

## Algebrske strukture

- **grupoid**  $(M, \cdot)$  urejen par z neprazno množico  $M$  in zaprto preacijo  $\cdot$ .
- **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  $\forall x \in M \exists x^{-1} \in M : x \cdot x^{-1} = x^{-1} \cdot x = e$ .
- **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 velja:

- $(R, +)$  je abelova grupa
- $\forall a, b, c \in R : a(b + c) = ab + ac$  (distributivnost)
- $\forall a, b, c \in R : (a + b)c = ac + bc$  (distributivnost)
- $\forall a, b \in R : ab \in R$  (zaprtost množenja)
- $\forall a, b, c \in R : (ab)c = a(bc)$  (asociativnost\*)
- $\exists e \in R \forall a \in R : e \cdot a = a = e \cdot a$  (enota\*)

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

Kolobar, ki ima vse naštet lastnosti je **obseg**.

## Delitelji nič in celi kolobarji

Naj bo  $R$  komutativen kolobar.

$a \in R, a \neq 0$  **delitelj nič**, 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 nič niso nikoli obrnljivi.

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

## Razširitve kolobarjev

Naj bo  $K$  kolobar **brez enote**:

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

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

$$\begin{aligned}K \times K - \{0\} / \sim \\ \frac{a}{b} \sim \frac{ka}{kb} \quad \forall k \in K - \{0\} \\ \frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'} \\ \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}\end{aligned}$$

Če bi bila  $b$  in  $b'$  delitelja nič, bi imeli težave.

Tako dobimo **obseg ulomkov za  $K$** .

## Wedderburnov izrek

Končen kolobar brez deliteljev nič je **obseg**.

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

## Karakteristika kolobarja

**Karakteristika** kolobarja  $R$  je najmanjši  $n \in \mathbb{N}$ , tako da velja

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

Če tak  $n$  ne obstaja je karakteristika enaka 0.

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

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

## Homomorfizem

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

$$\begin{aligned}f(a + b) &= f(a) + f(b) \\ f(a \cdot b) &= f(a) \cdot f(b)\end{aligned}$$

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

**Izomorfizem** je bijektivni homomorfizem.

**Avtomorfizem** je homomorfizem  $f : K \rightarrow K$ .

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

### Slika / zaloga vrednosti

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

$$f \text{ je surjektiv} \iff \text{Im} f = L$$

### Jedro / ničelna množica

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

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

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

$\text{Ker} f = \{x \in G \mid f(x) = e\}$  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 kolobarjih ločimo **leve** in **desne** ideale. Primer: matrike, kjer 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

Pravi ideal je **maksimalen**, če ni vsebovan v nobenem pravem idealu.

### 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.

### Kvocietni 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 operaciji:

$$\begin{aligned}(x + I) + (y + I) &= (x + y + I) \\ (x + I) \cdot (y + I) &= (x \cdot y + I)\end{aligned}$$

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

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

Funkcija

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

je bijekcija.

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

### Praideal

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

### Izrek o izomorfizmu

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

$$\begin{aligned}\bar{f} : K/\text{Ker } f &\rightarrow \text{Im } f \\ K/\text{Ker } f &\cong \text{Im } f \\ |K/\text{Ker } f| &= |\text{Im } f|\end{aligned}$$

## Kolobarji polinomov

### Računanje s kompleksnimi števili

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

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

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

### De Moivreova formula

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

### Osnovni izrek algebre

Vsak nekonstanten polinom  $a_n x^n + \dots + a_0$  ima natanko  $n$  kompleksnih ničel (štetih z večkratnostjo).

### 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  $a_n x^n + \dots + a_0$  je **primitiven**, če velja  $\gcd(a_0, \dots, a_n) = 1$

Kvadrati dajo pri deljenju s 4 vedno ostanek 0 ali 1.

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

Polinom  $x^2 + 1$  je nerazcepen v  $\mathbb{Z}_p[x] \iff p$  oblike  $p = 4k + 3$

## Kandidati za ničle polinoma

Naj bo  $p(x) = a_k x^k + \dots + a_0$ ;  $a_i \in \mathbb{Z}$ .

Kdaj je lahko  $\frac{m}{n}$ ;  $GCD(m, n) = 1$  ničla?

$$n|a_k \quad \text{in} \quad m|a_0$$

$p(x)$  nima linearnih faktorjev  $\iff$  nima ničel

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

## 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:  $\pm \frac{\text{delitelj } a_0}{\text{delitelj } a_n} = k$

	$a_n$	$a_{n-1}$	$\dots$	$a_0$
$k$	$ka_n$	$\dots$		
	$a_n$	$ka_n - a_{n-1}$	$\dots$	ostanek

### Eisensteinov kriterij

Naj bo  $a(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$  polinom.

Če  $\exists p \in \mathbb{P} : p|a_0, \dots, a_{n-1} \wedge p \nmid a_n \wedge p^2 \nmid a_0$

potem je  $a(x)$  **nerazcepen** nad  $\mathbb{Q}$ .

### Rodovne funkcije

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

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

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

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

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

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

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

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

### 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  $\mathbb{Z}_p[x]$  stopnje  $n$  je enako

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

## Eulerjeva funkcija

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

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

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

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

## Razširjen evklidov algoritem

**vhod:**  $(a, b)$   
 $(r_0, x_0, y_0) = (a, 1, 0)$   
 $(r_1, x_1, y_1) = (b, 0, 1)$   
 $i = 1$

**dokler**  $r_i \neq 0$ :  
 $i = i+1$   
 $k_i = r_{i-2} // r_{i-1}$   
 $(r_i, x_i, y_i) = (r_{i-2}, x_{i-2}, y_{i-2}) - k_i(r_{i-1}, x_{i-1}, y_{i-1})$   
**konec zanke**  
**vrni:**  $(r_{i-1}, x_{i-1}, y_{i-1})$

Trojica  $(d, x, y)$ , ki jo vrne razširjen evklidov algoritem z vhodnim podatkom  $(a, b)$ , zadošča:

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

## Gaussova cela števila

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



Gaussovo celo število  $x \neq 0$ , ki ni obrnljivo, je **nerazcepno**, če

$$x = y \cdot z \implies y \text{ obrnljivo} \vee z \text{ obrnljivo}$$

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 krožnici)

**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

Obseg je *komutativen* kolobar v katerem so vsi neničelni elementi *obrnljivi*.

### Razširitve obsegov

Če je  $K$  podobseg obsega  $F$ , pravimo, da je  $F$  **razširitev** 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**.

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

- Najmanjši podkolobar kolobarja  $F$ , ki vsebuje  $K \leq F$  in  $a \in F$  je

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

- 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

$$\begin{aligned} f_a : K[x] &\rightarrow F \\ p(x) &\mapsto p(a) \end{aligned}$$

$$\begin{aligned} \text{Im } f_a &= K[a] \\ \text{Ker } f_a &= \{p(x) \in K[x] \mid p(a) = 0\} \end{aligned}$$

- $a$  je **transcendenten** nad  $K$

$$\iff a \text{ ni ničala nobenega neničelnega polinoma iz } K[x]$$

$$\iff \text{Ker } f_a = (0)$$

$$\iff f_a \text{ injektivna}$$

- $a$  je **algebraičen** nad  $K$

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

Če so vsi elementi  $F$  algebraični nad  $K$ , je  $F$  **algebraična razširitev**. V nasprotnem primeru pa je  $F$  **transcendentna razširitev**.

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

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

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

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

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

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

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

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

Naj bo  $K \leq F \leq E$ ,  $F$  algebraična nad  $K$ ,  $E$  algebraična nad  $F$ . Potem je  $E$  algebraična nad  $K$ .

## Razpadni obseg polinoma

Razpadni obseg polinoma  $p(x)$  nad obsegom  $K$  označimo z  $K(p(x))$ . To je najmanjši podobseg  $K$  v katerem je  $p(x)$  povsem razcepen ( $K$  vsebuje vse ničle  $p(x)$ ).

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

Edini (do izomorfizma) obseg moči  $n^p$  je **Galoisov obseg**  $\text{GF}(p^n)$ .

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

## Galoisovi obsegi

$$\begin{aligned}\text{GF}(p) &\cong \mathbb{Z}_p & p \in \mathbb{P} \\ \text{GF}(p^n) &\cong \mathbb{Z}_p[x]/(u)\end{aligned}$$

- $u \in \mathbb{Z}_p[x]$  je nerazcepen polinom stopnje  $n$
- elementi  $\text{GF}(p^n)$  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  $\mathbb{Z}_p[x]$  nato pa vzamemo ostanek pri deljenju z  $u$

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

## Ciklotomski obseg

je oblike  $\mathbb{Q}(e^{\frac{2\pi i}{n}})$  kjer je  $n \in \mathbb{N}$ .

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

$\varphi$  je Eulerjeva funkcija.

## Konstruktibilna števila

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

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

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

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.

$\cdot$	1	$i$	$j$	$k$
1	1	$i$	$j$	$k$
$i$	$i$	-1	$k$	$-j$
$j$	$j$	$-k$	-1	$i$
$k$	$k$	$j$	$-i$	-1

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

## Vektorska oblika

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

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:

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

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

Konjugirani kvaternion:

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

Norma kvaterniona:

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

Inverz kvaterniona:

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

## Vrtenje vektorjev

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:

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

Definirajmo enotski kvaternion:

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

Zavrti vektor je potem:

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

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

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

Iz rotacijske matrike  $R$  lahko izračunamo os rotacije:

Os vrtenja je vzporedna lastnemu vektorju  $\vec{e}$  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  $\cos \varphi = \frac{\text{sl}(R)-1}{2}$

## Topologija

Naj bo  $X$  poljubna množica. Topologija na  $X$  je podana z družino odprtih množic  $\tau$ , 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

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

- $d(x, y) = 0 \iff x = y$
- $d(x, y) = d(y, x)$

- $d(x, y) + d(y, z) \geq d(x, z)$

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 ( $\forall a \in A \exists \varepsilon > 0 : K(a, \varepsilon) \subseteq A$ ).

$A$  je **zaprt množica**  $\iff A^c$  odprta  $\iff$  vsebuje vse svoje robne točke.

Naj bo  $A \subseteq X$ .

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

## Metrizabilnost

$(X, \tau)$  je metrizabilen, če obstaja metrika  $d$  na  $X$ , da  $\tau = \tau_d$

## Zveznost

Funkcija  $f : (X, \tau_X) \rightarrow (Y, \tau_Y)$  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  $f : (X, \tau_X) \rightarrow (Y, \tau_Y)$  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 zvezna, če je praslika vsake odprte množice odprta.*

Naslednje trditve so ekvivalentne:

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

## Homeomorfizmi

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

Prostora  $(X, \tau_X)$  in  $(Y, \tau_Y)$  sta **homeomorfna**. Oznaka  $X \approx Y$ .

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

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

Naslednje trditve so ekvivalentne:

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

## Kompaktnost

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

Prostor  $X$  je **kompakten**, če v vsakem odprtem pokritju  $X$  obstaja končno podpokritje.

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

$$A^{\text{zap}} \subseteq X^{\text{kompakten}} \implies A \text{ kompakten}$$

*Heine-Borel-Lebesgue:*

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

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 kompaktna.

$$f : X \rightarrow Y \text{ zvezna, } A^{\text{kompkt}} \subseteq X \implies f(A) \text{ kompaktna}$$

$X$  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  $X = A \amalg B$  na dve disjunktni, neprazni, odprti podmnožici.

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

$f : X \rightarrow Y$  zvezna,  $X$  povezana  $\implies f(X)$  povezana

$X$  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  $\implies X$  povezan

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