:

$\mathbb{Q}[a] \dots$ najmanjši podkolobar $\mathbb{C}$, ki vsebuje $\mathbb{Q}$ in a ,

$\mathbb{Q}(a) \dots$ najmanjši podobseg $\mathbb{C}$, ki vsebuje $\mathbb{Q}$ in a .

Izkaže se, da potem za algebraično število a velja

$$\mathbb{Q}[a] = \mathbb{Q}(a) \cong \mathbb{Q}[x]/(g_a).$$

V tem primeru je torej $\mathbb{Q}(a)$ razširitev obsega $\mathbb{Q}$ stopnje $[\mathbb{Q}(a) : \mathbb{Q}] = \deg(g_a)$.

Če je število a transcendentno, pa velja

$$\mathbb{Q}[a] \cong \mathbb{Q}[x], \mathbb{Q}(a) \cong \mathbb{Q}(x).$$

(a) Število $a = \sqrt[3]{2}$ je algebraično in ima minimalni polinom $g_a(x) = x^3 - 2$. Od tod sledi

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

kar pomeni, da je $\mathbb{Q}(\sqrt[3]{2})$ tridimenzionalni vektorski prostor nad $\mathbb{Q}$. Za bazo vzemimo števila $1, a, a^2$, vsak element $x \in \mathbb{Q}(\sqrt[3]{2})$ pa je potem oblike

$$x = a_0 + a_1 \sqrt[3]{2} + a_2 \sqrt[3]{4}$$

za neke $a_0, a_1, a_2 \in \mathbb{Q}$.

Ker je $\mathbb{Q}(\sqrt[3]{2})$ obseg, je tudi inverz števila $2 + \sqrt[3]{2} + \sqrt[3]{4}$ enake oblike. Izračunamo ga lahko z uporabo razširjenega evklidovega algoritma kot v Galoisovih obsegih, ali pa z nastavkom

$$(2 + \sqrt[3]{2} + \sqrt[3]{4})(a_0 + a_1 \sqrt[3]{2} + a_2 \sqrt[3]{4}) = 1.$$

Zgornjo enačbo lahko prevedemo v sistem linearnih enačb za neznanke $a_0, a_1, a_2 \in \mathbb{Q}$, ki ima rešitev $a_0 = 1, a_1 = 0$ in $a_2 = -\frac{1}{2}$. Torej je

$$\frac{1}{2 + \sqrt[3]{2} + \sqrt[3]{4}} = 1 - \frac{1}{2} \sqrt[3]{4}.$$

(b) Obseg $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ je najmanjši podobseg $\mathbb{C}$, ki poleg $\mathbb{Q}$ vsebuje še števili $\sqrt{3}$ in $\sqrt{5}$. Opišemo ga lahko tudi v obliki $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3})(\sqrt{5})$. Za izračun stopnje razširitve bomo uporabili produktno formulo

$$[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Pri tem smo upoštevali, da sta minimalna polinoma $g_{\sqrt{3}}(x) = x^2 - 3$ in $g_{\sqrt{5}}(x) = x^2 - 5$. Za bazo razširitve lahko vzamemo števila $1, \sqrt{3}, \sqrt{5}, \sqrt{15}$.

Za dano razširitev rečemo, da je *enostavna*, če je generirana z enim samim elementom. V našem primeru lahko preverimo, da je

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

Če pišemo $a = \sqrt{3} + \sqrt{5}$, lahko izrazimo:

$$\begin{aligned}\sqrt{3} &= \frac{a^3 - 14a}{4}, \\ \sqrt{5} &= \frac{a^3 - 18a}{-8}, \\ \sqrt{15} &= \frac{a^2 - 8}{2}.\end{aligned}$$

To pomeni, da lahko za bazo razširitve $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ vzamemo tudi števila $1, a, a^2, a^3$. $\square$

(6) Izračunaj stopnjo in bazo razširitve $\mathbb{Q}(e^{\frac{2\pi i}{n}})$ nad $\mathbb{Q}$, če je n praštevilo.

Rešitev: Obsegom oblike $\mathbb{Q}(e^{\frac{2\pi i}{n}})$, kjer je n naravno število, rečemo *ciklotomski obsegi*.

Vemo že, da je število $\omega = e^{\frac{2\pi i}{n}}$ rešitev enačbe $\omega^n = 1$, od koder sledi, da je število ω algebraično in da minimalni polinom g_ω deli polinom $x^n - 1$. Za vsak n lahko polinom $x^n - 1$ faktoriziramo v obliki

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \dots + x + 1).$$

V primeru, ko je n praštevilo, smo že pred časom pokazali, da je polinom

$$g_\omega(x) = x^{n-1} + x^{n-2} + \dots + x + 1$$

nerazcepen, zato je minimalni polinom števila $\omega = e^{\frac{2\pi i}{n}}$. Torej je $\mathbb{Q}(e^{\frac{2\pi i}{n}})$ razširitev obsega $\mathbb{Q}$ stopnje $n - 1$ z bazo $1, \omega, \omega^2, \dots, \omega^{n-2}$.

Opomba: Če n ni praštevilo, je polinom $x^{n-1} + x^{n-2} + \dots + x + 1$ razcepen. V tem primeru se izkaže, da je stopnja razširitve ciklotomskega obsega $\mathbb{Q}(e^{\frac{2\pi i}{n}})$ nad $\mathbb{Q}$ enaka $\phi(n)$, kjer je ϕ Eulerjeva funkcija. $\square$

(7) Poišči razpadna obsega naslednjih polinomov:

(a) $p(x) = x^4 + 1 \in \mathbb{Q}[x]$,

(b) $p(x) = x^3 - 3 \in \mathbb{Q}[x]$.

Rešitev: Razpadni obseg polinoma $p \in \mathbb{Q}[x]$ je najmanjši obseg $\mathbb{Q} \leq F \leq \mathbb{C}$, ki vsebuje vse ničle polinoma p .

(a) Polinom $p(x) = x^4 + 1$ ima štiri kompleksne ničle:

$$\begin{aligned}z_0 &= e^{\frac{i\pi}{4}} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, \\ z_1 &= e^{\frac{3i\pi}{4}} = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, \\ z_2 &= e^{\frac{5i\pi}{4}} = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}, \\ z_3 &= e^{\frac{7i\pi}{4}} = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}.\end{aligned}$$

Vidimo, da so vse ničle potence z_0 , kar pomeni, da so vsebovane v obsegu $\mathbb{Q}(z_0)$, ki pa je hkrati najmanjši obseg, ki vsebuje z_0 . Od tod sklepamo, da je razpadni obseg polinoma $p(x) = x^4 + 1$ enak $\mathbb{Q}(z_0) = \mathbb{Q}(e^{\frac{i\pi}{4}})$. Ker je polinom p nerazcepen nad $\mathbb{Q}$, je minimalni

polinom števila z_0 , od koder sledi, da je $[\mathbb{Q}(e^{\frac{i\pi}{4}}) : \mathbb{Q}] = 4$. Za bazo razširitve lahko vzamemo števila $1, z_0, z_0^2 = i, z_0^3 = z_1$. Ta razpadni obseg bi lahko zapisali tudi v obliki

$$\mathbb{Q}(e^{\frac{i\pi}{4}}) = \mathbb{Q}(\sqrt{2}, i).$$

(b) Ničle polinoma $p(x) = x^3 - 3$ so:

$$\begin{aligned} z_0 &= \sqrt[3]{3}, \\ z_1 &= \sqrt[3]{3} e^{\frac{2i\pi}{3}}, \\ z_2 &= \sqrt[3]{3} e^{\frac{4i\pi}{3}}. \end{aligned}$$

V tem primeru obseg $\mathbb{Q}(\sqrt[3]{3})$ ne vsebuje preostalih dveh ničel. Da dobimo razpadni obseg, mu moramo dodati še število $e^{\frac{2i\pi}{3}}$. Stopnjo razširitve $\mathbb{Q}(\sqrt[3]{3}, e^{\frac{2i\pi}{3}})$ lahko izračunamo z uporabo formule

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

Minimalni polinom števila $\sqrt[3]{3}$ je $g_{\sqrt[3]{3}}(x) = x^3 - 3$, števila $e^{\frac{2i\pi}{3}}$ pa $g_{e^{\frac{2i\pi}{3}}}(x) = x^2 + x + 1$. Torej je $[\mathbb{Q}(\sqrt[3]{3}, e^{\frac{2i\pi}{3}}) : \mathbb{Q}] = 6$ in

$$\mathbb{Q}(\sqrt[3]{3}, e^{\frac{2i\pi}{3}}) = \{a_0 + a_1\sqrt[3]{3} + a_2\sqrt[3]{9} + a_3e^{\frac{2i\pi}{3}} + a_4\sqrt[3]{3}e^{\frac{2i\pi}{3}} + a_5\sqrt[3]{9}e^{\frac{2i\pi}{3}} \mid a_i \in \mathbb{Q}\}.$$

□

- (8) Ugotovi, ali lahko pravilni 8-kotnik oziroma pravilni 9-kotnik konstruiramo samo s šestilom in ravnilom.

Rešitev: Pravilni n -kotnik lahko konstruiramo s šestilom in ravnilom, če sta $\cos \frac{2\pi}{n}$ in $\sin \frac{2\pi}{n}$ konstruktibilni števili. To pa velja natanko takrat, ko je ciklotomski obseg $\mathbb{Q}(e^{\frac{2\pi i}{n}})$ dobljen iz $\mathbb{Q}$ z zaporedjem razširitev stopnje 2.

V primeru $n = 8$ smo že izračunali, da velja

$$\mathbb{Q}(e^{\frac{2\pi i}{8}}) = \mathbb{Q}(e^{\frac{i\pi}{4}}) = \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2})(i).$$

Imamo torej razširitev stopnje 4, ki jo lahko dobimo z zaporedjem razširitev stopnje 2. Od tod računsko sledi, da lahko 8-kotnik konstruiramo samo s šestilom in ravnilom. Dejansko lahko konstrukcijo izvedemo z nekajkratno konstrukcijo simetral kotov.

Bolj zanimiv je primer $n = 9$, pri katerem konstrukcije ne znamo izvesti. Sedaj bomo pokazali, da je dejansko ne moremo izvesti. Pišimo $\omega = e^{\frac{2\pi i}{9}}$. Potem je $\omega^9 = 1$. Iz razcepa

$$\omega^9 - 1 = (\omega^3 - 1)(\omega^6 + \omega^3 + 1)$$

sledi, da je $\omega^6 + \omega^3 + 1 = 0$. Pri tem smo upoštevali, da $\omega^3 \neq 1$. Sedaj bomo pokazali, da je polinom

$$g_\omega(x) = x^6 + x^3 + 1$$

minimalni polinom števila ω . Če pišemo

$$g_\omega(x+1) = (x+1)^6 + (x+1)^3 + 1 = x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3,$$

lahko z uporabo Eisensteinovega kriterija za $p = 3$ sklepamo, da je nerazcepen polinom $g_\omega(x+1)$. Vendar pa mora biti potem nerazcepen tudi polinom $g_\omega(x)$.

Stopnja razširitve $\mathbb{Q}(e^{\frac{2\pi i}{9}})$ nad $\mathbb{Q}$ je torej enaka 6, kar pa pomeni, da je ne moremo zapisati kot zaporedje razširitev stopnje 2. □

(9) Z uporabo kvaternionov izračunaj matriko za rotacijo za kot $\phi = \pi$ okoli osi $\vec{e} = \left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}, 0\right)$.

Rešitev: Kvaternioni so števila oblike

$$\mathbb{H} = \{q = t + xi + yj + zk \mid t, x, y, z \in \mathbb{R}\}.$$

Kvaternioni i , j in k so imaginarne enote, množenje pa je definirano s formulami

$$i^2 = j^2 = k^2 = -1$$

in

$$ij = -ji = k, jk = -kj = i, ki = -ik = j.$$

Pogosto uporabljamo vektorsko notacijo

$$q = t + xi + yj + zk = (t, \vec{r}),$$

ki nam omogoča, da množenje izrazimo s formulo

$$q_1 q_2 = (t_1 t_2 - \vec{r}_1 \cdot \vec{r}_2, t_1 \vec{r}_2 + t_2 \vec{r}_1 + \vec{r}_1 \times \vec{r}_2).$$

Vektorje v $\mathbb{R}^3$ pri tem zapisu identificiramo s kvaternioni, ki imajo skalarni del enak nič. Podobno kot pri kompleksnih številih lahko definiramo konjugirani kvaternion s predpisom

$$q^* = (t, -\vec{r}).$$

Kvaternioni tvorijo nekomutativen kolobar z deljenjem, enotski kvaternioni pa tvorijo grupo

$$S^3 = \{(t, \vec{r}) \in \mathbb{R}^4 \mid t^2 + |\vec{r}|^2 = 1\}.$$

Enotske kvaternione lahko uporabimo za vrtenje vektorjev v $\mathbb{R}^3$. Definirajmo kvaternion

$$q = \cos \frac{\phi}{2} + \sin \frac{\phi}{2} \vec{e},$$

kjer je $\phi \in \mathbb{R}$ in $\vec{e} \in \mathbb{R}^3$ enotski vektor. Potem je s predpisom

$$R(\vec{e}, \phi) \vec{x} = q \vec{x} q^*$$

definirana rotacija $\mathbb{R}^3$ za kot ϕ okoli osi $\vec{e}$.

V našem primeru je $\phi = \pi$ in $\vec{e} = \left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}, 0\right)$, kar nam da:

$$\begin{aligned} q &= \vec{e}, \\ q^* &= -\vec{e}. \end{aligned}$$

Sedaj bomo izračunali, kako se zavrtijo bazni vektorji:

$$\begin{aligned} R(\vec{e}, \phi) \cdot \vec{i} &= \vec{e} \cdot i \cdot (-\vec{e}) = \frac{1}{2}(i + j)i(-i - j) = j, \\ R(\vec{e}, \phi) \cdot \vec{j} &= \vec{e} \cdot j \cdot (-\vec{e}) = \frac{1}{2}(i + j)j(-i - j) = i, \\ R(\vec{e}, \phi) \cdot \vec{k} &= \vec{e} \cdot k \cdot (-\vec{e}) = \frac{1}{2}(i + j)k(-i - j) = -k. \end{aligned}$$

Od tod sledi, da rotaciji $R(\vec{e}, \phi)$ ustreza rotacijska matrika

$$R(\vec{e}, \phi) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}.$$

Opomba: Rotacijske matrike so ortogonalne matrike z determinanto ena. Tvorijo grupo

$$\text{SO}(3) = \{R \in \mathbb{R}^{3 \times 3} \mid R^T R = I, \det(R) = 1\}.$$

Če je R rotacijska matrika, lahko os in kot rotacije izračunamo na naslednji način.

- Os vrtenja je vzporedna lastnemu vektorju $\vec{e}$ matrike R , ki ustreza lastni vrednosti $\lambda = 1$. Eksplicitno je za $\phi \notin \{0, \pi\}$ to vektor

$$\vec{e} = \frac{1}{2 \sin \phi} \begin{bmatrix} R_{32} - R_{23} \\ R_{13} - R_{31} \\ R_{21} - R_{12} \end{bmatrix}.$$

- Kot $\phi \in [0, \pi]$ dobimo iz formule $\cos \phi = \frac{\text{sl}(R)-1}{2}$.

□

(10) S kvaternioni izračunaj rotacijo $R = R_2 \circ R_1$, kjer je $R_1 = R(\vec{i}, \frac{\pi}{2})$ in $R_2 = R(\vec{j}, \frac{\pi}{2})$.

Rešitev: Pri prejšnji nalogi smo fiksen kvaternion $q \in S^3$ uporabili za izračun rotacijske matrike. Bolj splošno pa se da pokazati, da je preslikava $R : S^3 \rightarrow \text{SO}(3)$ s predpisom

$$R(q)\vec{x} = q\vec{x}q^*$$

surjektiven homomorfizem grup z jedrom $\ker R = \{1, -1\}$. Dejstvo, da je R homomorfizem grup pomeni, da kompozicija rotacij ustreza množenju kvaternionov.

V našem primeru lahko rotacijo $R(\vec{j}, \frac{\pi}{2})$ predstavimo s kvaternionom

$$q_2 = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}(0, 1, 0),$$

rotacijo $R(\vec{i}, \frac{\pi}{2})$ pa s kvaternionom

$$q_1 = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}(1, 0, 0).$$

Rotacijo $R(\vec{j}, \frac{\pi}{2}) \circ R(\vec{i}, \frac{\pi}{2})$ pa lahko potem predstavimo s kvaternionom

$$q = q_2 q_1 = (\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}(0, 1, 0))(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}(1, 0, 0)) = \frac{1}{2} + \frac{1}{2}(1, 1, -1).$$

Od tod lahko preberemo, da vrtimo okoli osi s smerjo $\vec{e} = \frac{\sqrt{3}}{3}(1, 1, -1)$, kot rotacije pa zadošča pogoju $\cos \frac{\phi}{2} = \frac{1}{2}$ oziroma $\phi = 120^\circ$. □