Teorija IPM — IŠRM 2024/25

Anton Luka Šijanec

26. junij 2025

Povzetek

Povzeto po zapiskih s predavanj profesorja Pavešića.

Kazalo

1 Algebra

1.1 Kolobarji in obsegi

Definicija. Naj bo K množica, $+ : K \times K \to K$ in $\cdot : K \times K \to K$ pa preslikavi (pišemo ju kot infiksna operatorja). Kolobar je trojica $(K, +, \cdot)$, če je $(K, +)$ abelova grupa in če velja distributivnost – $\forall a, b, c \in K : (a + b) \cdot c = a \cdot c + b \cdot c \wedge c \cdot (a + b) = c \cdot a + c \cdot b$. Poznamo bolj specifične kolobarje, če veljajo še kakšne dodatne lastnosti:

- Če je $\cdot$ asociativni operator ($\forall a, b, c \in K : (a \cdot b) \cdot c = a \cdot (b \cdot c)$), pravimo, da je $(K, +, \cdot)$ asociativni kolobar.
- Če je $\cdot$ komutativni operator ($\forall a, b \in K : a \cdot b = b \cdot a$), pravimo, da je $(K, +, \cdot)$ komutativni kolobar.
- Če obstaja enota za $\cdot$ ($\exists 1 \in K \forall a \in K : a \cdot 1 = 1 \cdot a = a$), pravimo, da je $(K, +, \cdot)$ unitalni kolobar oziroma kolobar z enoto.
- Če so vsi elementi iz $K \setminus \{0\}$ obrnljivi (0 je enota za $+$) ($\forall a \in K \setminus \{0\} \exists b \in K \ni: a \cdot b = b \cdot a = 1$), pravimo, da je $(K, +, \cdot)$ kolobar z deljenjem.

Opomba. Pri tem predmetu bomo kot kolobar, če ni drugače opredeljeno, označili asociativni kolobar z enoto.

Definicija. Obseg je asociativen unitalen komutativen kolobar z deljenjem.

Opomba. Nekateri pravijo, da je obseg asociativen unitalen kolobar z deljenjem (ne predpostavijo komutativnosti) in komutativnemu obsegu pravijo polje. Pri tem predmetu bomo kot obseg označili asociativen unitalen komutativen kolobar z deljenjem.

Zgled. Nekaj primerov kolobarjev:

- Naj bo K kolobar[1]. $K[x]$ so polinomi končne stopnje s koeficienti v K. Elementi so torej oblike $k_0 + k_1 x + k_2 x^2 + \cdots + k_n x^n$ za $k_0, \ldots, k_n \in K$. Označimo $K[x, y] \coloneqq (K[x])[y]$.

  $K[x]$ je asociativen/komutativen/unitalen, kakor hitro je tak tudi K. Četudi bi v K lahko delili, v $K[x]$ nikoli ne moremo. Noben polinom pozitivne stopnje ni obrnljiv (seveda pa so lahko obrnljivi polinomi stopnje 0).

- Naj bo K kolobar. $M_n(K)$ je množica kvadratnih matrik s koeficienti iz K.

  Velja K asociativen $\Rightarrow M_n(K)$ asociativen in K unitalen $\Rightarrow M_n(K)$ unitalen, NE velja pa vedno K komutativen $\Rightarrow M_n(K)$ komutativen. Slednja lastnost bi za poljuben K gotovo veljala le v primeru $n = 1$.

- Naj bo $(K, +, \cdot)$ kolobar. Naj bo $L \subseteq K$, zaprta za $-, \cdot$ ($\forall \circ \in \{-, \cdot\}, a, b \in L : a \circ b \in L$). Tedaj je $(L, +, \cdot)$ podkolobar v $(K, +, \cdot)$, označimo $L \leq K$.

  V podkolobar se gotovo preneseta lastnosti asociativnost in komutativnost.

- Naj bo $(K, +, \cdot)$ kolobar. $\mathcal{F}(X, K) \coloneqq \{f : X \to K\}$ (množica funkcij iz X v K). Običajno na tej množici definiramo $+, \cdot$ takole: $f + g = x \mapsto f(x) + g(x)$ in $f \cdot g = x \mapsto f(x) \cdot g(x)$.

  $(\mathcal{F}(X, K), +, \cdot)$ je kolobar.

- $\mathbb{Z}_n \coloneqq \{0, 1, 2, \ldots, n-1\}$, $+_n$ je seštevanje po modulu n , $\cdot_n$ je množenje po modulu n.

  $(Z_n, +_n, \cdot_n)$ je komutativni asociativni unitalni kolobar.

- Za $p(x) \in K[x]$ je $\left(K[x]/p(x), +_{p(x)}, \cdot_{p(x)}\right)$ kolobar.

- $\left(2^X, \cup, \cap\right)$ ni kolobar, ker ni inverzov za $\cup$.

- $\left(2^X, \oplus, \cap\right)$ je kolobar (boolov kolobar) za $A \oplus B = (A \setminus B) \cup (B \setminus A)$ (disjunktna unija). Nimamo sicer $\cdot$ inverzov, enota za $\cdot$ je X.

[1] Velikokrat samo površno krajše označimo, da je neka množica kolobar in impliciramo, da gre za trojico $(K, +, \cdot)$.

1.2 Delitelji niča

Definicija. $a \neq 0$ je delitelj niča, če $\exists b \neq 0 \ni: a \cdot b = 0$.

Zgled. Nekaj primerov:

- Naj bosta $f, g : \mathbb{R} \to \mathbb{R}$ s predpisoma $f(x) = x + |x|$ in $g(x) = x - |x|$. $f(x) \neq 0$, ker $f(1) = 2$ in $g(x) \neq 0$, ker $g(-1) = -2$. Velja $(f \cdot g)(x) = x^2 - |x|^2 = 0$, torej $f \cdot g = 0$, torej je f delitelj niča in g je delitelj niča.
- $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$
- V $\mathbb{Z}_4$ velja $2 \cdot_4 2 = 0$, v $\mathbb{Z}_6$ velja $2 \cdot_6 3 = 0$. Splošneje sta m in n v $\mathbb{Z}_{m \cdot n}$ delitelja niča.
- Naj bo X množica in $\left(2^X, \oplus, \cap\right)$ boolov kolobar. $\forall A \in 2^X : A \cap (X \setminus A) = \emptyset$, torej so vsi elementi, razen $\emptyset$ in X (enota za $\cap$), deliteji niča.

Trditev. Če je K kolobar brez deliteljev niča, je tudi $K[X]$ brez deliteljev niča.

Dokaz. Naj bosta $p(x)$ in $q(x)$ poljubna neničelna elementa: $0 \neq p(x) = a_n x^n + \cdots + a_n$ in $0 \neq q(x) = b_m x^m + \cdots + b_m$. Tedaj $p(x) \cdot q(x) = a_n b_m x^{n+m} + \cdots$. Ker je $a_n b_m$ neničelno, je $p(x) \cdot q(x)$ neničeln element. □

Trditev. $a \in K$ ne more biti hkrati obrnljiv in delitelj niča.

Dokaz. PDDRAA a je tak element. Naj bo $b \neq 0$ tak, da $a \cdot b = 0$. Naj bo c tak, da $c \cdot a = 1$. Tedaj

$$(ca)\, b = c\, (ab)$$

$$1b = c0$$

$$b = 0$$

$\lightning$ — protislovje $b = 0$ z $b \neq 0$. □

Pripomba. V $\mathbb{Z}$ ni deliteljev niča, obrnljiva pa sta le 1 in -1. Ni torej nujno, da je element v kolobarju bodisi obrnljiv bodisi je delitelj niča. Lahko nekateri elementi iz kolobarja niso niti eno niti drugo.

Trditev. Pravilo krajšanja. Če $a \neq 0$ ni delitelj niča, iz $ax = ay$ sledi $x = y$.

Dokaz.

$$ax = ay$$

$$ax - ay = 0$$

$$a(x - y) = 0$$

$$x - y = 0$$

$$x = y$$

□

Izrek. *Wedderburn. Končen komutativen kolobar brez deliteljev niča je obseg.*

Dokaz. Naj bo $K = \{x_1, \ldots, x_n\}$ kolobar. $\forall a \neq 0 \in K$: elementi $A \coloneqq \{ax_1, \ldots, ax_n\}$ so vsi medsebojno različni, sicer bi iz $ax_i = ax_j$ sledilo $x_i = x_j$. Eden izmed elementov A je 1, eden izmed elementov K je 1. Potemtakem $\exists x_i \ni: ax_i = 1 = x_i a \Rightarrow x_i$ je inverz a. □

Pripomba. Izrek velja brez predpostavljene komutativnosti. Tedaj bi podobno prišli do $ax_i = 1 = x_j a$ in veljalo bi $x_i = x_j$, kajti $(x_i a)\, x_j = x_i\, (a x_j) \Rightarrow 1 x_j = x_i 1$.

Definicija. Če je $(K, +, \cdot)$ kolobar z inverzi vseh neničelnih elementov, je $(K \setminus \{0\}, \cdot)$ grupa. Temu pravimo multiplikativna grupa kolobarja K. Če je K obseg, je njegova multiplikativna grupa abelova (po definiciji obsega).

1.3 Ulomki

Definicija. Naj bo K komutativni kolobar brez deliteljev niča. Ulomek je (a, b) oziroma $\frac{a}{b}$, kjer $b \neq 0$. Množica ulomkov je torej $K \times (K \setminus \{0\})$. Definirajmo relacijo $\frac{a}{b} \sim \frac{c}{d} \Leftrightarrow ad = bc$.

Trditev. Relacija $\sim$ nad ulomki je ekvivalenčna.

Dokaz. Simetrična in refleksivna je očitno. Tranzitivnost:

$$\frac{a}{b} \sim \frac{c}{d} \wedge \frac{c}{d} \sim \frac{e}{f} \Longrightarrow ad = bc \wedge cf = de \Longrightarrow adf = bcf = bde \Longrightarrow (af)\, d = (be)\, d \Longrightarrow af = be \Longrightarrow \frac{a}{b} \sim \frac{e}{f}$$

□

Definicija. $\operatorname{Frac}(K) \coloneqq (K \times (K \setminus \{0\})) / \sim$ so ekvivalenčni razredi ulomkov. Na $\operatorname{Frac}(K)$ vpeljemo $+$ in $\cdot$:

$$\frac{a}{b} + \frac{c}{d} \coloneqq \frac{ad + bc}{bd} \quad \frac{a}{b} \cdot \frac{c}{d} \coloneqq \frac{ac}{bd}.$$

Definicija je dobra, ker je neodvisna od izbire predstavnikov ekvivalenčnih razredov.

Trditev. V $\operatorname{Frac}(K)$ so vsi neničelni elementi (ničelni elementi so oblike $\frac{0}{b}$) obrnljivi.

Dokaz. $\frac{a}{b} \cdot \frac{b}{a} = \frac{a \cdot b}{b \cdot a} = 1$. □

Trditev. Naj bo K komutativni obseg brez deliteljev niča. Tedaj je $\operatorname{Frac}(K) = (K \times K \setminus \{0\} / \sim, +, \cdot)$ obseg (obseg ulomkov za kolobar K).

Zgled. Nekaj primerov:

1. $\operatorname{Frac}(\mathbb{Z}) = \mathbb{Q}$
2. Vedno obstaja funkcija $K \to \operatorname{Frac}(K)$. Funkcija $a \mapsto \frac{a}{1}$ je injektivna. Torej lahko na naraven način gledamo na K kot na podmnožico $\operatorname{Frac} K$. Gre za homomorfizem kolobarjev – podkolobar v $\operatorname{Frac} K$ ob upoštevanju zgornje identifikacije.
3. $\mathbb{R}[x]$ niso obseg, so pa komutativen kolobar brez deliteljev niča. Racionalne funkcije z realnimi koeficienti ($\mathbb{R}(x)$) so pa $\operatorname{Frac}(\mathbb{R}[x])$.
4. Naj bo K kolobar brez deliteljev niča. $K[x]$ je tudi kolobar brez deliteljev niča. Velja $\operatorname{Frac}(K[x]) = \operatorname{Frac}(K)(x)$. Recimo $\operatorname{Frac}(\mathbb{Z}[x]) = \mathbb{Q}(x)$.
5. Za K obseg velja $\operatorname{Frac}(K) = K$ — ob upoštevanju zgornje identifikacije iz točke 2, ki je tokrat tudi surjektivna, kajti $\frac{a}{b} = \frac{ab^{-1}}{1}$.

1.4 Karakteristika kolobarja

Oglejmo si K in 1. V zaporedju $1, 1+1, 1+1+1, \ldots$ se lahko pojavi 0, lahko pa tudi ne. Označimo

$$\overbrace{1 + \cdots + 1}^{n-\text{krat}} =: n1 \text{ (to ni multiplikativna operacija iz kolobarja)}$$

Definicija. Karakteristika K je

$$\operatorname{char} K \coloneqq \min_{n \in \mathbb{N}} n1 = 0$$

Če tak n ne obstaja, definiramo $\operatorname{char} K \coloneqq 0$.

Trditev. $\operatorname{char} K \neq 0 \Longrightarrow \forall a \in K : (\operatorname{char} K)\, a = 0$.

Dokaz. $\left(\overbrace{a + \cdots + a}^{\operatorname{char} K-\text{krat}}\right) = a \cdot \left(\overbrace{1 + \cdots + 1}^{\operatorname{char} K-\text{krat}}\right) = a \cdot 0 = 0$ □

Zgled. Nekaj primerov:

- $\operatorname{char} \mathbb{Z} = \operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = 0$

- $\operatorname{char} \mathbb{Z}_n = n$
- $\operatorname{char} \left(2^X, \oplus, \cap\right) = 2$
- $\operatorname{char} (K[x]) = \operatorname{char} K$
- $\operatorname{char} M_n(K) = \operatorname{char} K$

Trditev. Če je K kolobar brez deliteljev niča, je $\operatorname{char} K = 0$ bodisi je $\operatorname{char} K$ praštevilo.

Dokaz. Če je $\operatorname{char} k = m \cdot n$ za $m, n > 1$, velja $m1 \neq 0 \neq n1$ in $m1 \cdot n1 = (m \cdot n) 1 = 0$, torej $m1$ ali $n1$ sta delitelja niča. □

Definicija. V je vektorski prostor nad obsegom $F \iff (V, +)$ je abelova grupa in za operacijo množenja s skalarji $F \times V \to V$ velja $\forall w, v \in V, a, b \in F : 1 \cdot v = v \wedge (a + b) \cdot v = a \cdot v + b \cdot v \wedge a \cdot (v + w) = a \cdot v + a \cdot w \wedge (a \cdot b) \cdot v = a \cdot (b \cdot v)$.

Trditev. Če kolobar K vsebuje kot podkolobar nek obseg $F \leq K$, potem je K vektorski prostor nad F.

Dokaz. Po definiciji vektorskega prostora. □

Dejstvo. *Naj bo K kolobar in $\operatorname{char} K = p$. Tedaj $\left\{0, 1, 1+1, \ldots, \overbrace{1 + \cdots + 1}^{p-krat}\right\}$ so vsi različni. Ta množica je $\mathbb{Z}_p$. Velja K je vektorski prostor nad $\mathbb{Z}_p$. Posebej, če je K končen, velja $|K| = p^{\dim_{\mathbb{Z}_p} K}$. NE RAZUMEM*

Zgled. Naj bo X poljubna množica. $K \coloneqq \left(2^X, \oplus, \cap\right)$. $\forall A \in K : A \oplus A = \emptyset \Rightarrow \operatorname{char} K = 2$ in K ima $2^{|X|}$ elementov in K je vektorski prostor nad $\mathbb{Z}_2$ in velja $\mathbb{Z}_2 \cong \{\emptyset, X\} \leq K$.

1.5 Homomorfizmi kolobarjev

Definicija. Za K, L kolobarja je $f : K \to L$ homomorfizem $\Leftrightarrow \forall x, y \in K : f(x +_K y) = f(x) +_L f(y) \wedge f(x \cdot_K y) = f(x) \cdot_L f(y)$. Bijektivnemu homomorfizmu pravimo izomorfizem.

Zgled. Nekaj primerov:

- $id : \mathbb{Z} \to \mathbb{Q}$ in $id : \mathbb{Q} \to \mathbb{R}$ in $id : \mathbb{R} \to \mathbb{C}$ so homomorfizmi.
- $\mathbb{Z} \to \mathbb{Z}_n$ s predpisom $x \mapsto x \mod n$ je homomorfizem iz $(\mathbb{Z}, +, \cdot)$ v $(\mathbb{Z}_n, +_n, \cdot_n)$.
- konjugiranje: $\mathbb{C} \to \mathbb{C}$ s predpisom $z \mapsto \overline{z}$ je homomorfizem, kajti $\overline{z + w} = \overline{z} + \overline{w}$ in $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$.
- Naj bo $a \in \mathbb{R}$. Tedaj je $f_a : \mathbb{R}[x] \to \mathbb{R}$ s predpisom $p(x) \mapsto p(a)$ homomorfizem, ker so operacije na polinomih definirane na kodomeni: $(p + q)(a) = p(a) + q(a) \wedge (p \cdot q)(a) = p(a) \cdot q(a)$ po definiciji $+$ v $\mathbb{R}[x]$.
- Splošneje: $f : \mathcal{F}(X, K) \to K$ s predpisom $f \mapsto f(x_0)$ je tudi homomorfizem kolobarjev. VERJAMEM, AMPAK NE RAZUMEM ZAKAJ.
- $K \to M_n(K)$:
  - s predpisom $a \mapsto \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ je homomorfizem kolobarjev: $a + b = \begin{bmatrix} a+b & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}$ in $a \cdot b \mapsto \begin{bmatrix} a \cdot b & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}$
  - s predpisom $a \mapsto \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}$ pa NI homomorfizem kolobarjev, kajti $a \cdot b \mapsto \begin{bmatrix} 0 & a \cdot b \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}$.
- Odvedljive funkcije $C^{(1)}(\mathbb{R})$ so komutativen asociativen unitalen kolobar. Toda operacija odvajanja $C^{(1)}(\mathbb{R}) \to \mathcal{F}(\mathbb{R}, \mathbb{R})$ s predpisom $f \mapsto f'$ ni homomorfizem. Sicer velja $f + g \mapsto f' + g'$, toda ne ohranja produkta, ker $f \cdot g \mapsto f' \cdot g + f' \cdot g \neq f' \cdot g'$.
- Ali je $K \to K$ za komutativen kolobar K s predpisom $x \mapsto x^2$? $(x \cdot y)^2 \mapsto (x \cdot y) \cdot (x \cdot y) = x \cdot x \cdot y \cdot y = x^2 \cdot y^2$, toda $(x + y)^2 \mapsto x^2 + x \cdot y + y \cdot x + y^2 = x^2 + y^2 \Leftrightarrow \operatorname{char} K = 2$.

- $\mathbb{C} \to M_2(\mathbb{R})$ s predpisom $a + bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ je homomorfizem.

Trditev. $a \mapsto a^p$ je homomorfizem $\mathbb{Z}_p \mapsto \mathbb{Z}_p \iff p$ praštevilo.

Dokaz. $(x \cdot y)^p = x^p y^p$ velja. $(x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \cdots + \binom{p}{k}x^{p-k}y^k + \cdots + \binom{p}{p-1}xy^{p-1} + y^p \equiv x^p y^p \mod p$, ker imajo vsi vmesni členi, razen prvega in zadnjega, koeficient oblike

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

ki je vedno deljiv s p in zato enak 0 po modulu p. □

1.5.1 Lastnosti homomorfizmov

Trditev. Za homomorfizem $f : K \to L$ velja:

- $f(0) = 0$.

  Dokaz. $f(0) = f(0+0) = f(0) + f(0) \implies f(0) = 0$. □

- $f(-a) = -f(a)$

  Dokaz. $f(0) = f(a + (-a)) = f(a) + f(-a)$. □

- $f(1_K)$ ni nujno 1_L, kadar pa velja, pa pravimo, da je f unitalen homomorfizem oziroma da ohranja enko.

1.5.2 Jedro in slika homomorfizma in njune lastnosti

Definicija. Naj bo $f : K \to L$ homomorfizem. $\operatorname{Im} f \coloneqq \{f(x); \forall x \in K\}$ je slika f/zaloga vrednosti f in velja $\operatorname{Im} f \subseteq L$. $\operatorname{Ker} f \coloneqq \{x; f(x) = 0\}$ je jedro f oziroma praslika ničle — oznaki $f^{-1}(\{0\}) = f^*(\{0\})$.

Trditev. Za homomorfizem $f : K \to L$ veljaa:

- $\operatorname{Ker} f \leq K$

  Dokaz. Naj bosta $x, y \in \operatorname{Ker} F$ poljubna. Tedaj $f(x+y) = f(x)+f(y) = 0+0 = 0$ in $f(x \cdot y) = f(x) \cdot f(y) = 0 \cdot 0 = 0$. □

- $\operatorname{Im} f \leq L$

  Dokaz. Naj bosta $x, y \in \operatorname{Im} F$ poljubna. Tedaj $f(x) + f(y) = f(x+y)$ in $f(x) \cdot f(y) = f(x \cdot y)$. □

Trditev. Homomorfizem $f : K \to L$ je

- surjektiven $\Leftrightarrow \operatorname{Im} f = L$

  Dokaz. po definiciji □

- injektiven $\Leftrightarrow \operatorname{Ker} f = \{0\}$ (trivialno jedro)

  Dokaz. Naj bosta $x, y \in K$ poljubna.

  ($\Longleftarrow$) $\forall x, y \in K : f(x) = f(y) \Rightarrow 0 = f(x) - f(y) = f(x-y) \Rightarrow x = y$, ker je $f(a) = 0 \Leftrightarrow a = 0 \sim \operatorname{Ker} f = \{0\}$.

  ($\Longrightarrow$) $\forall x, y \in K : ((f(x) = f(y) \Leftrightarrow 0 = f(x) - f(y) = f(x-y)) \Rightarrow (x = y \Leftrightarrow x - y = 0)) \Rightarrow (x - y \in \operatorname{Ker} f \Rightarrow x - y$
  Vsak element v kolobarju lahko opišemo kot razliko dveh elementov v kolobarju, torej $\forall a \in K : a \in \operatorname{Ker} f \Rightarrow a = 0$.

  □

1.6 Ideali

Definicija. Podkolobar $I \leq K$ je ideal $\Leftrightarrow K \cdot I \subseteq I \wedge I \cdot K \subseteq I$, kjer je $A \cdot B = \{a \cdot b; \forall a \in A, b \in B\}$. Označimo $I \lhd K$.

Pripomba. V nekomutativnem kolobarju K se lahko zgodi, da za $I \leq K$ velja le eden izmed pogojev za ideal: $K \cdot I \leq I$ ali $I \cdot K \leq I$. Tak I, za katerega ne veljata obe lastnosti, pač ni ideal.

Dokaz. Naj bo $K = M_2(\mathbb{R})$ in $I = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}; \forall a, b \in \mathbb{R} \right\}$. Velja

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} = \begin{bmatrix} ax+by & 0 \\ cx+dy & 0 \end{bmatrix} \qquad \begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} \cdot \begin{bmatrix} xa & xb \\ ya & yb \end{bmatrix},$$

torej $K \cdot I \leq I$, a ne $I \cdot K \leq I$, torej gre le za levi ideal. Le če je I levi in desni ideal hkrati in s tem dvostranski ideal, je ideal. □

Trditev. $\operatorname{Ker} f$ je ideal.

Dokaz. $\forall x \in \operatorname{Ker} f, a \in K : ax \in \operatorname{Ker} f \wedge xa \in \operatorname{Ker} f$, kajti $0 = f(a) \cdot 0 = f(a) \cdot f(x) = f(a \cdot x) \Leftrightarrow ax \in \operatorname{Ker} f$ in podobno za xa. □

Zgled. Primeri idealov:

1. Neprava ideala: $\{0\}$ in K sta ideala za poljuben kolobar K. (ostali ideali so „pravi“)
2. $2\mathbb{Z} \lhd \mathbb{Z}$. (soda cela števila so ideal v celih številih)
3. za poljuben $n \in \mathbb{Z}$ velja $n\mathbb{Z} \lhd \mathbb{Z}$.
4. Ideali v $\mathbb{Q}$. Naj bo $I \lhd \mathbb{Q}, x \in I, a \neq 0, a \in \mathbb{Q}$. Tedaj $a = \frac{a}{x} \cdot x \in I$, torej $I = \mathbb{Q}$. V racionalnih številih so vsi ideali nepravi.
5. Pravi ideal ne vsebuje obrnljivih elementov. Če je $x \in I \lhd K$ obrnljiv, je $1 = x \cdot x^{-1} \in I$ in zato $\forall a \in K : a \cdot 1 \in I$, torej $I = K$. V obsegu so torej vsi ideali nepravi.

Definicija. Naj bo K komutativni kolobar in $x_1, \ldots x_n \in K$. Idealu $\{a_1x_1 + \cdots + a_nx_n; \forall a_1, \ldots, a_n \in K\}$ pravimo ideal, generiran z naborom $x_1, \ldots, x_n$ in ga označimo z $(x_1, \ldots, x_n)$.

1.6.1 Glavni ideal

Definicija. Naj bo K komutativni kolobar in $a \in K$. $(a) \coloneqq \{a \cdot x; x \in K\} = aK$ (večkratniki a) je ideal v K, generiran z a. Idealu, ki je generiran z enim elementom, pravimo glavni ideal. Alternativna definicija: glavni ideal je generiran z naborom moči 1.

Trditev. Velja

- $(a) = K \Leftrightarrow a$ je obrnljiv v K.

  Dokaz. Dokazujemo ekvivalenco.

  ($\Longrightarrow$) $\exists b \ni: b \cdot a = 1 \Rightarrow b = a^{-1}$ torej je a obrnljiv.

  ($\Longleftarrow$) Že dokazano zgoraj pri primeru 5.

  □

- K je obseg $\Leftrightarrow$ nima pravih idealov.

  Dokaz. Dokazujemo ekvivalenco.

  ($\Longrightarrow$) Že dokazano zgoraj pri primeru 5.

  ($\Longleftarrow$) $\forall a \neq 0 : (a) = K \Longrightarrow$ po prejšnji točki je a obrnljiv.

□

Trditev. V $\mathbb{Z}$ so vsi ideali glavni.

Dokaz. Naj bo $I \triangleleft \mathbb{Z}$. Kakšne so možnosti za I? Velja $I \leq \mathbb{Z} \implies 0 \in I$ in $\forall x \in I : -x \in I$. Denimo, da je a najmanjši pozitivni element v I. Trdimo, da je $I = (a)$. Očitno velja $I \supseteq (a)$. Dokazati je treba še $I \subseteq (a)$. $\forall x \in I \exists q \in \mathbb{Z}, r \in \mathbb{Z} : x = a \cdot q + r \wedge r < a \implies r = x - a \cdot q \in I$ (ker $x \in I$ in $a \cdot q \in I$). Ker je a najmanjši pozitivni element v I in $r < a$, je $r = 0$ in zato $x = a \cdot q$ in zato $I \subseteq (a)$ in zato $I = (a)$. □

Definicija. Kolobar, v katerem so vsi ideali glavni, imenujemo glavnoidealski kolobar.

Zgled. Ali je $(2) \cup (3) \triangleleft \mathbb{Z}$ ideal? Ne, ker ne vsebuje $3 - 2 = 1$ (multiplikativne enote) in zato ni podkolobar kolobarju $\mathbb{Z}$.

Trditev. Naj bo K obseg. Tedaj je $K[x]$ glavnoidealski kolobar.

Dokaz. Vemo, da so v $K[x]$ obrnljivi natanko tisti elementi, ki so obrnljivi v K. Naj bo $I \triangleleft K[x]$ poljuben. Tedaj $I \leq K[x]$ in zato $0 \in I \wedge \forall x \in I : x \in I \Rightarrow -x \in I$. Denimo, da je $p(x)$ poljuben polinom najnižje pozitivne stopnje v I. Dokažimo, da $I = (p(x))$. Očitno velja $I \subseteq (p(x))$. Dokažimo še $I \subseteq (p(x))$: $\forall s(x) \in I \exists q(x), r(x) \in I \ni$: $s = pq + r \wedge \deg r < \deg p \wedge r = s - pq \in I$ (ker $s \in I$ in $pq \in I$). Ker je p polinom z najmanjšo pozitivno stopnjo v I in $r \in I$, je $\deg r = 0$ in zato $I \subseteq (p(x))$ in zato $I = (p(x))$. □

Pripomba. Za a obrnljiv in x poljuben v K je $(a \cdot x) = (x)$. NE RAZUMEM, ampak je potrebno za dokaz.

Pripomba. Če K ni obseg, $K[x]$ ni glavnoidealski.

Zgled. V $\mathbb{Z}[x]$ vzemimo $I = (x, 2) = \{x \cdot p(x) + 2 \cdot q(x); \forall p(x), q(x) \in \mathbb{Z}[x]\}$. Ne obstaja element, ki deli 2 in x hkrati v $\mathbb{Z}[x]$.

Zgled. Naj bo K obseg. $K[x]$ je glavnoidealski, a ni obseg, ker ima prave ideale. $K[x, y] = (K[x])[y]$ ni glavnoidealski — (x, y) ni glavni ideal.

1.7 Kvocientni kolobarji

Definicija. Naj bo $I \triangleleft K$ poljuben ideal. Definirajmo relacijo $a \sim_I b :\Leftrightarrow a - b \in I$. Je ekvivalenčna, ker $a \sim_I a \Leftrightarrow 0 \in I$ (refleksivnost), $a - b \in I \Leftrightarrow b - a \in I$ (simetričnost), $a - b \in I \wedge b - c \in I \Rightarrow (a - b) + (b - c) \in I \Rightarrow a - c \in I$ (tranzitivnost). Z $K/\sim_I$ označimo množico ekvivalenčnih razredov. $[a] = a + I = \{a + i; \forall i \in I\}$.

Zgled. V $\mathbb{Z}$ vzemimo (5) in vpeljimo $\sim_{(5)}$: elementa sta ekvivalentna, če imata isti ostanek pri deljenju s 5: $[0] = \{0, -5, 5, -10, 10, \dots\}$, $[1] = \{1, 6, 11, -4, -9, \dots\}$, $[2] = \{2, 7, -3, 12, -8, \dots\}$.

Definicija. Definirajmo seštevanje $+_I$ in množenje $\cdot_I$ na $K/\sim_I$: $(a + I) +_I (b + I) \coloneqq (a + b) + I$ in $(a + I) \cdot_I (b + I) \coloneqq (a \cdot b) + I$.

Dokaz. Konkretnost definicije — definicija je dobra; naj bo $a + I = a' + I$ $(a - a' \in I)$ in $b + I = b' + I$ $(b - b' \in I)$.

$(a + b) + I = (a' + b') + I \iff a - a' + b - b' = (a + b) - (a' - b') \in I$

$(a \cdot b) + I = (a' \cdot b') + I \iff a \cdot b - a' \cdot b' = a \cdot (b - b') + (a - a') \cdot b' \in I$

□

Definicija. Za $I \triangleleft K$ je $(K/\sim_I, +_I, \cdot_I)$ kvocientni kolobar K/I.

Zgled. Nekaj primerov:

- $\mathbb{Z}_n = \mathbb{Z}/(n)$
- $K/(0) = K$
- $K/K = \{0\}$ — trivialni kolobar
- $\mathbb{R}[x]/(x)$: vsak element $\mathbb{R}[x]$ je v $a + (x)$ za nek $a \in \mathbb{R}$; oglejmo si $p(x) \in \mathbb{R}[x]$. Velja $p(x) = a_0 + a_1 x^1 + \dots + a_n x^n = a_0 + x\left(a_1 + a_2 x + a_3 x^2 + \dots + a_n x^{n-1}\right)$. Potemtakem $\mathbb{R}[x]/(x) \cong \mathbb{R}$.

- $\mathbb{R}[x]/(x^2)$: predstavniki so $(a+bx)+(x)$ za $a,b\in\mathbb{R}$. Pišimo jih kot (a,b). Velja $(a,b)+(c,d)=(a+b,c+d)$ in $(a,b)\cdot(c,d)=[(a+bx)(c+dx)]=\left[ac+adx+bcx+bdx^2\right]=[ac+adx+bcx]=(ac,ad+bc)$
- $\mathbb{R}[x]/(x^2+1)$: ostanki so linearni polinomi $(a+bx)$. Pišimo jih kot $(a,b)\in\mathbb{R}^2$. Velja $a+bx+(x^2+1)+c+dx+(x^2+1)=a+c+(b+d)x+(x^2+1)$, torej kot prej $(a,b)+(c,d)=(a+c,b+d)$. Velja

  $$[a+bx]\cdot[c+dx]=\left[ac+adx+bcx+\left(bdx^2\right)\right]=\left[ac+adx+bcx+\left(bd\left(x^2+1\right)-bd\right)\right]=[ac+adx+bcx-bd],$$

  torej $(a,b)\cdot(c,d)=(ac-bd,ad+bc)$. To je ravno množenje v $\mathbb{C}$. Torej $\mathbb{R}[x]/(x^2+1)\cong\mathbb{C}$.

1.8 Izrek o izomorfizmu NE RAZUMEM

Izrek. *Naj bo $\varphi:K\to L$ poljuben homomorfizem kolobarjev. Vemo, da je $\operatorname{Ker}\varphi\triangleleft K$. Pravilo $\overline{\varphi}:K/\operatorname{Ker}\varphi\xrightarrow{\cong}\operatorname{Im}\varphi$ s predpisom $\overline{\varphi}(x+\operatorname{Ker}\varphi):=\varphi(x)$ določa izomorfizem kolobarjev. Temu $\overline{\varphi}$ pravimo kvocientni homomorfizem.*

Dokaz. Definirajmo $\overline{\varphi}:x+\operatorname{Ker}\varphi\mapsto\varphi(x)$.

- Dobra definiranost: Naj bo $x'\in[x]\sim x+\operatorname{Ker}\varphi=x+\operatorname{Ker}\varphi$. Tedaj $x'=x+(x'-x)\Rightarrow\varphi(x')=\varphi(x)+\cancelto{0}{\varphi(x-x')}=\varphi(x)$, ker $x-x'\in\operatorname{Ker}\varphi$. Torej je $\overline{\varphi}$ dobro definiran.
- Ali je $\overline{\varphi}$ homomorfizem? Da:

  $$\overline{\varphi}\left((x+\operatorname{Ker}\varphi)\dot{+}(x'+\operatorname{Ker}\varphi)\right)=\overline{\varphi}\left(\left(x\dot{+}x'\right)+\operatorname{Ker}\varphi\right)=\varphi\left(x\dot{+}x'\right)=\varphi(x)\dot{+}\varphi(x')=\overline{\varphi}(x+\operatorname{Ker}\varphi)\dot{+}\overline{\varphi}(x+\operatorname{Ker}\varphi)$$

- $\operatorname{Im}\overline{\varphi}=\operatorname{Im}\varphi$, torej velja surjektivnost.
- $\operatorname{Ker}\overline{\varphi}=\operatorname{Ker}\varphi=0+\operatorname{Ker}\varphi\in K/\operatorname{Ker}\varphi$ (trivialno jedro $\Rightarrow$ injektivnost)

□

Zgled. Vzemimo $\mathbb{R}[x]$. Oglejmo si $\varphi_i:\mathbb{R}[x]\to\mathbb{C}$ s predpisom $p(x)\mapsto p(i)$. Velja $\operatorname{Ker}\varphi_i=$ polinomi, ki so deljivi z $(x-i)$ in posledično z $(x+i)$ (ker ničle nastopajo konjugirano), torej s produktom (x^2+1). Slika tega φ_i so vsa kompleksna števila. Torej $\overline{\varphi_i}:\mathbb{R}[x]/(x^2+1)\xrightarrow{\cong}\mathbb{C}$.

Vprašanje. *Kaj so ideali v K/I?*

Naj bo $q:K\to K/I$ homomorfizem in $J\triangleleft K$ poljuben. Tedaj $J\mapsto q_*(J)$. $q_*(J)=\{q(a);\forall a\in J\}=\{a+I;\forall a\in J\}$. Za poljubna $x\in K,a\in J$ velja $(x+I)\cdot(a+I)=x\cdot a+I\in q_*(J)$. Torej ideal v K se s q preslika v ideal v K/I. Torej obstaja bijekcija med ideali, ki vsebujejo I in ideali v K/I.

Izrek. *$q:K\to K/I$ kvocientni homomorfizem določa bijekcijo, ki ideale v K, ki vsebujejo I, preslika v ideale v K/I. $J\mapsto q_*(J)$ in $q^*(J')\hookleftarrow J'$.*

Zgled. Kaj so ideali v $\mathbb{Z}_{12}=\mathbb{Z}/(12)$? To so vsi ideali v $\mathbb{Z}$, ki vsebujejo ideal (12). V $\mathbb{Z}$ velja $(a)\leq(b)\Leftrightarrow b|a$. Torej so vsi ideali v $\mathbb{Z}_{12}$ ravno $(1)=\mathbb{Z},(2),(3),(4),(6),(12)$. Velja: $\mathbb{Z}/(12)=\{0\}$, $\mathbb{Z}/(3)=\{3,6,9,0\}$, $\mathbb{Z}/(6)=\{0,6\}$, $\mathbb{Z}/(2)=\{0,2,4,6,8,10\}$, $\mathbb{Z}/(4)=\{0,4,8\}$, $\mathbb{Z}(1)=\{0,1,2,3,4,5,6,7,8,9,10,11\}$.

Posledica. *K/I je obseg $\Longleftrightarrow$ K/I nima pravih idealov $\Longleftrightarrow$ v K ni idealov, ki vsebujejo I,razen I in K $\Longleftrightarrow$ v $K\nexists$ ideal $J\ni:I\neq J\wedge J\neq K\Longleftrightarrow I$ je maksimalen pravi ideal v K.*

Definicija. $a\in K$ je nerazcepen $\Leftrightarrow\nexists$ neobrnljiva $b,c\ni:a=b\cdot c$.

Trditev. V glavnoidealskem kolobarju K je ideal (a) maksimalen $\Leftrightarrow a$ je nerazcepen.

Dokaz. Dokazujemo ekvivalenco.

($\Rightarrow$) Naj bo (a) maksimalen in hkrati a razcepen. $a=b\cdot c$ za neobrnljiva b in $c\Longrightarrow(a)\triangleleft(b)\triangleleft K\wedge(a)\triangleleft(c)\triangleleft K$ in ker sta b in c neobrnljiva, $(a)\neq(b)\wedge(b)\neq k\wedge(a)\neq(c)\wedge(c)\neq K$. Sledi, da (a) ni maksimalen.

($\Leftarrow$) Dokazujemo, da če (a) ni maksimalen $\Rightarrow\exists b\ni:a=b\cdot c$. Ker (a) ni maksimalen, $\exists b\ni:(a)\overset{\neq}{\triangleleft}(b)\overset{\neq}{\triangleleft}K$. Velja $a=b\cdot c$ in c ni obrnljiv, ker $(a)\neq(b)$.

□

Zgled. $\mathbb{R}[x]/(x^2)$ ni obseg, ker je (x^2) razcepen nad $\mathbb{R}[x]$. $\mathbb{R}[x]/(x^2+1)$ je obseg, ker (x^2+1) ni razcepen nad $\mathbb{R}[x]$.

1.9 Obsegi

Zgled. Nekaj primerov:

- $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C} \leq \mathbb{C}(x)$, $\mathbb{R} \leq \mathbb{R}(x) \leq (\mathbb{R}(x))(y)$, $\mathbb{Z}_p \leq \mathbb{Z}_p(x)$.
- $\mathbb{Q} < \left\{a + b\sqrt{2}; a, b \in \mathbb{Q}\right\} < \mathbb{R}$

  Dokaz. Zaprtost za seštevanje, množenje, odštevanje, deljenje — da:

$$a + b\sqrt{2} + c + d\sqrt{2} = a + c + (b + d)\sqrt{2}$$

$$\left(a + b\sqrt{2}\right)\left(c + d\sqrt{2}\right) = a + c + ad\sqrt{2} + bc\sqrt{2} + 2bd = ac + 2bd + (ad + bc)\sqrt{2}$$

$$a + b\sqrt{2} - \left(c + d\sqrt{2}\right) = a - c + (b - d)\sqrt{2}$$

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{\left(a + b\sqrt{2}\right)\left(c - d\sqrt{2}\right)}{c^2 - 2d^2} = \frac{ac - 2bd}{c^2 - 2d^2} + \frac{-ad + bc}{c^2 - 2d^2}\sqrt{2}$$

  □

- $\left\{a + b\sqrt[3]{4} + c\sqrt[3]{16}; a, b, c \in \mathbb{Q}\right\}$ je obseg
- $\mathbb{Z}_2/\left(x^2 + x + 1\right)$ je obseg po prejšnjem izreku ker je $\mathbb{Z}_2$ glavnoidealski kolobar in $\left(x^2 + x + 1\right)$ nerazcepen polinom.

1.10 Konstruktibilna števila

... so števila, ki jih lahko konstruiramo z ravnilom in šestilom. Najprej nekaj uvodnih besed; recimo: ne poznamo splošne konstrukcije za razdelitev danega kota na tretjine (trisekcija kota). V 1837 so dokazali, da to za poljubni kot ni možno — za specifične pa seveda je, denimo za kot pravi kot.

Tipična vprašanja so naslednja:

- Ali je moč podvojiti kocko po volumnu, torej če imamo a, ali lahko dobimo b, da bo $2a^3 = b^3$ oziroma $b = \sqrt[3]{2}a$? Izkaže se, da ne.
- Ali je moč konstruirati kvadrat z enako ploščino kot dan krog? Ne.
- Ali je moč narisati pravilni mnogokotnik? Možno je narisati pravilne $\{3..6\}$ kotnike, sedemkotnika se ne da (dokazal Gauss). Gauss je tudi konstruiral sedemnajstkotnik.

Dopustni operaciji sta

- skozi dve točki potegnemo premico in
- za dani dve točki konstruiramo krožnico s središčem v eni točki, ki gre skozi drugo.
- Upoštevamo, da
  - so presečišča nove točke,
  - rišemo v ravnini in
  - veljajo ostali Evklidovi aksiomi.

Konstrukcija števil

1. Fiksiramo enotsko dolžino, t. j. 1 je konstruktibilno število.
2. Za konstruktibilni števili a in b je točka (a, b) konstruktibilna in obratno.
3. Konstruktibilni točki (a, b) in (c, d) tvorita konstruktibilno premico/krožnico.
4. Preseki slednjih so konstruktibilne točke.

Definicija. Označimo K kot množico vseh realnih števil, ki jih lahko dobimo kot rezultat končnega števila korakov 2–4.

Izrek. *K je obseg za operacije $+, -, \cdot, \div$ iz obsega realnih števil in velja $\mathbb{Q} < K < \mathbb{R}$.*

Dokaz. Dokazujemo več stvari:

- Zaprtost za $+$ je očitna: uporabimo šestilo za prenos seštevancev.
- Zaprtost za množenje: $(a \cdot b) : b = a : 1$ — BSŠ Naj bo $a \geq b$. Imejmo pravokotni trikotnik s katetama dolžin 1 in b. Konstruirajmo daljico dolžine a, ki je podaljšek katete dolžine 1 proti pravemu kotu. Narišimo vzporednico kateti dolžine b v krajišču daljice dolžine a, ki ni na izvornem trikotniku. Narišimo vzporednico hipotenuzi. Daljica, ki leži na narisani vzporednici in je omejena s premico, na kateri leži hipotenuza in premico, na kateri leži daljica dolžine a, je dolga $a \cdot b$ — Uporabili smo podobnost trikotnikov — skalirali smo izvorni trikotnik s faktorjem a.
- Deljenje napravimo podobno.
- Konstruiramo lahko koren poljubnega konstruktibilnega števila a: Na sredini krožnice premera $1 + a$ narišemo premico. Presečišči premice in krožnice naj bosta točki A in B. Na AB narišimo C, da bo $|CB| = a$. Torej je $|AC| = 1$. V točki C narišemo pravokotnico na premico in presečišče pravokotnice s krožnico označimo z D. Dobimo dva pravokotna trikotnika, enega s stranicami $\left(1, x, \sqrt{1 + x^2}\right)$ in drugega s stranicama $\left(x, a, \sqrt{a^2 + x^2}\right)$. Kote imata iste — podobna sta si — in posledično velja $\frac{a}{x} = \frac{x}{1}$ oziroma $a = x^2$ oziroma $x = \sqrt{a}$. Torej $\mathbb{Q} < K$.
- $\mathbb{R} \neq K$, ker je kardinalnost K števna, $\mathbb{R}$ pa ne. Končno mnogo korakov potrebujemo, da konstruiramo katerokoli število v K.

□

Dejstvo. *Vemo, da $\pi \notin K \wedge e \notin K$. Dokaz je zelo dolg.*

Opomba. Še danes ne vemo, ali je $\pi + e \in K$.

Definicija. Označimo s K_{n+1} najmanjši podobseg $\mathbb{R}$, ki vsebuje vse kvadratne korene pozitivnih elementov K_n. Naj bo $K_0 = \mathbb{Q}$.

Tedaj velja

$$\mathbb{Q} = K_0 \leq K_1 \leq K_2 \leq K_2 \leq \cdots \leq K = \bigcup_{n=1}^{\infty} K_n.$$

1.11 Razširitve obsegov

Definicija. Za $K \leq F$ (K podobseg F) pravimo: F je razširitev obsega $K \sim F$ je vektorski prostor nad K. Če je $[F : K] \coloneqq \dim_K F$ končna, gre za končno razširitev, če pa je neskončna, pa gre za neskončno razširitev.

Zgled. Nekaj primerov:

- $[\mathbb{R} : \mathbb{Q}]$ je neskončna razširitev
- $[\mathbb{C} : \mathbb{R}]$ je končna razširitev stopnje 2
- $\left[\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}\right) : \mathbb{Q}\right]$ je končna razširitev stopnje 6

Izrek. *Če je $K \leq F \leq E$, je $[E:K] = [E:F] \cdot [F:K]$.*

Dokaz. Privzemimo, da sta $m \coloneqq [F:K]$ in $n \coloneqq [E:F]$ končni. Tedaj $\exists \{x_1, \ldots, x_m\}$ baza za F nad K ZDB vsak element F lahko napišemo kot linearno kombinacijo m elementov obsega K in ti elementi so se medsebojno linearno neodvisni. Prav tako $\exists \{y_1, \ldots, y_n\}$ baza za E nad F. Dokažimo, da je $\{x_1, \ldots, x_m\} \cdot \{y_1, \ldots, y_n\}$ baza za E nad K:

- Ali razpenja cel E? Naj bo $e \in E$ poljuben. $e = f_1 y_1 + \cdots + f_n y_n$, $f_i \in F$ sedaj zapišimo kot linearne kombinacije elenentov iz K: $\forall i \in \{1..n\} : f_i = k_{i1} x_1 + \cdots + k_{im} x_m$. Potemtakem

$$e = \sum_{i=1}^{n} (f_i)\, y_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} k_{ij} x_j \right) y_i = \sum_{i,j} k_{ij} (x_j y_i).$$

- Ali je linearno neodvisna množica?

$$\sum_{i,j} k_{ij} x_j y_i = 0 = \sum_{i} \underbrace{\left(\sum_{j} k_{ij} x_j \right)}_{\in F} \overset{\text{el. baze}}{y_i} \Longrightarrow \sum_{j} k_{ij} \overset{\text{el. baze}}{x_j} = 0 \Longrightarrow k_{ij} = 0.$$

Torej smo dokazali, da je $\dim_K E = m \cdot n$.

□

Posledica. *$\nexists K \ni: \mathbb{R} < K < \mathbb{C}$; ker je $[\mathbb{C}:\mathbb{R}] = 1$ je bodisi $[K:\mathbb{R}] = 1$ in s tem $K = \mathbb{R}$ bodisi $[\mathbb{C}:K] = 1$ in s tem $\mathbb{C} = K$.*

Trditev. Najmanjši podkolobar F, ki vsebuje K in a je $K[a] \coloneqq \{p(a); p \in K[x]\}$. Najmanjši podobseg F, ki vsebuje K in a je $K(a) \coloneqq \left\{ \frac{p(a)}{q(a)}; p, q, \in K[x] \wedge q(a) \neq 0 \right\}$.

Dokaz. Vsak kolobar, ki vsebuje K in a mora vsebovati še vse potence a in njihove $k-$linearne kombinacije $k_0 + k_1 a + k_2 a^2 + \cdots + k_n a_n$.

Zlahka preverimo, da je množica vseh teh vrednosti zaprta za $+, -, \cdot$, torej je kolobar in sicer minimalni podkolobar F, ki vsebuje K in a.

Za dokaz trditve o podobsegih opazimo, da mora podobseg vsebovati še vse kvociente, ki jih predstavimo ravno z ulomki oblike $\frac{p(a)}{q(a)}$, kadar so ti definirani ($q(a) \neq 0$).

Preveriti moramo, da je množica teh vrednosti zaprta za $+, -, \cdot, \div$. Npr. za vsoto imamo

$$\frac{p(a)}{q(a)} + \frac{r(a)}{s(a)} = \frac{p(a)\, s(a) + q(a)\, r(a)}{q(a)\, s(a)},$$

kar je spet ulomek. Za ostale operacije je premislek podoben. □

Zgled. Nekaj zgledov:

- $\mathbb{Q}[\sqrt{2}] = \left\{ a_0 + a_1\sqrt{2} + a_2\sqrt{2} + \cdots + a_n\sqrt{2}^n; a_i \in \mathbb{Q}, \forall n \in \mathbb{N} \right\}$. Ker $\sqrt{2}^2 = 2$, lahko izraze poenostavimo in dobimo $\mathbb{Q}[\sqrt{2}] = \left\{ a + b\sqrt{2}; a, b \in \mathbb{Q} \right\}$.
- $\mathbb{R}[\pi] = \left\{ a_0 + a_1\pi + a_2\pi^2 + \cdots + a_n\pi^n; a_i \in \mathbb{Q}, \forall n \in \mathbb{N} \right\}$. Se to da poenostaviti? Ne.
- $\mathbb{R}[i] = \{a + bi; a, b \in \mathbb{R}\} = \mathbb{C}$
- $\mathbb{Q}(\sqrt{2}) = \left\{ \frac{a+b\sqrt{2}}{c+d\sqrt{2}}; a, b, c, d \in \mathbb{Q} \right\}$, toda $\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{(a+b\sqrt{2})(c-d\sqrt{2})}{(c+d\sqrt{2})(c-d\sqrt{2})} = \frac{a-2bd}{c^2-2d^2} + \frac{bc-ad}{c^2-2d^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, zato je $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$.
- $\mathbb{Q}(\pi) \neq \mathbb{Q}[\pi]$. Se to da razložiti?

Definicija. Definicije in oznake $K[a]$ in $K(a)$ lahko uporabimo tudi, kadar obsegu K dodamo več elementov: Naj bo $K \leq F, a_1, \ldots, a_n \in F$. Tedaj $K[a_1, \ldots, a_n]$ oziroma $K(a_1, \ldots, a_n)$ je najmanjši podkolobar (oz. podobseg) F, ki vsebuje K in $a_1, \ldots, a_n$. Velja: $K[a_1, a_2] = (K[a_1])[a_2] = (K[a_2])[a_1]$ in $K(a_1, a_2) = (K(a_1))(a_2) = (K(a_2))(a_1)$, t. j. elemente F lahko dodajamo postopoma in v poljubnem vrstnem redu.

Definicija. Razširitev je enostavna, če obsegu K dodamo en element $a \in F$.

Oglejmo si homomorfizma kolobarjev $\varphi_a : K[x] \to F$ s predpisom $p(x) \mapsto p(a)$. Ločimo možnosti, da je φ_a injektiven ali da φ_a ni injektiven.

$$\operatorname{Ker} \varphi_a = \{p(x) \in K[x]; p(a) = 0\}$$

Če je φ_a injektiven, je $\operatorname{Ker} \varphi_a = \{0\}$, torej a ni ničla nobenega netrivialnega polinoma s koeficienti v K. Tedaj pravimo, da je a transcendenten nad K.

Če nasprotni φ_a ni injektiven, potem obstaja netrivialen polinom s koeficienti v K, ki ima a za ničlo. Pravimo, da je a algebraičen nad K.

Če so vsi elementi F algebraični nad K, pravimo, da je F algebraična razširitev K. V nasprotnem primeru (t. j., če je vsaj en element F transcendenten nad K), pa je F transcendenten nad K.

Zgled. Nekaj primerov:

- $i \in \mathbb{C}$ je ničla polinoma $x^2 + 1 \in \mathbb{Q}[i]$, zato je i algebraičen nad $\mathbb{Q}$. Obseg $\mathbb{C}$ pa ni algebraična razširitev $\mathbb{Q}$, čer nekatera števila, npr. π, e niso ničle nobenega polinoma z racionalnimi koeficienti. Podobno $\mathbb{R}$ ni algebraična razširitev $\mathbb{Q}$.

  Opomba. Za dano število je običajno zelo težko dokazati, da ni ničla nobenega polinoma s koeficienti v $\mathbb{Q}$. Nasprotno pa ni prav nič težko dokazati, da obstajajo taka realna števila, ki so transcendentna nad $\mathbb{Q}$. $\mathbb{Q}$ je števen, zato je $\mathbb{Q}[x]$ števna, posledično pa je števna tudi množica njihovih realnih ničel. Torej so skoraj vsa realna števila transcendentna nad $\mathbb{Q}$.

- $\mathbb{C}$ je algebraična razširitev $\mathbb{R}$, ker je $a + bi \in \mathbb{C}$ ničla polinoma $x^2 - 2ax + \left(a^2 + b^2\right) \in \mathbb{R}[x]$.

Če je $a \in F$ transcendenten nad K, potem $\varphi_a : K[x] \to F$ lahko enolično razširimo na obseg ulomkov in dobimo injektivni homomorfizem $\overline{\varphi_a} : K(x) \to F$.

Izrek. *Če je a transcendenten nad $K \leq F$, potem je $K[a] \cong K[x]$ in $K(a) \cong K(x)$.*

Dokaz. Očitno. □

Zgled. $\mathbb{Q}[\pi] \cong \mathbb{Q}[e]$, ker sta oba izomorfna $\mathbb{Q}[x]$.

Definicija. Če je $a \in F$ algebraičen nad K, potem je $\operatorname{Ker} \varphi_a$ pravi ideal v $K[x]$. V $K[x]$ so vsi ideali glavni, zato je $\operatorname{Ker} \varphi_a = (g)$ ta nek polinom $g \in K[x]$. Če dodatno zahtevamo, da je g moničen (t. j., vodilni koeficient ima 1), potem je g enolično določen in mu pravimo minimalni polinom za element a nad K in ga označimo z $g_a(x)$.

Po izreku o izomorfizmu velja $K[a] \cong K[x]/(g_a)$.

Zgled. $\mathbb{Q}\left[\sqrt{2}\right] \cong \mathbb{Q}[x]/\left(x^2 - 2\right)$, ker $g_{\sqrt{2}}(x) = x^2 - 2$.

Lema. *Ideal $(g_a) \lhd K[x]$ je maksimalen.*

Dokaz. Dovolj je pokazati, da je $g_a(x)$ nerazcepen. Če bi veljalo $g(x) = p(x) \cdot q(x)$ za polinoma strogo nižje stopnje v $K[x]$, bi iz $0 = g(a) = p(a) \cdot q(a)$ dobili $p \in \operatorname{Ker} \varphi_a \wedge q \in \operatorname{Ker} \varphi_a$, torej $p(a) = 0$ ali $q(a) = 0$. To je v protislovju z zahtevo, da je g_a tak v $K[x]$, da ima najmanjšo stopnjo izmed tistih, ki anhilirajo a. □

Posledica. *$K[x]/(g_a)$ je obseg, torej $K(a) \cong K[a]$. Če je g_a polinom stopnje n, lahko $p \in K[x]$ enolično predstavimo kot $p = g_a \cdot q + r$, kjer je $\deg r < \deg n$. Zato je $K[x]/(g_a)$ vektorski prostor z bazo $1 + (g_a)$, $x + (g_a)$, $x^2 + g(a)$, ..., $x^{n-1} + (g_a)$. Izomorfizem $\overline{\varphi_a}$ to bazo preslika v elemente $1, a, \ldots, a^{n-1} \in F$. Potemtakem $K(a) = K[a]$ je $K-$vektorski prostor z bazo $1, a, a^2, \ldots, a^{n-1}$.*

Izrek. *Naj bo $a \in F$ algebraičen nad $K \leq F$. Tedaj velja*

1. *Obstaja natanko en moničnі polinom $g_a(a)$, ki deli vse polinome, ki imajo a za ničlo.*
2. *Minimalna razširititev $K(a) = K[a] \cong K[x]/(g_a(x))$.*
3. *$[K(a) : K] = \deg g_a$ ZDB stopnja razširitve (pišemo $\deg_K a$) = stopnja minimalnega polinoma*
4. *Baza za $K(a)$ nad K je $1, a, \ldots, a^{\deg g_a - 1}$.*

Posledica. *Če je F končna razširitev K, potem za vsak $a \in F$ velja $\deg_K a \mid [F : K]$.*

Dokaz. Iz $K \leq K(a) \leq F$ sledi $[F:K] = [F:K(a)] \cdot [K(a):K] = [F:K(a)] \cdot \deg_K a$. □

Ta posledica je ključna sestavina za odgovor na vprašanje o konstrukcijah z ravnilom in šestilom. Videli smo, da vsako zaporedje konstrukcij ustvari zaporedje realnih števil $a_1, \ldots, a_n$, kjer je a_i koren linearnega ali kvadratnega polinoma s koeficienti v $\mathbb{Q}(a_1, \ldots, a_{i-1})$. To pomeni, da leži vsako konstruktibilno število v neki razširitvi $\mathbb{Q}$ stopnje 2^m, torej velja:

Stopnja (nad $\mathbb{Q}$) konstruktibilnega števila je potenca števila 2.

Z drugimi besedami: Vsako konstruktibilno število dobimo s končnim zaporedjem operacij, kjer bodisi ostanemo v istem obsegu bodisi dodamo kvadratni koren nekega elementa $\Rightarrow$ vsako konstruktibilno število je v neki razširitvi stopnje 2^k obsega $\mathbb{Q}$.

Zgled. Nekaj primerov:

- Podvojitev kocke: $\sqrt[3]{2}$ ni konstruktibilno. $x^2 - 2$ je nerazcepen, moničen in ima $\sqrt[3]{2}$ za ničlo, vendar ni stopnje 2^k.
- Kvadratura kroga: $\sqrt{\pi}$ ni algebraično število. Ne bomo dokazali.
- Trisekcija kota: Dan je konstruktibilen kot α. α je konstruktibilen $\Leftrightarrow \cos\alpha$ in $\sin\alpha$ sta konstruktibilni števili. Ali velja $\cos\alpha$ konstruktibilen $\Rightarrow \cos\frac{\alpha}{3}$ konstruktibilen? Velja $\cos\alpha = 4\cos^3\frac{\alpha}{3} - 3\cos\frac{\alpha}{3}$.
  - Za $\alpha = 60°$: $\cos\alpha = \frac{1}{2}$. $4\cos^3\frac{\alpha}{3} - 3\cos\frac{\alpha}{3} - \frac{1}{2} = 0$. Dobimo polimom $4x^3 - 3x = \frac{1}{2} \sim 8x^3 - 6x = 1$, ki je nerazcepen, anhilira $\cos\frac{\alpha}{3}$ in je stopnje $3 \neq 2^k$. Kot $20°$ torej ni konstruktibilen.
  - Za $\alpha = 90°$: $\cos\alpha = 0$. $4\cos^3\frac{\alpha}{3} - 3\cos\frac{\alpha}{3} = 0$. Dobimo polimom $3x^3 - 3x = x\left(4x^2 - 3\right)$, $4x^2 - 3$ je stopnje 2^k.

  Sklep: $\cos\frac{\alpha}{3}$ je konstruktibilno $\Leftrightarrow 4x^3 - 3x - \cos\alpha$ je razcepen nad $\mathbb{Q} \Leftrightarrow$ ima racionalno ničlo.
- Pravilni $n-$kotniki: trikotnik, štirikotnik, petkotnik (s stranico $\deg_{\mathbb{Q}} \sqrt{\frac{5-\sqrt{5}}{2}} = 4 = 2^2$), šestkotnik, osemkotnik so konstruktibilni. Sedemkotnik ni, ker ima stranico z minimalnim polinomom $x^3 + x^2 - 2x - 1$.

Izrek. *Gauss-Wantzel. Pravilni $n-$kotnik je konstruktibilen z ravnilom in šestilom $\Leftrightarrow n = 2^k \cdot$(produkt različnih fermatovih praštevil).*

Definicija. Fermatova števila so oblike $2^{\left(2^k\right)} + 1 =: F_n$. Fermatova praštevila so fermatova števila, ki so praštevila. Prvih nekaj fermatovih števil: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$. F_5 do F_{32} so sestavljena. Za F_{33} in dalje so števila prevelika, da bi lahko preverili, če so sestavljena. Domnevajo, da so vsa nadaljna sestavljena.

Vrnimo se k splošnim razširitvam. Videli smo, da so vse transcendentne razširitve neskončne, enostavne algebraične razširitve pa so končne. Splošne algebraične razširitve so lahko neskončne. O njih govori naslednji izrek:

Izrek. *Velja:*

1. *Vsaka končna razširitev je algebraična.*

   Dokaz. $[F:K] = n$, $x \in F$. Tedaj $1, x, x^2, \ldots, x^n$ so linearno odvisni $\Rightarrow \exists k_1, \ldots, k_n$, ki niso vsi $0 \ni$: $k_0 + k_1 x + k_2 x^2 + \cdots + k_n x^n = 0 \sim x$ je ničla polinoma v K. □

2. *Naj bo $K \leq F$, $A \subseteq F$ algebraični nad F. Potem je $F(A)$ algebraična razširitev K.*

   Dokaz. Vsak element $K(A)$ je za pravilno izbrane $a_i \in A, p, q \in K[x_1, \ldots, x_n]$ oblike

   $$\frac{p(a_1, \ldots, a_n)}{q(a_1, \ldots, a_n)}.$$

   To pomeni, da je $a \in K(a_1, \ldots, a_n)$, ki je končna razširitev K. Po točki 1 je a algebraičen nad K. □

3. *Naj bo F algebraična razširitev K, E algebraična razširitev F. Potem je E algebraična razširitev K.*

   Dokaz. Naj bo $a \in E$. Po privzetku obstaja $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$, za katerega je $p(a) = 0$. To pomeni, da je a algebraičen nad $K(a_0, \ldots, a_1)$, kar je končna algebraična razširitev K. Sledi, da je a algebraičen nad K. □

1.12 Razpadni obseg

Naj bo $K \leq \mathbb{C}$ in $p(x) \in K[x]$. $\{a_1, \ldots, a_n\} \subseteq \mathbb{C}$ so ničle $p(x)$. Velja $K \leq K(a_1, \ldots, a_n) \leq \mathbb{C}$. $p(x)$ v $K(a_1, \ldots, a_n)$ razpade na linearne faktorje — $p(x) = (x - a_1) \cdots (x - a_n)$ in $K(a_1, \ldots, a_n)$ je najmanjša razširitev K s to lastnostjo.

Naj bo sedaj $p(x) \in \mathbb{Z}_p[x]$, specifično $x^2 + x + 1 \in \mathbb{Z}_2[x]$. V tem polinomu nimamo ničel — je nerazcepen. Kaj dodati?

$\left[\mathbb{Z}_2 / \left(x^2 + x + 1\right) : \mathbb{Z}_2\right] = 2$. Označimo $K \coloneqq \mathbb{Z}_2 / \left(x^2 + x + 1\right)$. Velja recimo $[x] = x + \left(x^2 + x + 1\right) \in K$. Naj bo $I \coloneqq \left(x^2 + x + 1\right)$.

$(x + I)^2 + (x + I) + 1 + I = x^2 + I + x + I + 1 + I = \left(x^2 + x + 1\right) + I = 0 + I$. Torej $x^2 + x + 1$ razpade na linearne faktorje v $K \geq \mathbb{Z}_2$. $a \coloneqq x + \left(x^2 + x + 1\right)$, $p(a) = a^2 + a + 1 = 0$. Elementi/predstavniki v K so $0, 1, x, x + 1$.

Ta kolobar ima naslednje tabele operacij:

$\cdot$	0	1	x	$1 + x$
0	0	0	0	0
1		1	x	$1 + x$
x			$x^2 \mod \left(x^2 + x + 1\right) = x + 1$	$x + x^2 \mod x^2 + x + 1 = 1$
$1 + x$	komut			$1 + 2x + x^2 = 1 + x = x \mod x^2 + x + 1$

$+$	0	1	x	$1 + x$
0	0	1	x	$1 + x$
1		0	$1 + x$	x
x			0	1
$1 + x$	komut			0

Kaj pa poljuben obseg in poljuben polinom? Naj bo $p(x) \in K[x]$. Ničle ima lahko v K in izven K. Ločimo dva primera:

- Vse ničle so elementi K: polinom je popolnoma razcepen nad K.
- Obstajajo ničle izven K: ima vsaj en nelinearen nerazcepen faktor. Naj bo $q(x)$ nerazcepen nelinearen faktor $p(x)$. V $K[x] / (q(x)) \geq K$. V tej razširitvi je $x + (q(x))$ ničla od $p(x)$.

  To deljenje $K[x]$ ponavljamo največ $n-$krat (za vsako ničlo). Na koncu dobimo razširitev F za K, ki vsebuje vse ničle $p(x)$. Pravimo, da v F $p(x)$ razpade na linearne faktorje.

Definicija. Razpadni obseg za $p(x) \in K[x]$ (nad K) je minimalna razširitev K, v kateri $p(x)$ razpade na linearne faktorje.

Izrek. *Razpadni obseg $p(x) \in K[x]$ nad K obstaja in je enoličen do izomorfizma ZDB poljubna razpadna obsega sta izomorfna.*

Dokaz. Obstoj smo poprej konstruktivno dokazali, enoličnosti pa ne bomo dokazali. □

Zgled. $x^2 - 2 \in \mathbb{Q}[x]$. Lahko vzamemo enega izmed dveh izomorfnih obsegov:

- $\mathbb{Q}\left(\sqrt{2}\right)$, kjer razpade na $\left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)$
- $\mathbb{Q}[x] / \left(x^2 - 2\right)$, kjer razpade na $(x - a)(x + a)$ za $a \coloneqq x + \left(x^2 - 2\right)$.

Razmišljajmo: Naj bo K končen obseg $\implies \operatorname{char} K$ je končno praštevilo. $K \geq \mathbb{Z}_p$, $n = [K : \mathbb{Z}_p] \Rightarrow K$ ima p^n elementov. $(K^* \coloneqq K \setminus \{0\}, \cdot)$ je grupa s $p^n - 1$ elementi. V vsaki končni grupi velja $\forall a \in G : a^{|G|} = 1$. Torej $\forall a \in K \setminus \{0\} : a^{(p^n - 1)} = 1$. Torej vsak $a \neq 0$ je ničla polinoma $x^{(p^n - 1)} - 1$. Vsi elementi K so ničle polinoma $x\left(x^{(p^n - 1)} - 1\right) = x^{(p^n)} - x \implies x^{p^n} - x = \Pi_{a_i \in K}(x - a_i)$.

Trditev. Če je K končen obseg, je K razpadni obseg polinoma $x^{|K|} - x$ nad $\mathbb{Z}_p$, kjer $p = \operatorname{char} K$.

Zgled. Če ima K 27 elementov, je K razpadni obseg polinoma $x^{27} - x$ nad $\mathbb{Z}_3$.

Trditev. Vzemimo p^n za p praštevilo in $n \in \mathbb{N}$. Naj bo $K \coloneqq$ minimalno velik razpadni obseg $x^{p^n} - x$ nad $\mathbb{Z}_p$. Naj bo $K' \subseteq K \ni$: $K' =$ (množica ničel $x^{p^n} - x$). Tedaj velja K' je obseg in $|K'| = p^n$.

Dokaz. Dokazujemo več stvari:

- $x^{p^n} - x$ nima večkratnih ničel: Če ima polinom $p(x)$ večkratne ničle, so te ničle skupne s $p'(x)$ (odvodom). Večkratne ničle nima, ker $\left(x^{(p^n)} - x\right)' = p^n x^{p^n - 1} - 1 \equiv 1 \mod p$ (konstanten polinom nima ničel). Torej ima K' p^n elementov.
- K' je zaprta za $+, -, \cdot, \div$ (je obseg): Vzemimo $a, b \in K'$ (velja, da $a^{p^n} = a$ in $b^{p^n} = b$).

$$ab = a^{p^n} b^{p^n} = (ab)^{p^n}$$

$$\frac{a}{b} = \frac{a^{p^n}}{b^{p^n}} = \left(\frac{a}{b}\right)^{p^n}$$

$$(a+b)^{p^n} = a^{p^n} + \binom{p^n}{1} a^{p^n - 1} b + \cdots + \binom{p^n}{p^n - 1} a b^{p^n - 1} + b^{p^n} = a^{p^n} + 0 + b^{p^n} = a^{p^n} + b^{p^n},$$

ker so vsi srednji koeficienti deljivi s p in zato v $\mod p = 0$. Podobno za

$$(a-b)^{p^n} = a^{p^n} - b^{p^n}.$$

□

Izrek. *$\forall p \in P, n \in \mathbb{N} \exists$ do izomorfizma natanko določen obseg, ki ima p^n elementov. Standardno ga označimo $GF(p^n)$. Dobimo ga kot razpadni obseg polinoma $x^{p^n} - x$ nad $\mathbb{Z}_p$.*

Zgled. Za opis $GF(p^n)$ je dovolj, če najdemo nerazcepni polinom $p(x)$ stopnje n nad $\mathbb{Z}_p$ (taki vselej obstajajo — ne bomo dokazali). Potem je $GF(p^n)$ izomorfen $\mathbb{Z}_p[x] / (p(x))$.

- $GF(4) = \mathbb{Z}_2[x] / \left(x^2 + x + 1\right)$
- $GF(27) = \mathbb{Z}_3[x] / \left(x^3 + 2x + 1\right)$

Za K končen kolobar brez deliteljev niča velja $K \cong GF(|K|)$.

2 Topologija

2.1 Uvod

Zvezna deformacija. Najprej si oglejmo zveznost funkcije $f : \mathbb{R} \to \mathbb{R}$.

Definicija. f zvezna v $x \Leftrightarrow \forall \varepsilon > 0 \exists \delta > 0 \ni: \forall a \in \mathbb{R} : |x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon$
Alternativno: f zvezna v $x \Leftrightarrow \forall (x_n)_{n \in \mathbb{N}} : \lim_{n \to \infty} x_n = x \Rightarrow \lim_{n \to \infty} f(x_n) = f(x)$.

Kaj pa zveznost na več dimenzijah, recimo $f : (x, y) \mapsto \left(x + y, x - y, x^2\right)$? Vzemimo splošno $f : X \to Y$. Definirajmo razdaljo/metriko na X in Y.

Definicija. Matrika na X je funkcije $d : X \times X \mapsto [0, \infty)$, da velja:

- simetričnost: $d(x, y) = 0 \Leftrightarrow x = y$
- definitnost: $d(x, y) = d(y, x)$
- trikotniška neenakost: $d(x, y) + d(y, z) \geq d(x, z)$

Zgled. Nekaj primerov:

- $\mathbb{R}$: $d(x, y) = |y, x|$
- $\mathbb{R}^2$:
  - Evklidska: $d_2((x_1, y_1), (x_2, y_2)) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$
  - Mahnattanska/newyorška: $d_1((x_1, y_1), (x_2, y_2)) = |x_2 - x_1| + |y_2 - y_1|$
  - $d_\infty((x_1, y_1), (x_2, y_2)) = \max\{|x_2 - x_1|, |y_2 - y_1|\}$

- Za poljubno množico X: $d_{\text{diskretna}}(x,y) = \begin{cases} 0 & ; x = y \\ 1 & ; x \neq y \end{cases}$

Definicija. Naj bo $f : (X, d_x) \to (Y, d_y)$ (množici smo opremili z metrikama). f je zvezna na $x \in X \Leftrightarrow \forall \varepsilon > 0 \exists \delta > 0 \forall a \in X : d_x(x,a) < \delta \Rightarrow d_y(f(x), f(a)) < \varepsilon$.

Definicija. $U \subseteq \mathbb{R}^2$ je odprta $\Leftrightarrow \forall x \in U \exists \varepsilon > 0 \ni$: $K(x,\varepsilon) \subseteq U$.

Definicija. Naj bo $A \subseteq \mathbb{R}^n$.

- $x \in \mathbb{R}^n$ je notranja za A, če $\exists \varepsilon > 0 \ni$: $K(x,\varepsilon) \subseteq A$
- $x \in \mathbb{R}^n$ je zunanja za A, če $\exists \varepsilon > 0 \ni$: $K(x,\varepsilon) \cap A = \emptyset$
- $x \in \mathbb{R}^n$ je mejna, če ni niti notranja niti zunanja ZDB $\forall \varepsilon > 0 : K(x,\varepsilon)$ seka A in A^C.
- Alternativna definicija odprtosti: A je odprta, če so vse njene točke notranje.

Definicija. Alternativna definicija zveznosti: f je zvezna $\Leftrightarrow$ praslika vsake odprte množice je odprta ZDB $U \subseteq Y$ odprta $\Rightarrow f^*(U) \subseteq X$ odprta.

2.2 Topološka struktura

Definicija. Naj bo X poljubna množica. Topološka struktura, krajše topologija, je podana z družino podmnožic $T \subseteq 2^X$, ki jim pravimo odprte množice in ki zadoščajo pogojem:

- poljubna unija elementov T je element T (implicira $\emptyset \in T$ — prazna unija)
- končen presek elementov T je element T (implicira $X \in T$ — prazen presek)

$A \subseteq X$ je zaprta, če je A^C odprta. Zaprte množice: $Z \coloneqq \{A \subseteq X; A^C \in T\}$. Za družino zaprtih množic velja:

- poljuben presek zaprtih množic je zaprt (implicira X je zaprta — prazen presek)
- končna unija zaprtih množic je zaprta (implicira $\emptyset$ je zaprta — prazna unija)

Zgled. Nekaj primerov:

- Odprte množice v $\mathbb{R}^n$ ustrezajo definiciji topologije
- $\{\emptyset, X\}$ je najmanjša možna topologija na X. Pravimo ji trivialna topologija.
- 2^x je največja možna topologija na X. Pravimo ji diskretna topologija.
- topologija, porojena z metriko $T_d = \{U \subseteq X;$ vse točke U so notranje glede na $d\}$
- najmanjša topologija, v kateri so točke zaprte $\Rightarrow$ končne množice so zaprte. $\{$končne podmnožice $X\} \cup \{X\}$ ustreza pogojem za družino zaprtih množic: $T_{kk} \coloneqq \{U \subseteq X; X - U$ končna$\} \cup \{\emptyset\}$ je topologija končnih komplementov. Če je X končna, je $T_{kk} = T_{\text{disk}}$. Če je X neskončna, je to druga, nova topologija.
- $d \to T_d$. Različne metrike lahko porodijo isto topologijo. Metrike d_1, d_2 in d_3 so topološko ekvivalentne. Krogle d_1 so rombaste, krogle d_2 so okrogle, krogle d_3 so kvadratne, pa vendar za poljubni metriki $e, f \in \{d_1, d_2, d_3\}$ velja, da $\forall x \in \mathbb{R}^2 \forall \varepsilon > 0 \exists \delta > 0 \ni$: $K_e(x,\delta) \subseteq K_f(x,\varepsilon)$.
- $T_{\text{diskr}} = 2^X$ je porojena z diskretno metriko. Majhne okolice so singletoni in unija singletonov je poljubna končna podmnožica.
- d_2 na $\mathbb{N}$ — $(\mathbb{N}, T_{d_2})$ je spet diskretna topologija, akoravno so razdalje tudi drugačne od $\{0,1\}$.
- Na $\mathbb{R}^2$ je T_{disk} strogo finejša od T_{d_2}, vsaka odprta množica v T_{d_2} je odprta množica v T_{disk}, vendar pa obstaja odprta množica v T_{disk}, ki ni odprta množica v T_{d_2}.

Vprašanje. *Ali je vsaka topologija porojena z neko metriko? Npr. ali je T_{kk} porojena z neko metriko? No, če je X končna, je T_{kk} porojena z diskretno metriko. Toda kaj če X ni končna?*

Naj bosta U in V poljubni odprti in $U \neq X \neq V \wedge U \neq V$. Trdimo, da se U in V iz topologije končnih komplementov vedno sekata. Intuitivno so namreč komplementi zaprtih (ki so pač le končne množice in X) zelo veliki. $(U \cap V)^C = U^C \cup V^C$ je končna $\Rightarrow U \cap V \neq \emptyset$.

Torej poljubni neprazni odprti množici imata neprazen presek. To pa se nikoli ne zgodi v topologiji, ki je porojena z metriko, kajti tam so namreč odprte množice, ki vsebujejo različne točke, lahko disjunktne – torej vedno lahko najdemo disjunktni odprti množici v neskončno veliki množici Z na topologiji, porojeni z metriko. Vzemimo točki x in y v (X', T_d), da $x \neq y$. Označimo $\delta \coloneqq d(x,y)$. Odprti množici $A \coloneqq X' \cap K\left(x, \frac{\delta}{3}\right)$ in $B \coloneqq X' \cap K\left(y, \frac{\delta}{3}\right)$ sta različni po trikotniški neenakosti — ako bi obstajal $z \in A \cap B$, bi veljalo $\left(d(x,z) \leq \frac{\delta}{3}\right) + \left(d(y,z) \leq \frac{\delta}{3}\right) \leq \frac{2\delta}{3} < (d(x,y) = \delta)$.

Definicija. Naj bo $(X,T), A \subseteq X$. Unija vseh elementov T, ki so vsebovani v A, je največji element T, ki je vsebovan v A. Pravimo mu notranjost A — $\operatorname{Int} A$ (interior).

Presek vseh zaprtih množic, ki vsebujejo A, je zaprt in najmanjša zaprta množica, ki vsebuje A. Pravimo ji zaprtje A — $\operatorname{Cl} A$ (closure) — označimo $\overline{A}$.

Meja $A \coloneqq \operatorname{Fr} A = \operatorname{Cl} A \setminus \operatorname{Int} A$ (frontier).

Zgled. $\operatorname{Cl}(A \cup B) \supseteq \operatorname{Cl}(A) \cup \operatorname{Cl}(B)$. Kaj pa $\subseteq$?

Velja $A \subseteq \operatorname{Cl}(A) \cup \operatorname{Cl}(B)$ in $B \subseteq \operatorname{Cl}(A) \cup \operatorname{Cl}(B)$, torej $A \cup B \subseteq \operatorname{Cl}(A) \cup \operatorname{Cl}(B)$ (zaprta množica, ki vsebuje A in B), toda $\operatorname{Cl}(A \cup B)$ je **najmanjša** zaprta množica, ki vsebuje $A \cup B \Longrightarrow A \cup B \subseteq \operatorname{Cl}(A \cup B) \subseteq \operatorname{Cl}(A) \cup \operatorname{Cl}(B) \Longrightarrow \operatorname{Cl}(A \cup B) = \operatorname{Cl}(A) \cup \operatorname{Cl}(B)$.

Kaj pa $\operatorname{Cl}(A \cap B) \subseteq \operatorname{Cl}(A) \cap \operatorname{Cl}(B)$? To velja. Kaj pa $\subseteq$? Ne velja, recimo $A = (0,1)$ in $B = (1,2)$: $\emptyset \neq \{1\}$.

2.3 Zveznost

Definicija. Naj bo $f : X \to Y$. $f_*(A) \coloneqq \{f(a) \in Y; a \in A\}$ je slika množice A s funkcijo f, $f^*(A) \coloneqq \{a \in X; f(a) \in A\}$ pa praslika množice A s funkcijo f.

Definicija. Naj bo $f : (X, T_X) \to (Y, T_Y)$ je zvezna, če je $\forall V \in T_Y : f^*(V) \in T_X$ ZDB če je praslika vsake odprte množice odprta ZDB če so praslike elementov T_Y elementi T_X.

Trditev. Kompozitum zveznih funkcij je zvezen.

Dokaz. Naj bo $f : (X, T_X) \to (Y, T_Y)$ zvezna, $g : (Y, T_Y) \to (Z, T_Z)$ zvezna. $g \circ f$ je zvezna, kajti $\forall w \in T_Z : g^*(w) \in T_Y \wedge f^*(g^*(w)) \in T_X \sim (g \circ f)^*(w) \in T_X$. □

Zgled. Naj bo $(X, d_X), (Y, d_Y)$ (npr. na $\mathbb{R}$ vzamemo $d(x,y) = |x - y|$).

- $f : X \to Y$, ki je zvezna glede na metriki d_X in d_Y, je zvezna tudi glede na porojeni topologiji T_{d_X} in T_{d_Y}.
- $f : (X, T_{\text{disk}}) \to (Y, T_{\text{katerakoli}})$ je vedno zvezna — vsak f iz diskretne topologije je vedno zvezen.
- $g : (X, T_{\text{katerakoli}}) \to (Y, T_{\text{triv}})$ je vedno zvezna — vsak g v trivialno topologijo je vedno zvezen.
- $id : (X, T) \to (X, T')$ je zvezna $\Leftrightarrow T' \subseteq T$, kajti $id^*(A) = A$.
- Intuicija za zveznost: „topologija je močnejša na domeni“
- Konstantna funkcija $c : (X, T_X) \to (Y, T_Y)$ ki slika $x \mapsto y_0$ je zvezna.

  Dokaz. $(\text{konst } y_0)^*(V \in T_Y) = \begin{cases} X & ; x_0 \in V \\ \emptyset & ; x_0 \notin V \end{cases}$ □

- Za $f : (\mathbb{R}, T_{kk}) \to (\mathbb{R}, T_{d_1})$ so edine zvezne funkcije konstante.

Izrek. *NTSE*

1. *$f : (X, T_X) \to (Y, T_Y)$ je zvezna (praslika vsake odprte množice je odprta)*
2. *praslika vsake zaprte množice je zaprta*

3. $\forall A \subseteq X : f_* \left(\overline{A}\right) \subseteq \overline{f_* (A)}$

Dokaz. Dokazujemo ekvivalenco

(1) $\Rightarrow$ (2) $\forall B : \overset{\text{komplement}}{Y \setminus B} \overset{\text{odprta}}{\in T_Y} \Rightarrow f^* (Y \setminus B) = X \setminus F^* (B) \in T_X$

(2) $\Rightarrow$ (1) Podobno.

(1) $\Leftrightarrow$ (3) Za $f : X \to Y$ in $A \subseteq X$ in $B \subseteq Y$ velja $f^* (f_* (A)) \supseteq A$ (enakost za injekcijo) in $f_* (f^* (B)) \subseteq B$ (enakost za surjekcijo)

($\Rightarrow$) Velja $f_* (A) \subseteq \overline{f_* (A)}$ in $A \subseteq f^* (f_* (A)) \subseteq f^* \left(\overline{f_* (A)}\right)$, ki je zaprta, ker je praslika zaprte po predpostavki, in $A \subseteq \overline{A} \subseteq f^* \left(\overline{f_* (A)}\right)$. Nadalje $f^* \left(\overline{A}\right) \subseteq f_* \left(f^* \left(\overline{f_* (A)}\right)\right) \subseteq \overline{f_* (A)} \Longrightarrow f_* \left(\overline{A}\right) \subseteq \overline{f_* (A)}$.

($\Leftarrow$) Vzemimo $B^{\text{zap.}} \subseteq Y$, ZDB $B = \overline{B}$. Trdimo, da $f^*(B)$ je zaprta. Velja $f_* \left(\overline{f^* (B)}\right) \overset{(3)}{\subseteq} \overline{f_* (f^* (B))} \subseteq \overline{B} = B$. Nadalje $\overline{f^* (B)} \subseteq f^* \left(f_* \left(\overline{f^* (B)}\right)\right) \subseteq f^* (B)$. Ker vselej velja $Z \subseteq \overline{Z}$, sledi $\overline{f^* (B)} = f^* (B)$, torej je $f^* (B)$ zaprta.

□

Opomba. Iz analize vemo, da, če za vsako točko x velja, da za vsako zaporedje, ki konvergira k x, velja, da s f preslikani členi konvergirajo k $f(x)$, je f zvezna. To je analog točke (3) zgornjega izreka.

2.4 Izomorfizem topologij

Definicija. $f : (X, T_X) \to (Y, T_Y)$ je homeomorfizem, če je bijekcija in inducira bijekciji med T_X in T_Y (inducirani bijekciji sta f^* in f_*).

Trditev. $f : (X, T_X) \to (Y, T_Y)$ je homeomorfizem $\Leftrightarrow$ f zvezna bijekcija in f^{-1} zvezna.

Dokaz. Očitno? □

Definicija. $(X, T_X) \approx (Y, T_Y)$ pomeni, da sta topološka prostora homeomorfna. Pišemo tudi $X \approx Y$. Je ekvivalenčna relacija.

Zgled. Primeri standardnih homeomorfizmov:

- $[a, b] \approx [c, d]$ za $a < b$ in $c < d$. Dovolj je dokazati, da $[0, 1] \overset{f}{\approx} [a, b]$, ker je $\approx$ ekvivalenčna. Ustrezen f je $x \mapsto a + (b - a) \cdot x$. Kadar takole ne specificiramo topologije, običajno impliciramo evklidsko. Ista f deluje za odprte in polodprte intervale, torej $[0, 1) \approx (0, 1] \approx [a, b)$.
- $(-\infty, \infty) \sim \left(\frac{-\pi}{2}, \frac{\pi}{2}\right)$ — $f = \arctan$. Vsi neprazni odprti intervali so si medsebojno homeomorfni.
- $[a, b] \not\approx (a, b) \not\approx (a, b] \not\approx [a, b]$.

2.5 Topološka lastnost

Definicija. Lastnost L je topološka, če se ohranja preko homeomorfizma: Če je $X \approx Y$ velja $L(X) \Leftrightarrow L(Y)$ ZDB $X \approx Y \Longrightarrow L(X) \Leftrightarrow L(Y)$.

Zgled. Kompaktnost in kardinalnost sta topološki lastnosti, omejenost pa ni.

Kadar ugotavljamo, da dva prostora nista homeomorfna, iščemo topološko lastnost, ki jima ni skupna.

2.6 Standardni homeomofizmi $\mathbb{R}^n \to \mathbb{R}^n$

- $$f(\vec{x}) = \frac{\vec{x}}{1+|\vec{x}|}$$

  je homeomorfizem, ki skrši prostor na kroglo $B^n \coloneqq K\left(\vec{0},1\right) = \{x^n \in \mathbb{R}^n; |\vec{x}| < 1\}$.

Definicija. Nekaj oznak: $B^n \coloneqq K\left(\vec{0},1\right) = \{x^n \in \mathbb{R}^n; |\vec{x}| < 1\}$, $\overline{B^n} \coloneqq \{x^n \in \mathbb{R}^n; |\vec{x}| \leq 1\}$, $S^{n-1} \coloneqq \{x^n \in \mathbb{R}^n; |\vec{x}| = 1\}$
Zakaj $n-1$? Ker je sfera manj dimenzijska od pripadajočega kroga — S^1 je krožnica v $\mathbb{R}^2$, S^2 je sfera v $\mathbb{R}^3$, $\{-1,1\} = S^0$ v $\mathbb{R}$.

Trditev. $S^1 \setminus \{(0,1)\} \approx \mathbb{R}$.

Dokaz. Ustrezen homeomorfizem, ki točko na krožnici preslika na $x-$os, je $f : S^1 \setminus \{(0,1)\} \to \mathbb{R}$ s predpisom $(x,y) \mapsto \frac{x}{1-y}$ in inverzom $\left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right) \hookleftarrow t$. □

Velja celo splošneje: $\mathbb{R}^{n+1} \supseteq S^n \setminus \left\{\left(\overset{n-\text{ničel}}{0,\ldots,0,,1}\right)\right\} \approx \mathbb{R}^n$ s homeomorfizmom $f : \mathbb{R}^n \times \mathbb{R} \mapsto \mathbb{R}^n$ s predpisom $(\vec{x},y) \mapsto \frac{\vec{x}}{1-y}$ in inverzom $\left(\frac{2\vec{x}}{|\vec{x}|^2+1}, \frac{|x^2|-1}{|x^2|+1}\right) \hookleftarrow \vec{x}$.

2.7 Kompaktnost

Definicija. Naj bo (X,T) topologija. $U \subseteq T$ je odprto pokritje $A \subseteq X$, če je unija elementov U cel A. Podpokritje U je $U' \subseteq U$, ki je tudi pokritje.

Definicija. $A \subseteq X$ je kompaktna, če **za vsako** odprto pokritje A obstaja končno podpokritje.

Pomembno! Seveda ni dovolj, da obstaja odprto pokritje A, ki je končno — to namreč vedno obstaja, odprta množica $X \in T$. Da je $A \subseteq X$ kompaktna, mora **poljubno** pokritje A vsebovati končno pokritje A. Nujno je treba tudi upoštevati, da so pokritja lahko samo iz odprtih množic.

Zgled. Primeri

- Vsaka končna množica je kompaktna.
- V metričnem prostoru je vsaka kompaktna množica omejena: $X = K(x_0,1) \cup K(x_0,2) \cup \cdots$ — kompaktnost pomeni, da je X pokrit že z nekim končnim naborom krogel.
- $(0,1)$ ni kompakten — $\left\{\left(\frac{1}{n},1\right); n = 2,3,4,\ldots\right\}$ nima končnega podpokritja.

  Alternativno: Kompaktnost je topološka lastnost in $(0,1) \approx \mathbb{R}$, ki je neomejen in zato ni kompakten. Podobno tudi $[0,\infty) \approx [0,1)$ ni kompakten.
- Naj velja $\lim_{n\to\infty} x_i = x$. Tedaj $\{x; i \in \mathbb{N}\} \cup \{x\}$ je kompaktna.
- $\mathbb{R}$ ni kompakten. Pokritje z intervali $\{(i,i+2); \forall i \in \mathbb{Z}\}$ nima končnega podpokritja.

Trditev. V metričnem prostoru je vsaka kompaktna množica omejena.

Dokaz. $K(x,1) \subseteq K(x,2) \subseteq \cdots$ so odprte množice, ki pokrivajo A za $x \in A$. Če je A kompakten, je vsebovan v največji iz tega končnega podpokritja in zato omejen. □

Trditev. V metričnem prostoru je vsaka kompaktna množica zaprta.

Dokaz. Naj bo A kompaktna. Vzemimo poljubno $x \notin A$ ($x \in A^C$). Velja, da je $\left\{K\left(a, \frac{d(a,x)}{2}\right); \forall a \in A\right\}$ odprto pokritje A. Obstajajo $K\left(a_1, \frac{d(a_1,x)}{2}\right), \ldots, K\left(a_n, \frac{d(a_n,x)}{2}\right)$, ki tvorijo končno odprto pokritje (ker je A kompaktna). Vzemimo $r \coloneqq \min_{i\in[n]}\left\{\frac{d(a_i,x)}{2}\right\}$. Zanj velja $K(x,r)$ ne seka A. Ker je $x \in A$ bil poljuben, je A^C odprta $\Rightarrow A$ zaprta. □

Pripomba. Torej je v metričnem prostoru vsaka kompaktna množica zaprta in omejena. V $\mathbb{R}^n$ velja celo ekvivalenca.

Izrek. *$[a,b]$ je kompakten.*

Dokaz. Naj bo U odprto pokritje $[a,b]$, sestavljeno iz samih odprtih intervalov. Naj bo $c \coloneqq \sup\{x \in [a,b]\,;\, [a,x] \text{ je pokrit s končn}$

Dokažimo, da je $[a,c]$ končno pokritje z elementi U. Ker je c pokrit z odprto množico v U, ta množica vsebuje še nek $x \in [a,c)$. Torej $[a,c]$ ima končno pokritje z elementi U.

Dokažimo, da je $c = b$. Če bi c ne bil b, bi imeli nek $q > c \ni$: $[a,q]$ ima končno pokritje, saj je c pokrit z neko odprto množico iz U, kar bi bilo v protislovju z definicijo c (supremum). ZDB $q > c \wedge [a,q]$ ima končno pokritje v $U \rightarrow\!\!\!\!\leftarrow c$ je supremum množice $[a,x]$, ki so pokriti s končno mnogo elementi U. □

Trditev. Zaprta podmnožica kompakta je kompakt.

Dokaz. Dokazujemo $A^{\text{zap.}} \subseteq X^{\text{kompakt}} \Rightarrow A$ kompakt. Vzemimo odprto pokritje U za A. $U \cup \{X \setminus A\}^{\text{odp.}}$ je odprto pokritje za X. Ker je X kompaktna, obstaja končno podpokritje. Prav to, če izvzamemo $\{X \setminus A\}$, pa je končno podpokritje U za A. □

Posledica. *$A \subseteq \mathbb{R}$ je kompaktna $\Leftrightarrow$ A zaprta in A omejena.*

Dokaz. Dokazujemo ekvivalenco. □

($\Rightarrow$) Dokazano že poprej.

($\Leftarrow$) A omejena $\Rightarrow$ vsebovana v $[a,b]^{\text{komp.}}$, torej je A zaprta podmnožica kompakta $[a,b]$ in s tem tudi sama kompaktna.

Izrek. *X, Y kompaktni $\Rightarrow X \times Y$ kompaktna.*

Definicija. Produktna topologija. Imejmo (X, T_X) in (Y, T_Y). Topologija na $X \times Y$ naj vsebuje vse možne unije produkov odprtih množic (škatlastih odprtih množic) iz X in Y.

Definicija je dobra, ker je produktna topologija res topologija, saj je zaprta za končne preseke. Induktiven dokaz:

$$\left(\bigcup_{\lambda} U_\lambda \times V_\lambda\right) \cap \left(\bigcup_{\mu} U_\mu \times V_\mu\right) = \bigcup_{\lambda,\mu} \left(\overset{\text{škatlasta odprta množica}}{(U_\lambda \times V_\lambda) \cap (U_\mu \times V_\mu)}\right)$$

Dejstvo. *Naj bo $f : Z \to X \times Y$. Označimo $f = (f_1, f_2)$. Tedaj velja f zvezna $\Leftrightarrow$ f_1, f_2 zvezni.*

Dokaz. Dokaz izreka. Naj bosta X, Y kompaktni. Naj bo U odprto pokritje za $X \times Y$ s škatlami. Za poljuben $x \in X$ si oglejmo $\{x\} \times Y$. Ta je kompakten in pokrit z U. Zanj obstaja končno podpokritje U: $U_1 \times V_1, \ldots, U_n \times V_n$ in sekajo $\{x\} \times Y$. Velja $U_x \coloneqq U_1 \cup \cdots \cup U_n$ je odprta množica.

$\{U_x; x \in X\}$ je odprto pokritje za $X \Rightarrow \exists$ končno podpokritje $U_{x_1}, \ldots, U_{x_m}$ za X. $U_{x_i} \times Y$ ima končno podpokritje, torej ima $X \times Y$ končno podpokritje. NE RAZUMEM. □

Pripomba. Posplošitev tega izreka je izrek Tihonova: poljuben (poljubne kardinalnosti) produkt kompaktov je kompakt.

Vprašanje. *Zakaj je produktna topologija ista kot naravna topologija $\mathbb{R} \times \mathbb{R}$?*

Zgled. Naj bo (X, T_X) določen z metriko d_X in (Y, T_Y) določen z metriko d_Y. Velja $d_{X\times Y}((x,y),(x',y')) = \max\{d_X(x,x'), d_Y(y,y')\}$ in za $X = Y = \mathbb{R}$ bi bili $d_X = d_Y$ evklidski metriki in $d_{X\times Y}$ bi bila ravno metrika d_3, ki porodi naravno topologijo.

Izrek. *Heine–Borel-Lebesgue. $A \subseteq \mathbb{R}^n$ kompaktna $\Leftrightarrow$ A zaprta $\wedge A$ omejena.*

Dokaz. Dokazujemo ekvivalenco.

($\Rightarrow$) $\mathbb{R}^n$ metričen $\Rightarrow$ kompakti so v metričnem prostoru zaprti in omejeni

($\Leftarrow$) A omejena $\Rightarrow$ je vsebovana v dovolj velikem kompaktnem kvadru $[a_1, b_1] \times \cdots \times [a_n, b_n]$. Ker je A poleg tega, da je vsebovana v kompaktu, še zaprta, je kompaktna.

□

Izrek. *Bolzano-Weierstrass. Vsako omejeno zaporedje v $\mathbb{R}$ ima konvergentno podzaporedje.*

Lema. *V kompaktnem prostoru ima vsaka neskončna množica stekališče.*

Dokaz. Dokaz leme. Naj bo A brez stekališča v kompaktnem X. Tedaj $\forall x \in X \exists$ okolica U_x, ki vsebuje le končno elementov A. $\{U_X, x \in X\}$ ima končno podpokritje, ker je X kompaktna. Vsak element iz tega končnega podpokritja vsebuje le končno elementov A, unija vseh pa vsebuje vse elemente A, torej je A tudi sam končen $\rightarrow\!\leftarrow$ — to je v protislovju s predpostavko, da je A neskončen. □

Dokaz. Dokaz izreka. Ker je $(x_n)_{n\in\mathbb{N}}$ omejeno, leži v nekem kompaktu. Ločimo dva primera:

- $\{x_n; n \in \mathbb{N}\}$ je končna: Vsaj en x_i se pojavi neskončnokrat. To je stekališče in tudi podzaporedje samo s tem elementom konvergiral.
- $\{x_n; n \in \mathbb{N}\}$ je neskončna. Po lemi ima stekališče. Stekališče je limita podzaporedja.

□

Trditev. Naj bo $f : X \to Y$ zvezna, $A \subseteq X$ kompaktna. Tedaj velja $f_*(A)$ je kompaktna. ZDB zvezna funkcija kompakte slika v kompakte.

Dokaz. Naj bo U odprto pokritje za $f_*(A)$. Naj bo $\{f^*(P); P \subseteq U\}$ odprto pokritje za A. Potemtakem, ker je A kompaktna, obstaja odprto podpokritje za A: $f^*(V_1), \ldots, f^*(V_n)$ in sledi, da je $V_1, \ldots, V_n$ odprto podpokritje za $F_*(A)$. NE RAZUMEM, nekako je treba uporabiti zveznost. □

Posledica. *Če je zvezna $f : X^{komp.} \to \mathbb{R}$, potem f zavzame* min *in* max *— torej ni le omejena, temveč tudi doseže* inf *in* sup.

Dokaz. $f_*(X)$ je kompaktna $\subseteq \mathbb{R} \Longrightarrow f_*(X)$ je zaprta in omejena $\Longrightarrow f_*(X)$ ima inf in sup in ker je zaprta, ju doseže. □

Izrek. *Cantorjev izrek/princip sendviča. Naj bo $F_1 \supseteq F_2 \supseteq F_3 \supseteq \cdots$ padajoče zaporedje zaprtih nepraznih podprostorov v kompaktnem X. Tedaj je $\bigcap F_n \neq \emptyset$. Dodatno, če je X metričen in je $\lim_{i\to\infty} \operatorname{diam} F_i = 0$, je v preseku natano ena točka (ZDB za $\mathbb{R}$: $[a_1, b_1] \supseteq [a_2, b_2] \supseteq \cdots$ in če $\lim_{i\to\infty}(b_i - a_i) = 0 \Longrightarrow$ v preseku je natanko ena točka).*

Definicija. Naj bo (X, d) metričen in $A \subseteq X$. Premer množice A je $\operatorname{diam} A := \sup_{a,a' \in A} d(a, a')$.

Dokaz. PDDRAA $F_1 \supseteq F_2 \supseteq F_3 \supseteq \cdots \ni: \bigcap_i F_i = \emptyset$ in $\forall i : F_i$ zaprta in neprazna. Tedaj si oglejmo $X \setminus F_1 \subseteq X \setminus F_2 \subseteq X \setminus F_3 \subseteq \cdots$ (naraščajoče zaporedje odprtih množic). Velja $\cup_i (X \setminus F_i) = X$ (po predpostavki, da je presek F_i prazen). To je odprto pokritje X. A ker je X kompakten, obstaja končno podpokritje $X \setminus F_1 \cup X \setminus F_2 \cup \cdots \cup X \setminus F_n = X$. Zaradi vsebovanosti sledi, da je $X \setminus F_n = X$, torej $F_n = \emptyset$, kar je v protislovju s predpostavko, da $\forall i : F_i \neq \emptyset$. □

2.8 Povezanost

Definicija. Prostor X je **nepovezan**, kadar ga lahko razcepimo na **disjunktno** unijo dveh **nepraznih odprtih** podmnožic ZDB kadar $\exists A, B \ni: X = A \cup B \wedge A, B$ odprti, neprazni, disjunktni. Prostor X je povezan, kadar ni nepovezan.

Zgled. Nekaj primerov:

- X s trivialno topologijo je povezan.
- X z eno samo točko je povezan.
- $\mathbb{Q}$ z evklidsko topologijo je nepovezan, npr. $\mathbb{Q} = \left(-\infty, \sqrt{2}\right) \cup \left(\sqrt{2}, \infty\right)$.

Trditev. NTSE

1. X povezan.
2. X ne moremo zapisati kot disjunktno unijo dveh nepraznih zaprtih množic
3. $\emptyset$ in X sta edini odprto-zaprti množici.
4. $\nexists$ zvezna surjekcija $f : X \to \{0, 1\}$.

Dokaz. Ker $X = A \oplus B$ za A, B disjunktni neprazni odprti množici, velja $A^C = B$ in $B^C = A$, torej sta A in B tudi obe zaprti. Če takih ni, ni razcepov, s čimer dokažemo, da so medsebojno ekvivalentne trditve 1, 2 in 3.

Dokaz trditve 4: Če imamo razcep $X = A \oplus B$ za A, B disjunktni neprazni odprti množici, najdemo zvezno surjekcijo $f : X \to \{0,1\}$ takole: $f(x) = \begin{cases} 0 & ; x \in A \\ 1 & ; \text{sicer } (x \in B) \end{cases}$. Da lahko govorimo o zveznosti funkcije v $\{0,1\}$, to množico implicitno oplemenitimo z metriko $d(a,b) = \begin{cases} 0 & ; a = b \\ 1 & ; a \neq b \end{cases}$. Obratno, če obstaja taka zvezna surjekcija $f : X \to \{0,1\}$, pa je ustrezen razcep $f^*(0), f^*(1)$. □

Izrek. *Povezane podmnožice $\mathbb{R}$ so natanko intervali.*

Dokaz. Dokazujemo ekvivalenco $A \subseteq \mathbb{R}$ povezana $\Leftrightarrow$ A interval.

($\Rightarrow$) PDDRAA $A \subseteq \mathbb{R}$ ni interval $\iff \exists a < b \leq c \ni: a, c \in A \wedge b \notin A \implies (-\infty, b) \cap A, (b, \infty) \cap A$ je netrivialni odprt razcep $\implies A$ ni povezana.

($\Leftarrow$) Naj bo I interval. PDDRAA ni povezan $\implies \exists$ zaprt razcep $I = A \oplus B$ za A, B zaprti neprazni disjunktni. Vzemimo $a \in A, b \in B$. BSŠ $a < b$. Naj bo $c \coloneqq \sup\{x; [a,x] \in A\}$. Ker A zaprta $\Rightarrow c \in A$. Ker A odprta $\Rightarrow \exists \varepsilon > 0 \ni: [c, c+\varepsilon] \subseteq A \Rightarrow \left[a, c + \frac{\varepsilon}{2}\right] \subseteq A$. To je v $\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow$ z definicijo c (sup).

□

Trditev. $[a,b) \not\approx (a,b)$

Dokaz. PDDRAA $\exists$ homeomorfizem $f : [0,1) \to (0,1) \implies f|_{(0,1)} : (0,1) \mapsto (0,1) \setminus \{f(0)\}$ je tudi homeomorfizem $\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow$, ker bi to bil homeomorfizem med povezanim in nepovezanih prostorom. □

Trditev. Zvezna slike povezane množice je povezana.

Dokaz. Naj bo $f : X^{\text{pov.}} \to Y$ zvezna surjekcija. Dokažimo, da Y povezana. PDDRAA Y ni povezana. Tedaj bi obstajala zvezna surjekcija v $\{0,1\}$. Recimo ji g. Tedaj bi bil $g \circ f$ zvezna surjekcija iz X v $\{0,1\}$, kar je v $\rightarrow\!\!\!\!\!\!\times\!\!\!\!\!\!\leftarrow$ z dejstvom, da je X povezana. □

Dejstvo. *X_λ povezane $\wedge \bigcap_\lambda X_\lambda \neq 0 \implies \bigcup_\lambda X_\lambda$ povezana.*

Dejstvo. *X, Y povezani $\implies X \times Y$ povezana.*

Trditev. A povezana $\wedge A \subseteq B \subseteq \overline{A} \implies B$ povezana.

Dokaz. Naj bo $f : B \to \{0,1\}$ zvezna. Trdimo, da f ni surjekcija. Ker A povezana, $f|_A : A \to \{0,1\}$ ni surjekcija. Denimo, da $f_*(A) = 0$. Tedaj, ker f zvezna, $f\left(\overline{A}\right) \subseteq \overline{f(A)} = \{0\} \implies f$ ni surjekcija. □

Definicija. X je povezan s potmi, če za poljubni $x_0, x_1 \in X$ obstaja pot — zvezna $f : [0,1] \to X$ in $f(0) = x_0 \wedge f(1) = x_1$.

Trditev. Če je X povezan s potmi, je povezan.

Dokaz. Očitno iz prejšnjih dveh trditev. □

Pripomba. V $\mathbb{R}$ so podmnožice povezane natanko takrat, ko so povezane s potmi.

Zgled. $f(x) : (0,1) \to [0,1]$ s predpisom $x \mapsto \sin \frac{\pi}{x}$ tvori krivuljo $I \subseteq \mathbb{R}^2$. Naj bo $\overline{I}$ zaprtje te krivulje. Slednje je povezano, a ne s potmi, saj ni poti od 1 do 0.

Trditev. Če je $U^{\text{odp.}} \subseteq \mathbb{R}^n$, je U povezana $\Leftrightarrow$ U povezana s potmi.

Dokaz. Dokazujemo ekvivalenco.

($\Leftarrow$) Velja.

($\Rightarrow$) Naj bo $x_0 \in U$ in $A \coloneqq \{x \in U; \exists \text{pot v } U \text{ od } x_0 \text{ do } x\}$. Očitno je A odprta (če lahko pridemo do x, lahko tudi do njene okolice). Nadalje velja, da je A^C odprta (če ne moreš priti do $a \in A^C$, ne moreš priti niti do neke njene okolice). Potemtakem je A odprta in zaprta. Ker je A povezana, sledi $A = U$ ali $\emptyset$, torej je $A = U$.

□

3 Fourierova vrsta in fourierova transformacija

3.1 Fourierova vrsta

Funkcije $\sin x$, $\sin 2x$, $\sin 3x$, ... so $2\pi-$periodične, na intervalu $[0,\pi]$ naredijo po $1,2,3,\ldots$ nihajev. S seštevanjem z različnimi utežmi dobivamo nove $2\pi-$periodične funkcije.

Vsako sinusoido lahko razumemo kot nihanje z neko frekvenco. Če seštevamo nihanje z različnimi frekvencami je vsaj z grafa praktično nemogoče razbrati, katere frekvence smo sešteli.

Pa denimo, da je dana funkcija $f(x)$ (podana bodisi s formulo bodisi grafično bodisi numerično), za katero nekako vemo, da je vsota sinusnih funkcij:

$$f(x) = b_1 \sin x + b_2 \sin 2x + b_3 \sin 3x + \cdots + b_n \sin nx.$$

Želimo dobiti eksplicitno formulo za b_i za dano f. Je $2\pi-$periodična, liha in integrabilna.

Za $k,l \in \mathbb{N}$ velja formula (upoštevamo $2\sin(kx)\sin(lx) = \cos((k-l)x) - \cos((k+l)x)$)

$$\int_{-\pi}^{\pi} \sin(kx)\sin(lx)\,dx = \frac{1}{2}\int_{-\pi}^{\pi} \cos((k-l)x) - \cos((k+l)x)\,dx = \frac{1}{2}\left(\frac{\sin((k-l)x)}{k-l} - \frac{\sin((k+l)x)}{k+l}\right)\Bigg|_{-\pi}^{\pi} = 0,$$

kadar $k \neq l$, sicer, ko $k = l$, pa velja

$$\int_{-\pi}^{\pi} \sin(kx)\sin(lx)\,dx = \frac{1}{2}\int_{-\pi}^{\pi} \cancelto{0}{\cos\left((k-l)x\right)} - \cancelto{0}{\cos\left((k+l)x\right)}\,dx = \frac{1}{2}2\pi = \pi,$$

torej skupaj

$$\int_{-\pi}^{\pi} \sin(kx)\sin(lx)\,dx = \begin{cases} 0 & ; k \neq l \\ \pi & ; k = l \end{cases}.$$

To pomeni, da bo veljalo

$$\int_{-\pi}^{\pi} f(x)\sin(kx)\,dx = \int_{-\pi}^{\pi} (b_1 \sin x + \cdots + b_n \sin nx)\sin(kx)\,dx =$$

$$= \int_{-\pi}^{\pi} b_1 \sin x \sin(kx) + \cdots + b_k \sin(kx)\sin(kx) + \cdots + b_n \sin(nx)\sin(kx)\,dx =$$

$$= \cancel{\int_{-\pi}^{\pi} b_1 \sin x \sin(kx)\,dx} + \cdots + \int_{-\pi}^{\pi} b_k \sin(kx)\sin(kx)\,dx + \cdots + \cancel{\int_{-\pi}^{\pi} b_n \sin(nx)\sin(kx)\,dx} = b_k\pi,$$

ker smo tako dokazali v prejšnji trditvi.

Velja torej

$$b_k := \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\sin(kx)\,dx.$$

Te koeficiente pa lahko izračunamo za poljubno integrabilno funkcijo, ne le za tako, ki je liha in $2\pi-$periodična, vendar se bo, če dobljene koeficiente uporabimo v obrazcu $s(x) = b_1 \sin(x) + \cdots$, s s f ujemal le, če je f liha in $2\pi-$periodična. Radi bi se znebili omejitve lihosti in računalni frekvečne komponente tudi za sode funkcije.

Vsako funkcijo lahko razcepimo na sodi in lihi del (na vsoto sodega in lihega dela) takole:

$$f(x) = \overbrace{\frac{f(x) - f(-x)}{2}}^{\text{sodi del} =: f_s} + \overbrace{\frac{f(x) - f(-x)}{2}}^{\text{lihi del} =: f_l}.$$

Sodi del lahko zapišemo kot vsoto kosinusov, lihi del pa kot vsoto sinusov. Zankrat se še omejimo na lihe $2\pi-$periodične funkcije.

Zgled. Oglejmo si $f(x) = x$ na $[-\pi,\pi]$:

$$b_k = \frac{1}{\pi}\int_{-\pi}^{\pi} x \sin kx dx =$$

per partes $u = x$, $dv = \sin kx dx$, $du = dx$, $v = \frac{-\cos kx}{k}$:

$$= \frac{1}{\pi}\left(\frac{-1}{k}x\cos(kx)\Big|_{-\pi}^{\pi} + \frac{1}{k}\underbrace{\int_{-\pi}^{\pi}\cos kx dx}_{0,\ \text{integral periodične na periodi}}\right) = (-1)^{k+1}\frac{2}{k\cancel{\pi}}\cancel{\pi} = (-1)^{k+1}\frac{2}{k}.$$

Torej $f(x) = 2\sin x - \frac{2}{2}\sin 2x + \frac{2}{3}\sin 3x - \frac{2}{4}\sin 4x + \cdots \pm \frac{2}{n}\sin nx + \cdots$.

Naj bo $f(x)$ liha in $2\pi-$periodična. Tedaj definirajmo $n-$ti fourierov približek in označimo $\overline{f_n(x)} = b_1\sin x + b_2\sin 2x + \cdots + b_n\sin nx$, kjer $b_k := \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\sin(kx)\,dx$.

Naj bo $s_n(x) = c_1\sin x + c_2\sin 2x + \cdots + c_n\sin nx$ neka druga funkcija.

Ne trdimo, da je na vsakem naboru točk $\overline{f_n}$ bolj prilegajoča f kot neka druga funkcija (torej recimo s_n). Trdimo pa, da se najbolje prilega v povprečju na celem intervalu izmed vseh drugih funkcij. Formuliramo naslednji izrek:

Izrek. *Naj bo $f(x)$ liha integrabilna funkcija, $\overline{f_n}$ in s_n kot zgoraj. Potem velja*

$$\forall s_n : \int_{-\pi}^{\pi}\left(f(x) - \overline{f_n}(x)\right)^2 dx \le \int_{-\pi}^{\pi}(f(x) - s_n(x))\,dx$$

Dokaz. NE ZNAM DOKAZATI. □

Naj bo sedaj $f(x)$ liha in integrabilna na $[-\pi,\pi]$. Delne vsote $\overline{f_1}(x), \overline{f_2}(x), \ldots$ tvorijo fourierovo sinusno vrsto $b_1\sin x + b_2\sin 2x + b_3\sin 3x + \ldots$. Ali ta vrsta konvergira? Če konvergira, kaj je njena limita? Zaželjeno je, da konvergira k $f(x)$. Dokaz je težak za splošen f. Omejimo se na naslednji izrek:

Izrek. *Naj bo $f(x)$ dvakrat zvezno odvedljiva liha funkcija in naj velja $f(-\pi) = f(\pi) = 0$. Potem je pripadajoča fourierova vrsta konvergentna in velja, da je $\lim_{n\to\infty}\overline{f_n}(x) = f(x)$.*

Dokaz.

$$\pi b_k = \int_{-\pi}^{\pi} f(x)\sin kx dx =$$

Per partes $u = f(x)$, $dv = \sin kx dx$, $du = f'(x)\,dx$, $v = \frac{1}{k}\cos(kx)$:

$$= \cancel{\frac{-1}{k}f(x)\cos(kx)\Big|_{-\pi}^{\pi}}^{0} + \frac{1}{k}\int_{-\pi}^{\pi} f'(x)\cos kx dx =$$

Per partes $u = f'(x)$, $du = f''(x)$, $dv = \cos kx dx$, $v = \frac{1}{k}\sin kx$. Prvi člen pokrajšamo, ker $f(\pm\pi) = 0$.

$$= \cancel{\frac{1}{k^2}\sin kx f'(x)\Big|_{-\pi}^{\pi}}^{0} - \underbrace{\frac{1}{k^2}}_{k\to 0}\int_{-\pi}^{\pi}\overbrace{f''(x)}^{\text{omejena}}\sin kx dx$$

Kot vidimo, gredo členi vrste s $\frac{1}{k^2}$ proti 0, zato je funkcijska vrsta konvergentna. S tem dokažemo prvo točko.

Dokaz druge točke: po Weierstrassovem izreku lahko vsako funkcijo aproksimiramo s polinomi na $[,]$, polinome pa s sinusi. □

Sedaj pa še odpravimo lihost. $f(x) = f_s(x) + f_l(x)$. Izpeljati moramo še aproksimacijo s kosinusi:

$$\int_{-\pi}^{\pi}\cos kx\cos lx dx = \begin{cases} 0 & ; k \ne l \\ \pi & ; k = l \ne 0 \\ 2\pi & ; k = l = 0 \end{cases}$$

in označimo

$$a_k := \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\cos(kx)\,dx \quad \forall k \in \{0..n-1\}.$$

Fourierovo vrsto za f definiramo kot $\overline{f}(x) := \frac{a_0}{2} + a_1\cos x + b_1\sin x + a_2\cos 2x + b_2\sin 2x + \cdots$ in velja, da je izmed vseh takih vrst s sinusi in kosinusi stopnje do n fourierova najboljši povprečni približek funkcije f.

Izrek. *Naj bo $f(x)$ dvakrat zvezno odvedljiva in $2\pi-$periodična. Potem velja, da fourierova vrsta enakomerno konvergira proti funkciji $f(x)$.*

Dokaz. Ne bomo dokazali. □

Kaj pa, če f ni $2\pi-$periodična? $\overline{f}(x)$ je še vedno $2\pi-$periodična (periodično nadaljevanje) funkcije $f(x)$.

Definicija. $f(x)$ je odsekoma odvedljiva funkcija, če je odsekoma zvezna in ima v vseh točkah levi in desni odvod.

Izrek. *Splošni izrek brez dokaza. Naj bo $f : [-\pi, \pi] \to \mathbb{R}$ odsekoma odvedljiva. Potem je pripadajoča fourierova vrsta konvergentna in velja, da je $\overline{f} = f$ v vseh točkah, kjer je f zvezna. V točkah nezveznosti pa je $\overline{f}(x)$ enaka povprečju med levo in desno limito $f(x)$ pri tej točki.*

Zgled. Nekaj primerov:

- $\cos^2 2x - \frac{\sin^3 3x}{4} = \frac{1}{2} - \frac{3}{16}\sin 3x + \frac{1}{2}\cos 4x + \frac{1}{16}\sin 9x$
- $f(x) = x$: funkcija je liha, torej so vsi koeficienti pred kosinusi (b_k) enaki 0. $x = 2\left(\sin x - \frac{\sin 2x}{2} + \frac{\sin 3x}{3} - \frac{\sin 4x}{x} + \cdots\right)$.

3.2 Fourierova transformacija

Če uporabimo kompleksna števila in obrazec

$$e^{ix} = \cos x + i\sin x, \quad e^{-ix} = \cos x - i\sin x$$

torej

$$\cos x = \frac{1}{2}\left(e^{ix} + e^{-ix}\right), \quad \sin x = \frac{1}{2i}\left(e^{ix} - e^{-ix}\right),$$

lahko fourierovo vrsto zapišemo bolj simetrično:

$$\frac{a_0}{2} + \sum_{n=0}^{\infty} a_n \cos nx + b_n \sin nx = \frac{a_0}{2} + \sum_{n=1}^{\infty} a_n \frac{1}{2}\left(e^{inx} + e^{-inx}\right) + b_n \frac{1}{2i}\left(e^{inx} - e^{-inx}\right) =$$

$$= \frac{a_0}{2} + \sum_{n=1}^{\infty} \frac{a_n - ib_n}{2} e^{inx} + \frac{a_n + ib_n}{2} e^{-inx} = \sum_{-\infty}^{\infty} c_n e^{inx},$$

kjer je $c_0 = \frac{a_0}{2}$, $c_n = \frac{a_n - ib_n}{2}$, $c_{-n} = \frac{a_n + ib_n}{2}$. Te kompleksne koeficiente Fourierove vrste izračunamo direktno z enotno formulo

$$c_n = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)\, e^{-inx} dx, \quad n \in \mathbb{Z}$$

oziroma na periodi $2L$:

$$c_n = \frac{1}{2L}\int_{-L}^{L} f(x)\, e^{-in\frac{x\pi}{L}} dx$$

3.2.1 Približek na $\mathbb{R}$

Doslej smo približke našli le kot periodične funkcije s poljubno veliko periodo. Izkaže se, da je moč narediti fourierovo transformacijo tudi na celotnem $\mathbb{R}$ in ne več samo za celoštevilske frekvence:

$$\hat{f}(\omega) := \frac{1}{2\pi}\int_{-\infty}^{\infty} f(x)\, e^{i\omega x} dx, \quad \omega \in \mathbb{R}$$

Velja $\hat{f} : \mathbb{R} \to \mathbb{C}$. $\Re$ del je kosinusni del nihanja, $\Im$ del pa sinusni del.

Definicija. $\hat{f}$ pravimo fourierova transformiranka f. Operaciji $f \mapsto \hat{f}$ pravimo Fourierova transformacija.

Za obstoj integrala zahtevamo, da je f absolutno integrabilna, t. j. $\int_{-\infty}^{\infty} |f(x)|\, dx < \infty$.
Tipično je f

- bodisi odsekoma zvezna na $[a, b]$ in ničelna levo in desno od tega intervala
- bodisi periodična
- bodisi definirana povsod in gre v neskončnosti dovolj hitro proti 0 — $\lim_{x\to\pm\infty} f(x) = 0$.

Zgled. Nekaj primerov:

- $f(x) = \begin{cases} 1 & ; -a \le x \le a \\ 0 & ; sicer \end{cases}$. Naredimo fourierovo transformacijo:

$$\frac{1}{2\pi}\int_{-\infty}^{\infty} f(x)\, e^{-i\omega x} dx = \frac{1}{2\pi}\int_{-a}^{a} e^{-i\omega x} dx = \frac{1}{2\pi}\int_{-a}^{a} \left(\cos\omega x - \cancelto{0,\ \text{liha}}{i\sin\omega x}\right) dx = \frac{1}{2\pi}\ \frac{\sin\omega x}{\omega}\Big|_{-a}^{a} = \frac{\sin(a\omega)}{\pi\omega}$$

  Torej $\hat{f}(\omega) = \frac{1}{\pi}\frac{\sin a\omega}{\omega}$.

- $f(x) = \begin{cases} e^{-ax} & ; x \ge 0 \\ 0 & ; x < 0 \end{cases}$. Naredimo fourierovo transformacijo:

$$\frac{1}{2\pi}\int_{0}^{\infty} e^{-ax} e^{-i\omega x} dx = \frac{1}{2\pi}\int_{0}^{\infty} e^{-(a+i\omega)x} dx = \frac{1}{2\pi}\ \frac{e^{-(a+i\omega)x}}{-(a+i\omega)}\Big|_{0}^{\infty} = \frac{1}{2\pi(a+i\omega)}$$

3.2.2 Lastnosti Fourierove transformacije

Trditev. Velja:

- $a\hat{f} + bg = a\hat{f} + b\hat{g}$ — linearnost integrala
- $f(x)$ absolutno integrabilna $\Rightarrow \lim_{\omega\to\pm\infty} \hat{f}(\omega) = 0$ (brez dokaza)
- Dana je $g(\omega) \mapsto \overline{g}(\omega)$.

$$\overline{g}(x) = \int_{-\infty}^{\infty} g(\omega)\, e^{i\omega x} d\omega$$

  je obratna formula za fourierovo transformacijo — inverzna fourierova transformacija.

Izrek. *Naj bo $f(x)$ absolutno integrabilna in odsekoma odvedljiva. Tedaj je tudi $\hat{f}(\omega)$ absolutno integrabilna in velja $\overline{\hat{f}}(x) = f(x)$ v vseh točkah, kjer je f zvezna. V točkah nezveznosti je $\overline{\hat{f}}$ enaka povprečju leve in desne limite.*

Trditev. Velja

1. $f(x), f'(x)$ absolutno integrabilni $\Longrightarrow (\hat{f'}) = i\omega\hat{f}(\omega)$

   Dokaz.

$$\frac{1}{2\pi}\int_{-\infty}^{\infty} f(x)\, e^{-i\omega x} dx =$$

   per partes: $u = e^{-i\omega x}$, $du = -i\omega e^{-i\omega x}$, $dv = f(x)\,dx$, $v = f(x)$

$$= \cancel{\frac{1}{2\pi} f(x) e^{-i\omega x}\Big|_{-\infty}^{\infty}} + i\omega\int_{\infty}^{\infty} f(x)\, e^{-i\omega x} dx = i\omega\hat{f}(\omega)$$

   □

2. $f(x), g(x) = xf(x)$ absolutno integrabilni $\Longrightarrow \left(\hat{f}\right)' = -i\hat{g}$

   Dokaz. $\left(\hat{f}\right)' = -ix\overline{\left(\hat{\ }\right)}(\cancel{f}) = -ix\hat{f}(x) = -i\hat{g}(\omega)$ □

Posledica. *Fourierova transformiranka Gaussove funkcije je Gaussova funkcija:*

$$f(x) = e^{-\frac{x^2}{2}} \Longrightarrow \hat{f}(\omega) = \frac{1}{\sqrt{2\pi}} e^{-\frac{\omega^2}{2}}$$

3.2.3 Interpretacija Fourierove vrste v vektorskem prostoru s skalarnim produktom

Naj bo V vektorski prostor, $\vec{v}, \vec{u} \in V$. Skalarni produkt $\vec{u} \cdot \vec{v}$ je komutativen, bilinearen, $\vec{u} \cdot \vec{u} \geq 0, \vec{u} \cdot \vec{u} = 0 \Leftrightarrow \vec{u} = 0$. Z njim lahko definiramo normo $|\vec{u}| \coloneqq \sqrt{\vec{u} \cdot \vec{u}}$ in kot med vektorjema: $\cos \alpha = \frac{\vec{u} \cdot \vec{v}}{|\vec{u}| \cdot |\vec{v}|}$. Torej $\vec{u} \times \vec{v}$ sta ortogonalna, če je $\vec{u} \times \vec{v} = 0$. Iz ortogonalnosti sledi linearna neodvisnost:

$$\begin{aligned} a\vec{u} + b\vec{v} = \vec{0} \quad / \cdot \vec{u} \qquad &\Rightarrow \qquad a\,|\vec{u}|^2 = 0 \Rightarrow a = 0 \\ a\vec{u} + b\vec{v} = \vec{0} \quad / \cdot \vec{v} \qquad &\Rightarrow \qquad b\,|\vec{v}|^2 = 0 \Rightarrow b = 0 \end{aligned}$$

Če so $\vec{u_1}, \vec{u_2}, \vec{u_3}, \dots \in V$ paroma ortogonalni, jih lahko uporabimo za bazo (vsaj prostora, ki ga razpenjajo):

$$\vec{u} = \frac{\vec{u} \cdot \vec{u_1}}{\vec{u_1} \cdot \vec{u_1}} \cdot \vec{u_1} + \frac{\vec{u} \cdot \vec{u_2}}{\vec{u_2} \cdot \vec{u_2}} \cdot \vec{u_2} + \cdots$$

3.2.4 Analiza signala

Naj bo $s(x)$ vsota sinusov in kosinusov raznih frekvenc. Dovolj je, če si zapišemo amplitude, ki pripadajo dani frekvenci, da rekonstruiramo s.

Zgled. Nekaj primerov:

- $\sin x$ nam da sinusne koeficiente $(0, 0, 0, 0, \dots)$ in kosinusne koeficiente $(0, 1, 0, 0, \dots)$
- $\sin^2 x = \frac{1}{2} - \frac{1}{2} \cos 2x$ nam da sinusne koeficiente $(0, 0, 0, 0, \dots)$ in kosinusne koeficiente $\left(\frac{1}{2}, 0, -\frac{1}{2}, 0, \dots\right)$
- $x = 2\left(\sin x - \frac{\sin 2x}{2} + \frac{\sin 3x}{3} - \cdots\right)$ nam da sinusne koeficiente $\left(0, \frac{1}{2}, -1, \frac{2}{3}, \dots\right)$ in kosinusne koeficiente $(0, 0, 0, 0, \dots)$

Temu prikazu se reče fazna slika (fazni portret) funkcije oziroma slika v faznem prostoru.

Ideja je, da se v faznem portretu jasno vidi, katere frekvence je dovolj upoštevati za primerno natančen približek.