

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  $\forall x \in M \ \exists x^{-1} \in M : x \cdot x^{-1} = x^{-1} \cdot x = e$ .
- **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
- $\forall a, b, c \in R \quad : \quad a(b + c) = ab + ac$  (distributivnost)
- $\forall a, b, c \in R \quad : \quad (a + b)c = ac + bc$  (distributivnost)
- $\forall a, b \in R \quad : \quad ab \in R$  (zaprtost množenja)
- $\forall a, b, c \in R \quad : \quad (ab)c = a(bc)$  (asociativnost\*)
- $\exists e \in R \ \forall a \in R \quad : \quad e \cdot a = a = e \cdot a$  (enota\*)

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

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

Delitelji niča in celi kolobarji

Naj bo  $R$  komutativen koloboar. Tedaj je  $a \in R, \ a \neq 0$  **delitelj niča**, če

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

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

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 niča* 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 niča, bi imeli težave.*

Tako dobimo **obseg ulomkov za K**.

Wedderburnov izrek

Končen kolobar brez deliteljev niča 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

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

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

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

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

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

Jedro / ničelna množica

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

$$\begin{aligned} \forall a \in K, \forall x \in \text{Ker}f : \quad f(ax) &= f(a)f(x) = 0 \\ \implies \text{Ker}f &\triangleleft K \end{aligned}$$

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.

$K$  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  $x, y \in K$ .

$$\begin{aligned} (x) = Kx &= \{kx \mid k \in K\} \\ (x, y) = (x) + (y) &= \{kx + ly \mid k, l \in K\} \end{aligned}$$

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  $\sim$ :

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

$K$  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:

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

$(K/I, +, \cdot)$  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  $d|x$ . 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:

$$\begin{aligned} \bar{f} : K/\text{Ker}f &\rightarrow \text{Im}f \\ \bar{f}(x + \text{Ker}f) &= f(x) \\ K/\text{Ker}f &\cong \text{Im}f \end{aligned}$$

Kolobarji polinomov

Računanje s kompleksnimi števili

$$z = x + iy = re^{i\varphi} = r(\cos \varphi + i \sin \varphi)$$
$$r = |z| = \sqrt{x^2 + y^2} \quad \varphi = \arg z = \arctan \frac{y}{x}$$
$$(a + bi)^{-1} = \frac{1}{a + bi} = \frac{a - bi}{a^2 + b^2}$$

De Moivreova formula

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

Osnovni izrek algebre

Vsak nekonstanten polinom  $a_nx^n + \dots + a_0$  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**.

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

Gaussova lema

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

Hornerjev algoritem

$$a_nx^n + \dots + a_0 = 0$$

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

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

Eisensteinov kriterij

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

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

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

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

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

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

Mobiusova formula

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

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

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

Eulerjeva funkcija

$$\varphi(n) = |\{k \in [n] : D(n, k) = 1\}|$$

= št. proti  $n$  tujih števil, ki so  $\leq n$

$$\varphi(p) = p - 1 \qquad p \in \mathbb{P}$$

$$\varphi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$$

$$\sum_{d|n} \varphi(d) = n$$

Najveĉji skupni delitelj

Za polinoma  $a, b \in F[x]$  obstaja enoliĉno doloĉen najveĉji skupni delitelj  $d = \gcd(a, b)$ .

Razširjen evklidov algoritem

```
vhod: (a, b)
(r0, x0, y0) = (a, 1, 0)
(r1, x1, y1) = (b, 0, 1)
i = 1

dokler ri ≠ 0:
i = i+1
ki = ri-2 // ri-1
(ri, xi, yi) = (ri-2, xi-2, yi-2) - ki(ri-1, xi-1, yi-1)
konec zanke
vrni: (ri-1, xi-1, yi-1)
```

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

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

Gaussova cela števila

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

Gaussovo celo število  $x \neq 0$ , ki ni obrnljivo, je **nerazceпно**, ĉe

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

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

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

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

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* ≤ *F*.

*F* je avtomatično tudi vektorski prostor nad *K* dimenzije dim<sub>*K*</sub>(*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* ≤ *F* in *a* ∈ *F* je

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

- Najmanjši podobseg obsega *F*, ki vsebuje *K* ≤ *F* in *a* ∈ *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* ≤ *F* in *a* ∈ *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*

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

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

$\iff f_a$  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* ∈ *F* *transcendenten* nad *K*, je

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

Če je *a* ∈ *F* *algebraičen* nad *K*, velja:

- ∃ natanko določen **minimalni polinom** *g<sub>a</sub>* ∈ *K*[*x*], ki deli vse polinome z ničlo v *a*. *g<sub>a</sub>* **moničen** (*vodilni koef.* = 1)
- Ker *f<sub>a</sub>* = (*g<sub>a</sub>*)
- K*(*a*) = *K*[*a*] ≅ *K*[*x*]/(*g<sub>a</sub>*)
- [*K*(*a*) : *K*] = deg *g<sub>a</sub>*, **stopnja** *a* nad *K* (oznaka: deg<sub>*K*</sub> *a*)
- Ideal (*g<sub>a</sub>*) ≺ *K*[*x*] je maksimalen  $\implies K[x]/(g_a)$  je obseg

Naj bo *F* končna razširitev *K*, potem za vsak *a* ∈ *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* ≤ *F* in *A* ⊆ *F* množica števil, ki so algebraična nad *K*. Potem je *K*(*A*) algebraična nad *K*.

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 *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 izomorfná  $\mathbb{Z}_p(x^{p^n} - x)$ .

Edini (do izomorfizma) obseg moči *n<sup>p</sup>* je **Galoisov obseg** GF(*p<sup>n</sup>*).

Naj bo *K* končen kolobar (ne nujno komutativen). Če *K* nima deliteljev ničá, je |*K*| = *p<sup>n</sup>* in *K* ≅ GL(*n<sup>p</sup>*).

Galoisovi obsegi

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

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

- u* ∈  $\mathbb{Z}_p[x]$  je nerazcepen polinom stopnje *n*
- elementi GF(*p<sup>n</sup>*) 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/obrnljivih elementov (*GF*(*p<sup>n</sup>*)\*, ·) ≅ ( $\mathbb{Z}_{p^n-1}$ , ·) je vedno izomorfná 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* ∈ ℕ.

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

φ je Eulerjeva funkcija.

Konstruktibilna števila

Število *a* ∈ ℝ je konstruktibilno  $\iff$

$$a \in F_n \qquad \mathbb{Q} = F_0 \leq \cdots \leq F_n$$

kjer je [*F<sub>j</sub>* : *F<sub>j-1</sub>*] = 2 za ∀*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.

·	1	<i>i</i>	<i>j</i>	<i>k</i>
1	1	<i>i</i>	<i>j</i>	<i>k</i>
<i>i</i>	<i>i</i>	−1	<i>k</i>	− <i>j</i>
<i>j</i>	<i>j</i>	− <i>k</i>	−1	<i>i</i>
<i>k</i>	<i>k</i>	<i>j</i>	− <i>i</i>	−1

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

Vektorska oblika

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

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:

$$q_1 q_2 = (t_1 t_2 - \vec{r_1} \cdot \vec{r_2}, \quad t_1 \vec{r_2} + t_2 \vec{r_1} + \vec{r_1} \times \vec{r_2})$$

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

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 φ ∈ ℝ.

Enotski kvaternioni tvorijo grupo:

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

Definirajmo enotski kvaternion:

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

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

$A$  je **zaprta množica** 



⟺


A

c




{\displaystyle \iff A^{\complement }}

 odprta 



⟺


{\displaystyle \iff }

 vsebuje vse svoje robne točke.

Naj bo  $A\subseteq X$ .

- Notranjost** 



Int
(
A
)
=
A
˘


=
{\displaystyle \operatorname {Int} (A)=\dot {A}=}

 največja odprta množica vsebovana v  $A$ .
- Zaprtje** 



Cl
(
A
)
=
A
¯


=
{\displaystyle \operatorname {Cl} (A)=\bar {A}=}

 najmanjša zaprta množica, ki še vsebuje v  $A$  = presek vseh zaprtih množic, ki vsebujejo  $A$
- Rob** 



Fr
(
A
)
=
∂
A
=
A
˙


=
Cl
(
A
)
−
Int
(
A
)


{\displaystyle \operatorname {Fr} (A)=\partial A=\dot {A}=\operatorname {Cl} (A)-\operatorname {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 zvezva, če je praslika vsake odprte množice odprta.*

Naslednje trditve so ekvivalentne:

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

## 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:*

$A\subseteq\mathbb{R}^n$  je kompakten 



⟺


{\displaystyle \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 kompaktn.

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

$X$  kompakten 



⟺


{\displaystyle \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 



⟹


{\displaystyle \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 



⟹


{\displaystyle \implies }

  $X$  povezan

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