Algebrske struktre

- grupoid (M, \cdot) urejen par z neprazno množico M in zaprto opreacijo \cdot .
- polgrupa grupoid z asociativno operacijo $\forall x, y, z \in M : (x \cdot y) \cdot z = x \cdot (y \cdot z).$
- monoid polgrupa z enoto $\exists e \in M \ \forall x \in M$: $e \cdot x = x \cdot e = x$.
- grupa polgrupa v kateri ima vsak element inverz $\forall x \in M \ \exists x^{-1} \in M : x \cdot x^{-1} = x^{-1} \cdot x =$
- abelova grupa grupa s komutativno operacijo $\forall x, y \in M : x \cdot y = y \cdot x$.

Kolobarji

Kolobar je množica R skupaj z dvema operacijama $(oznaka: +, \cdot)$ tako, da velia:

- (R, +) je abelova grupa
- $\forall a, b, c \in R$: a(b+c) = ab + ac Tako dobimo obseg ulomkov za K. (distrubutivnost)
- $\forall a,b,c \in R$: (a + b)c = ac + bc Wedderburnov izrek (distrubutivnost)
- $\forall a, b \in R : ab \in R \text{ (zaprtost množenja)}$
- $\forall a, b, c \in R : (ab)c = a(bc) \text{ (asociativnost*)}$
- $\exists e \in R \ \forall a \in R : e \cdot a = a = e \cdot a \ (\text{enota*})$

Kolobar je **komutativen**, če $\forall a, b \in R : ab = ba$. Kolobar je kolobar z delieniem, če $\forall a \in R$ – $\{0\}\ \exists a^{-1} \in R:\ aa^{-1} = 1\ \text{element}\ 1\ \text{je}\ enota$ kolobarja.

Kolobar, ki ima vse naštete lastnosti je obseg.

Delitelji niča in celi kolobarji

Naj bo R komutativen kolobar. $a \in R$, $a \neq 0$ delitelj niča, če

$$\exists b \in R, \ b \neq 0 : \ ab = 0$$

Če ima kolobar K enoto 1, rečemo, da je element $x \in K$ obrnljiv, če $\exists y \in K : xy = 1$. Delitelji niča niso nikoli obrnljivi.

Cel kolobar je komutativen kolobar z enoto (1 \neq 0), ki nima deliteljev niča.

Razširitve kolobariev

Naj bo K kolobar **brez enote**:

$$\mathbb{Z} \times K = \{n \in \mathbb{Z}, a \in K$$
$$(n, a) + (m, b) = (n + m, a + b)$$
$$(n, a) \cdot (m, b) = (nm, nb + am + ab)$$

Naj bo K komutativen kolobar brez deliteljevniča vendar niso vsi elementi obrnljivi. Dodamo ulomke definirane kot ekvivalenčne razrede dvojic z ekvivalenčno (refleksivno, simetrično, tranzitivno) relacijo \sim .

$$K \times K - \{0\} /_{\sim}$$

$$\frac{a}{b} \sim \frac{ka}{kb} \quad \forall k \in K - \{0\}$$

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}$$

$$\frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}$$

Če bi bila b in b' delitelja niča, bi imeli težave.

Končen kolobar brez deliteljev niča je obseg.

Posledica: \mathbb{Z}_n je obseg $\iff n \in \mathbb{P}$

Karakteristika kolobaria

Karakteristika kolobaria R je najmaniši $n \in \mathbb{N}$. tako da velia

$$\forall a \in R : na = \underbrace{a + a + \dots + a}_{n-\text{krat}} = 0$$

Če tak n ne obstaja je karakteristika enaka 0.

Če je $1 \in R$, je char(R) = red enote oziromanajmanjši $n \in \mathbb{N}$, da je $1 \cdot n = 0$.

Če je R cel kolobar, je $\operatorname{char} R \in \{0\} \cup \mathbb{P}$.

Homomorfizem

Naj bosta K, L kolobarja. $f: K \to L$ je **homomorfizem**, če $\forall a, b \in K$ velia:

$$f(a+b) = f(a) + f(b)$$
$$f(a \cdot b) = f(a) \cdot f(b)$$

Iz aditivnosti sledi: f(0) = 0 in f(-a) = -f(a).

Izomorfizem je bijektivni homomorfizem.

Avtomorfizem ie homomorfizem $f: K \to K$.

Če je f(1) = 1, pravimo, da je homomorfizem unitalen. Če je unitelen in če je a obrnljiv, potem ie $f(a^{-1}) = f(a)^{-1}$.

Slika / zaloga vrednosti

Zaloga vrednosti f je $f(K) = \{f(a) \mid a \in K\} =$ Im K < L.

f ie suriektiven \iff Im f = L

Jedro / ničelna množica

Praslika 0 je $f^{-1}(0) = \{a \in K \mid f(a) = 0\} =$ $\operatorname{Ker} f \leq K$.

$$\forall a \in K, \forall x \in \text{Ker} f : f(ax) = f(a)f(x) = 0$$

$$\implies \text{Ker} f \triangleleft K$$

 $\operatorname{Ker} f = \{x \in G | f(x) = e\}$ je jedro homomorfizma.

Ideali

Podkolobar $I \leq K$ je ideal, če velja $I \cdot K \subseteq I$ in $K \cdot I \subseteq I$. Oznaka: $I \triangleleft K$.

V nekomutativnih kolobariih ločimo leve in desne ideale. Primer: matrike, kier so izbrani stolpci ničelni, so levi ideali. Matrike z ničelnimi vrsticami so **desni** ideali.

K in $\{0\}$ sta neprava ideala.

(komutativen) kolobar K je obseg \iff nima pravih idealov.

Še več, pravi ideali ne vsebujejo obrnljivih elementov.

Maksimalen ideal

torej oblike $(x-a), a \in \mathbb{C}$.

Pravi ideal je **maksimalen**, če ni vsebovan v nobenem pravem idealu. Med njim in celim kolobarjem ni nobenega pravega ideala. Generiran je z nerazcepnim elementom. osnovni izrek algebre: nerazcepni so linearni.

Glavni ideali

Naj bo K kolobar in $x, y \in K$.

$$(x) = Kx = \{kx \mid k \in K\}$$

$$(x,y) = (x) + (y) = \{kx + ly \mid k, l \in K\}$$

Kolobar je **glavno idealski**, če se vsi njegovi ideali glavni.

Če je F obseg, je F[x] glavno idealski, maksimalni ideali pa pripadajo natanko nerazcepnim polinomom.

Kvocientni ideal

Za dvostranski ideal $I \triangleleft K$ definiramo ekvivalenčno relacijo \sim :

$$\forall a, b \in K : a \sim b \iff a - b \in I$$

K razdelimo na ekvivalenčne razrede $K/_{\sim}$, ki pa jih lahko označimo tudi z K/I. Ekvivalenčni razred, ki pripada $x \in K$ označimo [x] ali pa (x + I).

Dodamo opreaciji:

$$(x+I) + (y+I) = (x+y+I)$$

 $(x+I) \cdot (y+I) = (x \cdot y + I)$

 $(K/I, +, \cdot)$ je kolobar in podeduje lastnosti K.

K/I (K komutativen kolobar) je **obseg** \iff I maksimalen ideal.

Funkcija

 $f: \{ideali\ v\ K,\ ki\ vsebujejo\ I\} \leftrightarrow \{ideali\ v\ K/I\}$

je bijekcija.

Ideali v K/(x) so oblike (d+(x)), kjer d|x. Če je d nerazcepen, je ideal maksimalen.

Praideal

Ideal P v kolobarju K je praideal, če je $P \neq K$ in če $\forall a, b \in K : ab \in P \implies a \in P \lor b \in P$.

Izrek o izomorfizmu

Naj bo $f: K \to L$ homomorfizem kolobarjev (velja tudi za grupe). Potem je $\operatorname{Ker} f \triangleleft K$ in imamo naravni izomorfizem:

$$\bar{f}: K/\mathrm{Ker}f \to \mathrm{Im}f$$

$$K/\mathrm{Ker}f \cong \mathrm{Im}f$$

$$|K/\mathrm{Ker}f| = |\mathrm{Im}f|$$

Kolobarji polinomov

Računanje s kompleksnimi števili

Polarni zapis kompleksnega števila:

$$z = re^{i\varphi} = r(\cos\varphi + i\sin\varphi)$$

$$z = x + iy = re^{i\varphi} = r\left(\cos\varphi + i\sin\varphi\right)$$

$$z = |z| \cdot e^{i\varphi}$$

$$|z|^6 \cdot e^{6i\varphi} = 1 \cdot e^{2k\pi i}$$

$$r = |z| = \sqrt{x^2 + y^2} \qquad \varphi = \arg z = \arctan\frac{y}{x}$$

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

 $z^{2} = |z|^{2} \cdot e^{2i\varphi} = 4 \cdot e^{i\left(\frac{\pi}{2} + 2k\pi\right)} \to 2\varphi = \frac{\pi}{2} + k\pi$ Kako smo dobili tisti prvi $\frac{\pi}{2} + 2k\pi$? $z = 4(\cos\varphi + i\sin\varphi) \rightarrow \sin\varphi = 1 \rightarrow \varphi = \frac{\pi}{2} + 2k\pi$ Končen rezultat: $z = 2 \cdot e^{i(\frac{\pi}{4} + k\pi)}$

Računanje kompleksnega korena $\sqrt{5+12i}$ $\sqrt{z} = \pm \sqrt{|z|} \left(\cos\frac{\varphi}{2} + i\sin\frac{\varphi}{2}\right)$ $\cos \frac{\varphi}{2} = \pm \sqrt{\frac{1 + \cos \varphi}{2}} \quad \sin \frac{\varphi}{2} = \pm \sqrt{\frac{1 - \cos \varphi}{2}}$ Predznaka izberemo z upoštevanjem kvadranta, v katerem leži z. $|z| = \sqrt{5^2 + 12^2} = 13$ $\cos \varphi = \frac{x}{|z|} = \frac{5}{13}$

Ta cos vstavimo v zg. formule, te pa v za \sqrt{z} Na koncu moraš koren vstaviti nazaj v OG enačbo!

De Moivreova formula

$$z^n = r^n \left(\cos\varphi n + i\sin\varphi n\right)$$

Osnovni izrek algebre

ima natanko n kompleksnih ničel (štetih z p = 4k + 3večkratnostio).

Trigonometrične identitete

$$\sin(x \pm y) = \sin(x)\cos(y) \pm \cos(x)\sin(y)$$

$$\cos(x \pm y) = \cos(x)\cos(y) \mp \sin(x)\sin(y)$$

$$\tan(x \pm y) = \frac{\tan(x) \pm \tan(y)}{1 \mp \tan(x)\tan(y)}$$

$$\cot(x \pm y) = \frac{\cot(x)\cot(y) \mp 1}{\tan(x) \pm \tan(y)}$$

$$\sin^2(x) + \cos^2(x) = 1$$

$$1 + \cot^2(x) = \frac{1}{\sin^2(x)}$$

$$1 + \tan^2(x) = \frac{1}{\cos^2(x)}$$

$$\sin\frac{x}{2} = \pm\sqrt{\frac{1 - \cos x}{2}}$$

$$\cos\frac{x}{2} = \pm\sqrt{\frac{1 + \cos x}{2}}$$

Mali Fermantov izrek

$$\forall a \in \mathbb{Z}, p \in \mathbb{P}: a^p \equiv_p a$$

Polinomi

Polinom je razcepen, če ga lahko zapišemo kot produkt dveh nekonstantnih polinomov. Nekonstanten polinom, ki ni razcepen je nerazcepen.

Element je razcepen, če ga lahko zapišemo kot $a \cdot b$, kjer a in b nista obrnljiva.

Polinom $a_n x^n + \cdots + a_0$ je **primitiven**, če velja $\gcd(a_0,\ldots,a_n)=1$

Kvadrati dajo pri deljenju s 4 vedno ostanek 0 ali

Množica neničelnih kvadratov v \mathbb{Z}_p grupo za množenje moči $\frac{p-1}{2}$

Vsak nekonstanten polinom $a_n x^n + \cdots + a_0$ Polinom $x^2 + 1$ je nerazcepen v $\mathbb{Z}_p[x] \iff$ poblike

Kandidati za ničle polinoma

Naj bo $p(x) = a_k x^k + \dots + a_0; \quad a_i \in \mathbb{Z}.$ Kdaj je lahko $\frac{m}{n}$; GCD(m,n) = 1 ničla?

$$n|a_k$$
 in $m|a_0$

p(x) nima linearnih faktorjev \iff nima ničel

Ničle polinoma $x^p - x$ v \mathbb{Z}_p , če je p praštevilo: $x^{p} - x = x(x-1)(x-2)...(x-(p-1))$

Gaussova lema

 $p(x) \in \mathbb{Z}[x]$ razcepen nad \mathbb{Z}

 $\iff p(x) \text{ razcepen nad } \mathbb{Q}$

Hornerjev algoritem

$$a_n x^n + \dots + a_0 = 0$$

- možne cele ničle: \pm delitelji a_0
- možne racionalne ničle: $\pm \frac{\text{delitelji } a_0}{\text{delitelji } a_n} = k$

Eisensteinov kriterij

Naj bo $a(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ polinom. Če $\exists p \in \mathbb{P} : p | a_0, \dots, a_{n-1} \land p \nmid a_n \land p^2 \nmid a_0$ potem je a(x) nerazcepen nad \mathbb{Q} .

Rodovne funkcije

$$\sum_{n=0}^{\infty} q^n = \frac{1}{1-q} \qquad \sum_{n=0}^{b} q^n = \frac{1-q^{b+1}}{1-q}$$

$$\sum_{n=a}^{\infty} q^n = \frac{q^a}{1-q} \quad \sum_{n=a}^{b} q^n = \frac{q^a - q^{b+1}}{1-q}$$

$$a^{n} - b^{n} = (a - b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1})$$

$$(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k$$

$$\frac{1}{(1-x)^n} = \sum_{k=0}^n {n+k-1 \choose k} x^k$$

$$B_{\lambda}(x) = \sum_n {\lambda \choose n} x^n = (1+x)^{\lambda}; \qquad {\lambda \choose n} = \frac{\lambda^n}{n!}$$

$${n \choose k} = \frac{n!}{k!(n-k)!}$$

$${n \choose k} = {n-1 \choose k-1} + {n-1 \choose k}$$

Mobiusova formula

$$\mu(n) = \begin{cases} 1 & n = 1, \\ 0 & \exists p \in P : p^2 | n \\ (-1)^k & n \text{ je produkt } k \text{ različnih praštevil.} \end{cases}$$

Število nerazcepnih polinomov v $\mathbb{Z}_n[x]$ stopnje n je

$$N_p(n) = \frac{p-1}{n} \sum_{d|n} \mu(\frac{n}{d}) p^d$$

Eulerjeva funkcija

$$\begin{split} \varphi(n) &= |\{k \in [n] : D(n,k) = 1\}| \\ &= \text{ it. proti } n \text{ tujih itevil, ki so } \leq n \\ \varphi(p) &= p - 1 \qquad p \in \mathbb{P} \\ \varphi(p^k) &= p^k - p^{k-1} = p^k (1 - \frac{1}{p}) \\ \sum_{d \mid n} \varphi(d) &= n \end{split}$$

Največji skupni delitelj

Naj bo F obseg in $p, q \in F[x]$. največji skupni delitelj polinomov p in q je polinom $d = \gcd(p, q)$, ki zadošča:

- d|p in d|q
- \bullet vsak polinom, ki deli p in q deli tudi d
- \bullet vodilni koeficient d je enak 1.

Največji skupni delitelj obstaja in je enolično določen. Obstajata polinoma s in $t \in F[x]$ tako da

$$s \cdot p + t \cdot a = d$$

Razširjen evklidov algoritem

$$\begin{array}{lll} \textit{vhod}: & (a,b) \\ & (r_0, \ x_0, \ y_0) \ = \ (a, \ 1, \ 0) \\ & (r_1, \ x_1, \ y_1) \ = \ (b, \ 0, \ 1) \\ & i = 1 \\ & \textit{dokler} \ \ r_i \ \neq \ 0: \\ & i = i+1 \\ & k_i = r_{i-2}//r_{i-1} \\ & (r_i, x_i, y_i) \ = \ (r_{i-2}, x_{i-2}, y_{i-2}) - k_i(r_{i-1}, x_{i-1}, y_{i-1}) \\ & \textit{konec} \ \ \textit{zanke} \\ & \textit{vrni}: \ (r_{i-1}, x_{i-1}, y_{i-1}) \end{array}$$

algoritem z vhodnim podatkomk (a, b), zadošča:

$$ax + by = d$$
 in $d = \gcd(a, b)$

Vodilni koeficient od gcd je 1. S tem, s čimer deliš/množiš gcd, moraš deliti/množiti tudi s in t.

Gaussova cela števila

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}\$$

Trojica (d, x, y), ki jo vrne razširjen evklidov Gaussovo celo število $x \neq 0$, ki ni obrnljivo, je

nerazcepno, če

$$x = y \cdot z \implies y$$
obrn
ljivo $\vee \, z$ obrn
ljivo

Števili x in y sta **asociativni**, če velja y = ax, kjer je a obrnljiv.

Liho praštevilo $p \in \mathbb{P}$ je nad $\mathbb{Z}[i]$ nerazcepno \iff p = 4k + 3

Norma Gaussovega celega št je $N(a+bi) = a^2 + b^2$.

Norma je multiplikativna: $N(z \cdot w) = N(z) \cdot N(w)$

a+bi je obrnljivo $\implies \exists c+di \ni : (a+bi)\cdot (c+di) = 1$ Na desni strani uporabimo normo in dobimo: $N(a+bi) \cdot N(c+di) = 1 \cdot 1 = 1$ a + bi je obrnljivo $\iff N(a + bi) = 1$ (leži na enotski krožinici)

Obrnljiva števila so 1, -1, i, -i

Vsak par Gaussovih celih števil $z, w \in \mathbb{Z}[i]$ lahko zapišemo kot

$$z = kw + r$$

Kjer je N(z) > N(w) in N(r) < N(w)

Obsegi

neničelni elementi obrnljivi.

Razširitve obsegov

Če je K podobseg obsega F, pravimo, da je Frazširitev obsega K in pišemo $K \leq F$.

F je avtomatično tudi vektorski prostor nad K dimenzije $\dim_K(F) = [F:K].$

Če je [F:K] končna, je F končna razširitev, sicer pa je **neskončna razširitev**.

$$K \leq F \leq E \implies [E:K] = [E:F] \cdot [F:K]$$

• Najmaniši podkolobar kolobaria F, ki vsebuje $K \leq F$ in $a \in F$ ie

$$K[a] = \{p(a) \mid p(x) \in K[x]\}$$

• Najmanjši podobseg obsega F, ki vsebuje $K \leq F$ in $a \in F$ je

$$K(a) = \left\{ \frac{p(a)}{q(a)} \mid p(x), q(x) \in K[x] \right\}$$

Enostavne razširitve obsegov

Razširitev je enostavna, če je generirana z enim samim elementom.

Naj bo $K \leq F$ in $a \in F$. Oglejmo si homomorfizem

$$f_a: K[x] \to F$$

 $p(x) \mapsto p(a)$

$$Im f_a = K[a]$$

$$Ker f_a = \{ p(x) \in K[x] \mid p(a) = 0 \}$$

- a je transcendenten nad K
- ⇔ a ni ničala nobenega neničelnega polinoma iz K[x]
- $\iff \operatorname{Ker} f_a = (0)$
- $\iff f_a \text{ injektivna}$
- a je algebraičen nad K

$$\iff \exists p(x) \in K[x], p \neq 0: p(a) = 0$$

Obseg je komutativen kkolobar v katerem so vsiČe so vsi elementi F algebraični nad K, je Falgebraična razširitev. V nasprotnem primeru pa je F transcendentna razširitev.

Če je $a \in F$ transcendenten nad K, je

$$K[a] \cong K[x]$$
 $K(a) \cong K(x)$

Če je $a \in F$ algebraičen nad K, velja:

- \exists natanko določen **minimalni polinom** $q_a \in$ K[x], ki deli vse polinome z ničlo v a. q_a **moničen** (vodilni koef. = 1)
- $\operatorname{Ker} f_a = (q_a)$
- $K(a) = K[a] \cong K[x]/(g_a)$
- $[K(a) : K] = \deg g_a$, stopnja a nad K $(oznaka: deg_{\kappa} a)$
- Ideal $(g_a) \triangleleft K[x]$ je maksimalen \Longrightarrow $K[x]/(q_a)$ je obseg

Naj bo F končna razširitev K, potem za vsak $a \in F$ velia

$$\deg_K(a)|[F:K]$$

Vse transcendentne razširitve so neskončne, algebraične pa so lahko končne ali pa neskončne (če dodamo več elementov).

Naj bo K < F in $A \subseteq F$ množica števil, ki so algebraična nad K. Potem je K(A) algebraična nad

Naj bo K < F < E, F algebraična nad K, E algebraična nad F. Potem je E algebraična nad K.

Razpadni obseg polinoma

Razpadni obseg polinoma p(x) nad obsegom Koznačimo z K(p(x)). To je najmanjši podobseg K v katerem je p(x) povsem razcepen (K vsebuje vse $ni\check{c}le\ p(x)$).

Za vsak n obstaja razširitev stopnje n obsega \mathbb{Z}_p . Vsaka taka razširitev je izomorfna $\mathbb{Z}_n(x^{p^n}-x)$.

Edini (do izomorfizma) obseg moči n^p je Galoisov obseg $GF(p^n)$.

Naj bo K končen kolobar (ne nujno komutativen). Če K nima deliteljev niča, je $|K| = p^n$ in $K \cong$ $GL(n^p)$.

Galoisovi obsegi

$$GF(p) \cong \mathbb{Z}_p \qquad p \in \mathbb{P}$$

 $GF(p^n) \cong \mathbb{Z}_p[x]/(u)$

- $u \in \mathbb{Z}_p[x]$ je nerazcepen polinom stopnje n
- elementi $GF(p^n)$ so ostanki polinomov iz \mathbb{Z}_p pri deljenju z polinomom u
- seštevanje je enako kot seštevanje v $\mathbb{Z}_p[x]$
- produkt izračunamo v $\mathbb{Z}_n[x]$ nato pa vzamemo ostanek pri deljenju z u

Množica neničelnih/obrnljivih elementov $(GF(p^n)^*,\cdot)\cong (\mathbb{Z}_{p^n-1},\cdot)$ je vedno izomorfna neki ciklični grupi. Generatorjem te grupe rečemo primitivni elementi Galoisovega obsega.

Ciklotomski obseg

ie oblike $\mathbb{O}(e^{\frac{2\pi i}{n}})$ kier ie $n \in \mathbb{N}$.

$$\left[\mathbb{Q}(e^{\frac{2\pi i}{n}}):\mathbb{Q}\right] = \varphi(n)$$

 φ je Eulerjeva funkcija.

Konstruktibilna števila

Število $a \in \mathbb{R}$ je konstruktibilno \iff

$$a \in F_n$$
 $\mathbb{Q} = F_0 \le \dots \le F_n$

kjer je $[F_i : F_{i-1}] = 2$ za $\forall j = 1, ..., n$.

Število je konstruktibilno, če leži v zaporedju razširitev stopnje 2.

Kvaternioni

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

Kvaternioni so nekomutativen kolobar z deljenjem.

Prvi operand je na začetku vrstice, drugi pa na vrhu stolpca.

Vektorska oblika

$$q = t + xi + yj + zk = (t, \overrightarrow{r})$$
 $\overrightarrow{r} = (x, y, z)$

Vektorje $\vec{x} = (x_1, x_2, x_3) \in \mathbb{R}^3$ identificiramo s kvaternioni $(0, \vec{x})$, ki imajo skalarni del enak 0.

Množenje izrazimo s formulo:

$$q_1q_2 = (t_1t_2 - \vec{r_1} \cdot \vec{r_2}, \ t_1\vec{r_2} + t_2\vec{r_1} + \vec{r_1} \times \vec{r_2})$$

$$\vec{a} \times \vec{b} = \begin{vmatrix} \mathbf{i} & \mathbf{j} & \mathbf{k} \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix}$$

Konjugirani kvaternion:

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

Norma kvaterniona:

$$|q|^2 = qq^* = t^2 + x^2 + y^2 + z^2 = t^2 + ||\vec{r}||^2$$

Inverz kvaterniona:

$$q^{-1} = \frac{q^*}{|q|^2}$$

Vrtenie vektoriev

Vektor $\vec{x} \in \mathbb{R}^3$ bomo zavrteli okoli osi $\vec{e} \in \mathbb{R}^3$, $|\vec{e}| = 1$ za kot $\varphi \in \mathbb{R}$.

Enotski kvaternioni tvorijo grupo:

$$s^3 = \{(t, \overrightarrow{r}) \in \mathbb{H} \mid t^2 + ||\overrightarrow{r}||^2 = 1\}$$

Definirajmo enotski kvaternion:

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

Zavrten vektor ie potem:

$$R(\overrightarrow{e}, \varphi)\overrightarrow{x} = q\overrightarrow{x}q^*$$

Rotacijske matrike so ortogonalne matrike z determinanto 1 in tvorijo grupo:

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

rotacije:

Os vrtenja je vzporedna lastnemu vektorju \vec{e} Naj bo $A \subseteq X$. matrike R, ki ustreza lastni vrednosti $\lambda = 1$. Za $\varphi \notin \{0,\pi\}$:

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

Kot rotacije pa dobimo s formulo $\cos \varphi = \frac{\mathrm{sl}(R) - 1}{2}$

Topologija

Naj bo X poljubna množica. Topologija na X je podana z družino odprtih množic τ , ki je zaprta za poljubne unije in končne preseke.

Prazna unija je prazna množica, prazen presek pa cela množica.

Najmanjša možna topologija je $\tau = \{\emptyset, X\}$ trivialna.

Največja možna topologija je $\tau = P(X)$ diskretna.

Topologija glede na metriko

 $d: X \times X \to [0, \infty)$ je metrika, če velja:

- $d(x,y) = 0 \iff x = y$
- \bullet d(x,y) = d(y,x)
- $d(x,y) + d(y,z) \ge d(x,z)$

Topologija iz metrike na X je:

$$\tau_d = \{ U \subseteq X \mid U \text{ odprta glede na } d \}$$

A je **odprta množica**, če so vse točke notranje $(\forall a \in A \exists \varepsilon > 0 : K(a, \varepsilon) \subseteq A).$

Iz rotacijske matrike R lahko izračunamo os A je **zaprta množica** \iff A^{\complement} odprta \iff vsebuje vse svoje robne točke.

- Notranjost $Int(A) = \mathring{A} = največja odprta$ množica vsebovana v A.
- Zaprtje $Cl(A) = \bar{A} = najmanjša zaprta$ množica, ki še vsebuje v A= presek vseh zaprtih množic, ki vsebujejo A
- Rob Fr(A) = $\partial A = \dot{A} = \text{Cl}(A) \text{Int}(A)$

Metrizabilnost

 (X,τ) je metrizabilen, če obstaja metrika d na X.

Zveznost

Funkcija $f:(X,\tau_X)\to (Y,\tau_Y)$ je zvezna v točki $x \in X$, če lahko za vsako odprto okolico V točke f(x) najdemo odprto okolico U točke x, da velja $f(U) \subset V$.

Funkcija $f:(X,\tau_X)\to (Y,\tau_Y)$ je zvezna, če

$$\forall x \in X \ \forall \varepsilon > 0 \ \forall \delta > 0 \ \forall x' \in X :$$

$$d(x, x') < \delta \implies d(f(x), f(x')) < \varepsilon$$

Ekvivalentna topološka definicija:

$$\forall V \in \tau_Y : f^{-1}(V) \in \tau_X$$

Funkcija je zvezva, če je praslika vsake odprte množice odprta.

Naslednje trditve so ekvivalentne:

- $f: X \to Y$ je zvezna
- $\forall A^{\text{odp}} \subseteq Y : f^{-1}(A) \text{ odprta } \forall X$
- $\forall B^{\text{zap}} \subseteq Y : f^{-1}(B) \text{ zaprta v } X$
- $\forall A \subset X : f(\bar{A}) \subset \overline{f(A)}$

Homeomorfizmi

 $f:(X,\tau_X)\to (Y,\tau_Y)$ je homeomorfizem, če je f bijekcija in sta f in f^{-1} zvezni.

Prostora (X, τ_X) in (Y, τ_Y) sta homeomorfna. Oznaka $X \approx Y$.

 $f: X \to Y$ je **odprta**, če je slika vsake odprte množice odprta.

 $f:X\to Y$ je **zaprta**, če je slika vsake zaprte množice zaprta.

Naslednje trditve so ekvivalentne:

- $f: X \to Y$ ie homeomorfizem
- f je zvezna bijekcija in f^{-1} je zvezna
- f je zvezna in odprta bijekcija
- f je zvezna in zaprta bijekcija

Kompaktnost

Odprto pokritie množice X ie vsaka družina (odprtih množic) $\mathcal{U} \subseteq \tau$, katere unija je cel X.

Prostor X je kompakten, če v vsakem odprtem pokritiu X obstaja končno podpokritie.

- Vsaka končna množica je kompaktna.
- V metričnem prostoru je vsaka kompaktna množica omejena.

 $A^{\operatorname{zap}} \subset X^{\operatorname{kompakten}} \Longrightarrow A \operatorname{kompakten}$

 $Heine ext{-}Borel ext{-}Lebesque:$

 $A \subseteq \mathbb{R}^n$ je kompakten \iff A zaprt in omejen

V kompaktnem prostoru ima vsaka neskončna množica vsaj eno stekališče.

Bolzano-Weierstrass:

Vsako omejeno zaporedje v \mathbb{R}^n ima konvergentno podzaporedje.

Zvezna slika kompakta je kompakt.

 $f: X \to Y$ zvezna, $A^{\text{kompkt}} \subset X \implies f(A)$ kompakt

X kompakten \iff v vsaki družini zap. podmnožic X, ki ima prazen presek, obstaja končna podmnožica, ki ima prazen presek.

Povezanost

Separacija množice X je razdelitev $X = A \coprod B$ na deve disjunktni, neprazni, odprti podmnožici.

Prostor, ki ima separacijo je **nepovezan**, sicer pa ie **povezan**.

Alternativna definicija:

- X je povezan, če ga ni mogoče razdeliti na dve disjunktni neprazni množici
- X je povezan, če sta njegovi edini podmnožici, ki sta zaprti in odprti hkrati, \emptyset in X.

Povezane množice v \mathbb{R} so natanko intervali.

Zvezna funkcije ohranjajo povezanost. $f: X \to Y$ zvezna, X povezana $\Longrightarrow f(X)$

X je **povezan s potmi**, če za polubna $a, b \in X$ obstaja **pot** $p:[0,1] \rightarrow X$, zvezna, p(0) = a, p(1) = b.

X povezan s potmi $\Longrightarrow X$ povezan

Če je L povezan in je $L \subseteq M \subseteq \bar{L}$, je tudi M povezan.