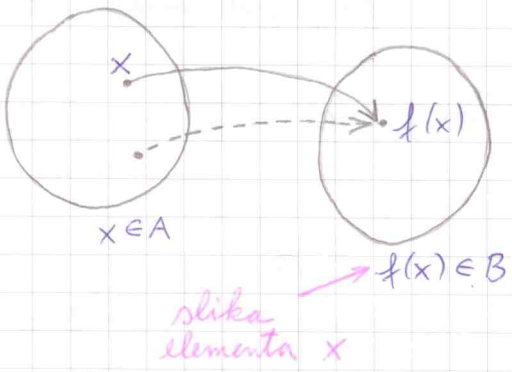
Osnovne algebrske strukture

Preslikave in relacije

A, B, f

$f : A \longrightarrow B$ (B: kodomena; A: definicijsko območje ali domena)



$\forall x \in A \quad f(x) \in B$

$Z_f = \{ f(x) : x \in A \} \quad Z_f \subseteq B$

Zaloga vrednosti

f je **surjektivna** $\overset{\text{def.}}{\iff} Z_f = B$

Velja: f surjektivna $\iff \forall y \in B \; \exists x \in A : y = f(x)$

f je **injektivna** $\overset{\text{def.}}{\iff} (x_1, x_2 \in A, f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$

$$\left.\begin{matrix} x_1, x_2 \in A \\ x_1 \neq x_2 \end{matrix}\right\} \Rightarrow f(x_1) \neq f(x_2)$$

$f : A \to B$ je **bijektivna** (bijekcija), kadar je surjektivna in injektivna

Naj bo f bijekcija. ($f : A \to B$)
Potem obstaja taka preslikava $g : B \to A$, da velja
$g(f(x)) = x \quad \forall x \in A$ in
$f(g(y)) = y \quad \forall y \in B$

g imenujemo inverz preslikave f oznaka: $g \equiv f^{-1}$

Recimo, da sta dani presl. f, g;

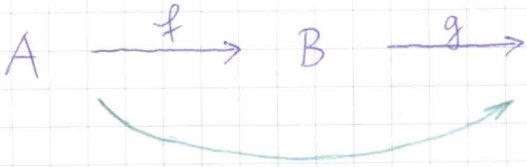
$f: A \to B$, $g: B \to A$, za kateri veljá

$$g(f(x)) = x \quad \forall x \in A \quad \text{in}$$
$$f(g(y)) = y \quad \forall y \in B.$$

← Kaj lahko sklepamo, če je ← samo eno od tega res?

Potem sta f in g bijekciji in velja $g = f^{-1}$.

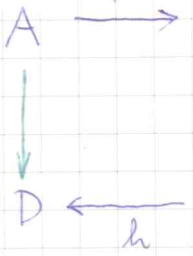
$f: A \to B$
$g: B \to C$
} „skomponiramo"



gf
$(g \circ f)$

$$gf(x) = g(f(x)) \quad \forall x \in A$$

diagram komutira



$$\boxed{h(gf) = (hg)f}$$

$h(gf)(x) = h(gf(x)) =$
$= h(g(f(x)))$

$(hg)f(x) = hg(f(x)) =$
$= h(g(f(x)))$

$$\boxed{hgf}$$

$id_A: A \longrightarrow A$

identična preslikava ali identiteta

$id_A(x) = x$ identična preslikava množice A

f bijekcija $f: A \longrightarrow B$

$\exists_g \; g: B \longrightarrow A$, tako da velja $\boxed{gf = id_A \quad fg = id_B}$

g je inverz preslikave f;

$g = f^{-1}$

$f: A \longrightarrow B$

$Gr(f) = \{(x,y) : y = f(x), x \in A\}$

graf preslikave f

$Gr(f) \subseteq A \times B$

Relacije

A, B neprazni množici

Relacija med el. iz A in el. iz B je podmnožica kart. produkta $A \times B$;

$R \subseteq A \times B$

Npr. $f: A \longrightarrow B$; $Gr(f)$ je relacija...

Če je $B = A$; $R \subseteq A \times A$

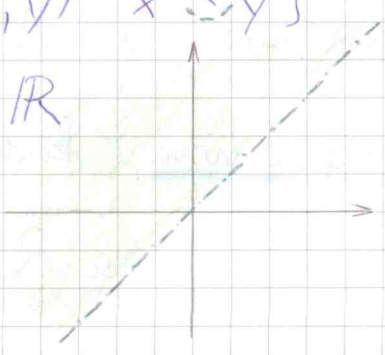
R je relacija na A.

Npr. $A = \mathbb{R}$, $R = \{(x,y) : x \leq y\}$

R je relacija na $\mathbb{R}$

$R \equiv \leq$

$(x,y) \in R \equiv x R y$



Nekaj primerov:

1) $\leq$ je relacija na $\mathbb{R}$

2) A - množica premic vzporednost: $p_1 \parallel p_2$
(p_1, p_2 - premici) je relacija na A

3) $M \neq \emptyset$; $A = \mathcal{P}M$
relacija inkluzije na A
$M_1 \subseteq M_2$ $(M_1, M_2 \in \mathcal{P}M)$

4) Pravokotnost premic
$p \perp q$

5) A - množica daljic v $\mathbb{R}^3$
$e, f \in A$
$e \cong f$ skladnost

6) Deljivost v $\mathbb{N}$
$n_1 \mid n_2$ $(\exists\, k \in \mathbb{N} : n_2 = k \cdot n_1)$

7) $A = \mathbb{Z} \times \mathbb{N} = \{(m, n) : m \in \mathbb{Z}, n \in \mathbb{N}\}$

$\sim$ relacija ekvivalence v A:
$(m_1, n_1) \sim (m_2, n_2)$, kadar velja
$m_1 n_2 = m_2 n_1$

Relacija R na A je

(1) refleksivna, kadar velja

$a R a \quad \forall a \in A;$

(2) simetrična, kadar velja sklep:

$$a R b \Rightarrow b R a \; ; \quad a, b \in A$$

(3) antisimetrična, kadar velja sklep:

$$(a R b \text{ in } b R a) \Rightarrow a = b ;$$

(4) tranzitivna, kadar velja sklep:

$$(a R b \text{ in } b R c) \Rightarrow a R c .$$

Relacija R na A je delna urejenost, kadar je refleksivna, antisimetrična in tranzitivna.

Relacija R na A je relacija ekvivalence oz. ekvivalenčna relacija, kadar je refleksivna, simetrična in tranzitivna.

Primeri 1), 3), 6) so delno urejeni, primeri 2), 5), 7) so ekvivalenčne relacije.

Ekvivalenčne relacije

R je ekvivalenčna relacija v množici A.

$a \in A$, $[a] = \{ x \in A : x R a \}$

ekvivalenčni razred elementa a

- namesto R navadno pišemo $\sim$

$$[a] = \{ x \in A : x \sim a \}$$

$a \in [a]$ (refleksivnost!)

$a, b \in A$

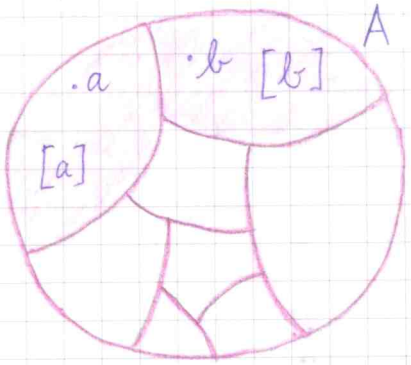
$[a], [b]$; recimo, da je presek $[a] \cap [b]$ neprazen, torej $\exists\, c \in [a], c \in [b]$

Naj bo $x \in [a]$. Torej $x \sim a$.
Vemo, da je $c \sim a$ in zato $a \sim c$ (simetričnost!)

Zaradi tranzitivnosti je $x \sim c$.
Ker je $c \sim b$, velja $x \sim b$ (tranzitivnost!),
torej $x \in [b]$.

Zato je $[a] \subseteq [b]$.
$a \leftrightarrow b \Rightarrow [b] \subseteq [a]$.
Vboje skupaj da $[a] = [b]$.

Torej velja: $[a] \cap [b] \neq \emptyset \Rightarrow [a] = [b]$
oziroma $[a] \neq [b] \Rightarrow [a] \cap [b] = \emptyset$
sta disjunktna



$[a] \cap [b] = \emptyset$

$\bigcup_{a \in A} [a] = A$

Množico A smo razčlenili na ekvivalenčne razrede.

$A/_\sim = \{[a] : a \in A\}$

kvocientna množica

Primer (7): $A = \mathbb{Z} \times \mathbb{N}$

$$(m_1, n_1) \sim (m_2, n_2) \overset{def.}{\iff} m_1 n_2 = m_2 n_1$$

$$(m_1, n_1) \equiv \frac{m_1}{n_1}$$

$$\frac{m_1}{n_1} \sim \frac{m_2}{n_2} \iff m_1 n_2 = m_2 n_1$$

$$A/_\sim = \mathbb{Q}$$

Operacije

Operacija na A je preslikava

$$A \times A \longrightarrow A$$
$$(a, b) \longmapsto a \circ b$$

kompozitum elementa a z b

Zgledi: $A = \mathbb{R}$, $\circ$ seštevanje $+$
množenje $\cdot$

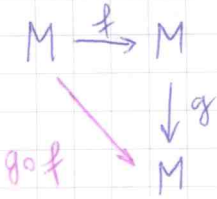
$$(a, b) \longmapsto a + b$$
$$(a, b) \longmapsto a \cdot b$$

$A = \mathbb{R}^3$, $\circ$ vektorsko množenje (produkt)

$$(\vec{a}, \vec{b}) \longmapsto \vec{a} \times \vec{b}$$

$M \neq \emptyset \quad A = F(M) = \{ f : M \to M \}$
preslikave iz M vase

$\circ$ komponiranje preslikav je operacija na A



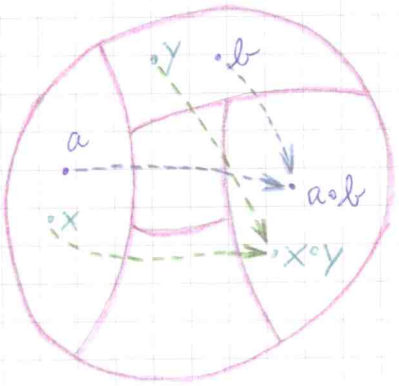
$(f,g) \in A \times A$

$f \circ g \in A$

$(f,g) \longmapsto f \circ g$

$(A, \circ)$ $\circ$ operacija na A

$(A, \sim)$ $\sim$ ekvivalenčna relacija na A



$A/\sim$

Operacija $\circ$ je usklajena z ekvivalenčno relacijo $\sim$, kadar velja sklep:

$(x \sim a)$ in $(y \sim b) \Rightarrow$
$(x \circ y \sim a \circ b)$

grupoid

$(M, \circ)$, $(M, \sim)$

$\circ$ je usklajena z $\sim$:

komponiramo ekvivalenčne razrede

$x_1 \sim x$, $y_1 \sim y \Rightarrow x_1 \circ y_1 \sim x \circ y$

$M/\sim = \{[x] : x \in M\}$

V $M/\sim$ vpeljemo operacijo $\bullet$:

$[x] \bullet [y] = [x \circ y]$, $x, y \in M$

$[x_1] = [x]$ $(x_1 \sim x)$

$[y_1] = [y]$ $(y_1 \sim y)$

usklajenost

Zaradi usklajenosti op. $\circ$ z rel. $\sim$ je definicija dobra.

$\Rightarrow [x_1 \circ y_1] = [x \circ y]$
$(x_1 \circ y_1 \sim x \circ y)$

Primer: $M = \mathbb{Z} \times \mathbb{N}$

$(m_1, n_1) \sim (m_2, n_2) \overset{def.}{\Leftrightarrow} m_1 n_2 = m_2 n_1$

$(M, +)$: $(m_1, n_1) + (m_2, n_2) = (m_1 n_2 + m_2 n_1,\ n_1 n_2)$

Operacija $+$ je usklajena z rel. $\sim$

$M/_\sim = (\mathbb{Z} \times \mathbb{N})/_\sim \equiv \mathbb{Q}$

$(m, n) \equiv \frac{m}{n}$ $\qquad \frac{m_1}{n_1} + \frac{m_2}{n_2} = \frac{m_1 n_2 + m_2 n_1}{n_1 n_2}$

$(M/_\sim, \oplus) \equiv \boxed{(\mathbb{Q}, +)}$

$[(m_1, n_1)] \oplus [(m_2, n_2)] = [(m_1, n_1) + (m_2, n_2)]$

Homomorfizem in izomorfizem

$M = \{1, -1\}$, operacija je množenje

$N = \{e, f\}$, -"- komponiranje preslikav

$e = id_{\mathbb{C}} : \mathbb{C} \to \mathbb{C} \quad (e(z) = z \ \forall z \in \mathbb{C})$

$f : \mathbb{C} \to \mathbb{C} \quad (f(z) = \bar{z} \ \forall z \in \mathbb{C})$

$f \circ f = e \ (= id_{\mathbb{C}})$

(M)

$\cdot$	1	-1
1	1	-1
-1	-1	1

(N)

$\circ$	e	f
e	e	f
f	f	e

$e \ldots 1$

$f \ldots -1$

$(M, \cdot)$ in $(N, \circ)$ sta izomorfna;

Def. Naj bo $\circ$ operacija na množici M_1 in $\bullet$ operacija na M_2. Preslikava

$f : M_1 \to M_2$ je homomorfizem, kadar velja $f(x \circ y) = f(x) \bullet f(y)$ za vsak $x, y \in M_1$.

Taka preslikava je izomorfizem, če je hkrati še bijektivna.

Bijektiven homomorfizem imenujemo izomorfizem.

Trditev: Inverz izomorfizma je izomorfizem.

Dokaz: Naj bo $f: M_1 \to M_2$ izomorfizem med $(M_1, \circ)$ in $(M_2, \bullet)$. Preslikava $f^{-1}: M_2 \to M_1$ je bijektivna. (ker je f bijektivna)

Dokažimo, da je f^{-1} homomorfizem.

$$f^{-1}(u \bullet v) = f^{-1}(f(x) \bullet f(y)) \quad \Leftrightarrow$$

$u, v \in M_2 \qquad \exists\, x, y \in M_1 : f(x) = u,\ f(y) = v$

$$\Leftrightarrow f^{-1}(f(x \circ y)) = x \circ y = f^{-1}(u) \circ f^{-1}(v)$$

$$x = f^{-1}(u), \quad y = f^{-1}(v)$$

Grupe

Polgrupa je neprazna množica, skupaj z operacijo, ki je asociativna:

$$(a \circ b) \circ c = a \circ (b \circ c)$$

za vse elemente te množice.

Element e polgrupe S imenujemo enota (ali nevtralni element), kadar velja:

$$a \circ e = e \circ a = a$$

za vsak $a \in S$.

Primeri: $(\mathbb{N},+)$, $(\mathbb{N},\cdot)$, $(\mathbb{Z},+)$, $(\mathbb{Z},\cdot)$, $(\mathbb{R},+)$, $(\mathbb{R},\cdot)$, $F(M) - f: M \to M$

množica vseh preslikav z operacijo komponiranja

Edino $(\mathbb{N},+)$ nima enote.

e_1, e_2 enoti polgrupe S

$e_1 \overset{\uparrow}{=} e_1 \circ e_2 \overset{\uparrow}{=} e_2$

(e_2 enota) (e_1 enota)

Trditev. V polgrupi z enoto je enota ena sama.

Grupa je polgrupa z enoto, v kateri za vsak element obstaja inverz:

$$\forall a \in G \quad \exists b \in G : \quad a \circ b = b \circ a = e.$$

$(G,\circ)$ - grupa

Primeri: $(\mathbb{Z},+)$, $(\mathbb{R},+)$, $(\mathbb{R}\setminus\{0\},\cdot)$, $(\mathbb{R}^+\setminus\{0\},\cdot)$,
$S(M) = \{ f: M \to M ;\ f \text{ bijekcija} \}$

$(S(M),\circ)$ je grupa simetrij množice M

M končna: $M = \{1,2,3,\dots,n\}$
$S(M)$ = grupa permutacij reda n ali simetrična grupa reda n

$$S(M) \equiv S_n$$

$a \in G$, b_1, b_2 inverza

$$a \circ b_1 = b_1 \circ a = e \qquad a \circ b_2 = b_2 \circ a = e$$

$$(\overbrace{b_1 \circ a}^{e}) \circ b_2 = b_2 \quad \Rightarrow \quad \boxed{b_1 = b_2}$$

$$b_1 \circ (\underbrace{a \circ b_2}_{e}) = b_1$$

Izrek. V grupi obstaja za vsak element natanko en inverz.

$a \in G$; a^{-1} - inverz

$a \circ a^{-1} = a^{-1} \circ a = e$

Def. Podgrupa grupe $(G, \circ)$ je podmnožica $H \subseteq G$ skupaj z operacijo $\circ$ iz $(G, \circ)$, če velja sklep:

$$(a \in H, b \in H) \Rightarrow a \circ b^{-1} \in H.$$

Zahtevamo še, da je $H \neq \emptyset$.

1) Enota e grupe G pripada podgrupi H:

$a \in H \Rightarrow \underbrace{a \circ a^{-1}}_{e} \in H$ ($b = a$ v def.)

2) Velja: $a \in H \Rightarrow a^{-1} \in H$

(v def. $a = e$, $b = a$)

$(\underbrace{e}_{1)} \in H, a \in H) \Rightarrow \underbrace{e \circ a^{-1}}_{a^{-1}} \in H$

podgrupa je zaprta za invertiranje

3) $a, b \in H \Rightarrow a \circ b \in H$

$b \in H \overset{2)}{\Rightarrow} b^{-1} \in H \qquad a, b \in H \Rightarrow a, b^{-1} \in H$

$\Rightarrow a \circ (b^{-1})^{-1} \in H$

torej $a \circ b \in H$.

$b \circ b^{-1} = b^{-1} \circ b = e$

$(b^{-1})^{-1} = b$

Zato je $(H, \circ)$ grupa.

Primeri: $(\mathbb{Z}, +)$ je podgrupa $(\mathbb{R}, +)$;

$(\mathbb{R}^+ \setminus \{0\}, \cdot)$ je podgrupa $(\mathbb{R} \setminus \{0\}, \cdot)$;

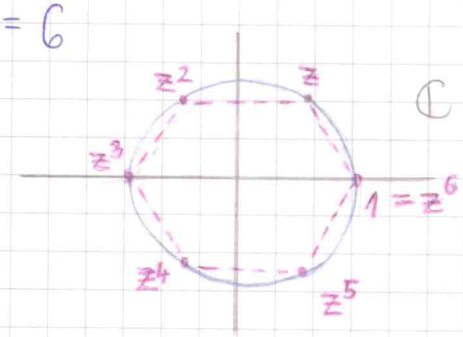
$C_n = \{1, z, z^2, \dots, z^{n-1}\}$

$z = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n} \in \mathbb{C}$

n-ti koren enote

$(C_n, \cdot)$ - ciklična grupa reda n

$n = 6$



$(C_n, \cdot)$ je podgrupa grupe $(\mathbb{C} \setminus \{0\}, \cdot)$

$S^1 = \{z \in \mathbb{C} : |z| = 1\}$

$(S^1, \cdot)$ je podgrupa grupe $(\mathbb{C} \setminus \{0\}, \cdot)$;

$C_n \subset S^1 \subset \mathbb{C}$

1) $G = \{e\}$; e - enota

trivialna grupa $e \circ e = e$

2) $G = \{e, a\}$, e - enota

$\circ$	e	a
e	e	a
a	a	?

$a \circ a = a$? $\Rightarrow$

$(a \circ a) \circ a^{-1} = a \circ a^{-1}$

$a \circ (a \circ a^{-1}) = a \circ a^{-1} = e$

$a \circ e = a$

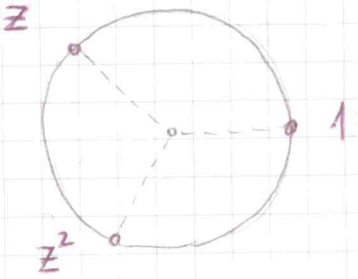
$\Rightarrow a = e$

Torej je $a \circ a = e$ (= ?)

Obstaja grupa z dvema elementoma: C_2.

C_3 - ciklična grupa

$\{1, z, z^2\}$, $z^3 = 1$



$G = \{e, a, b\}$ ... grupa 3 elem.

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

različni el.

$a \circ a \ (= a^2)$

1) $a^2 = e$?

2) $a^2 = a$?

3) $a^2 = b$?

2) $a \circ a = a \mid a^{-1}$

$(a \circ a) \circ a^{-1} = a \circ a^{-1}$

$a \circ (a \circ a^{-1}) = e$

$a \circ e = e$

$\Rightarrow a = e$

2) ne gre

1) $a \circ a = e$

$\circ$	e	a
e	e	a
a	a	e

$\{e, a\}$ podgrupa grupe G

$b \circ e$, $b \circ a$ sta različna ← če imamo poleg e in a še b

$(b \circ e = b \circ a \Rightarrow b^{-1} \circ (b \circ e) = b^{-1} \circ (b \circ a)$

$\Rightarrow (\underbrace{b^{-1} \circ b}_{e}) \circ e = (\underbrace{b^{-1} \circ b}_{e}) \circ a \Rightarrow e = a$)

↑ $b \circ a \neq b$

b, $b \circ a$

$b \circ a \neq a$ ($b \neq e$) ← $b \circ a \neq a$

$e, a, b, b \circ a$ štirje razl. el. (če $b \circ a \neq e$)

$\Rightarrow \left.\begin{matrix} b \circ a = e \\ a \circ a = e \end{matrix}\right\} a = b$

1) ne gre (ostane le 3), torej velja $a^2 = b$.

$f : C_3 \longrightarrow G$

$f(1) = e \quad f(z) = a \quad f(z^2) = b$

DOMAČA VAJA: premisli za 4el, 5el, ...

f je izomorfizem grup C_3 in G

Homomorfizmi grup

G_1, G_2 grupi

$e_1 \in G_1$ enota $\quad e_2 \in G_2$ enota

$f : G_1 \longrightarrow G_2$ homomorfizem

$f(x \circ y) = f(x) \circ f(y)$

Zaloga vrednosti homomorfizma f: image/imidž

$\operatorname{im} f = \{ f(x) : x \in G_1 \}$ je podgrupa grupe G_2.

Dokaz:

$f(e_1) = e_2$

$y \in G_2 \qquad e_2 \circ y = y$

$y = f(e_1) \Rightarrow e_2 \circ f(e_1) = y \circ f(e_1) = y$

$y = f(x), \quad x \in G_1$

$y \circ f(e_1) = f(x) \circ f(e_1)$

$y^{-1} \circ (y \circ f(e_1)) = y^{-1} \circ y$

$f(\underbrace{x \circ e_1}_{x}) = f(x) = y$

$(\underbrace{y^{-1} \circ y}_{\|}) \circ f(e_1) = e_2$

$e_2 \circ f(e_1) = f(e_1)$

Zato $e_2 \in \text{im } f$.

im f = zaprt za komponiranje

$f(u), f(v) \in \text{im } f$

$f(u) \circ f(v) = f(u \circ v) \in \text{im } f$ ✓

$f(x^{-1}) = f(x)^{-1} \quad (x \in G_1)$ ⊛

$f(x^{-1}) \circ f(x) = f(\underbrace{x^{-1} \circ x}_{e_1}) = f(e_1) = e_2$

$\|$

$f(x)^{-1} \circ f(x)$

$f(x) \circ f(x^{-1}) = f(\underbrace{x \circ x^{-1}}_{e_1}) = f(e_1) = e_2$

$\Rightarrow$ ⊛ Od tod sledi zaprtost im f za invertiranje.

$f(x^{-1}) = f(x)^{-1} \quad (x \in G_1)$

Ker $f(x^{-1}) = f(x)^{-1}$ in $f(x^{-1}) \in \text{im } f \Rightarrow f(x)^{-1} \in \text{im } f$

$f(x)^{-1}$ pa je ravno inverz k $f(x)$, zato je im f res zaprt za inventiranje. ∎

$f: G_1 \to G_2$ naj bo homomorfizem grup

$e_1 \in G_1$ $e_2 \in G_2$ sta enoti velmo: $f(e_1) = e_2$

Jedro homomorfizma f je $\ker f = \{x \in G_1 : f(x) = e_2\}$

(1) $\ker f$ je podgrupa grupe G_1

(2) f je injekcija $\Leftrightarrow \ker f = \{e_1\}$

Simetrične grupe $(S_n, \circ)$

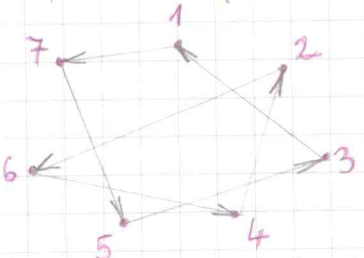
$S_n = \{\pi : \{1,2,\dots,n\} \to \{1,2,\dots,n\};\ \pi \text{ bijekcija}\}$

$$\pi \downarrow \begin{matrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{matrix} \qquad \{\pi(1), \pi(2), \dots, \pi(n)\} = \{1,2,\dots,n\}$$

π - permutacija (reda n)

Zapis: $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ $\pi(k) = i_k$

S_n ima $n!$ elementov. $\pi \in S_7$, $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$



$a_1, \dots, a_k \in \{1,2,\dots,n\}$ različni

$\sigma = (a_1, a_2, \dots, a_k) \in S_n$ je cikel, kadar velja:

$\sigma(a_i) = a_{i+1}$ za $i = 1,2,\dots,k-1$

$\sigma(a_k) = a_1$

$\sigma(p) = p$ za $p \in \{1,\dots,n\} \setminus \{a_1, \dots, a_k\}$

Red ali dolžina cikla σ je k. $(k > 1)$

$k = 1$: $(a_1) = id$

Naš primer: $\sigma_1 = (1,7,5,3) = (7,5,3,1) = \dots$

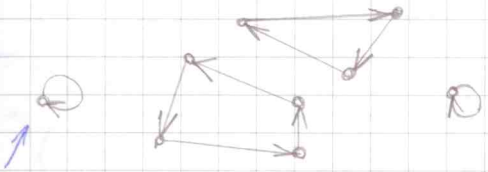
$\sigma_2 = (2,6,4)$

$\pi = \sigma_2 \circ \sigma_1 = \sigma_1 \circ \sigma_2$

cikla σ_1 in σ_2 sta disjunktna, kadar sta pripadajoči množici disjunktni; v tem primeru sta

Velja trditev:

Vsaka permutacija je kompozitum paroma disjunktnih ciklov. Pri tem cikli med sabo komutirajo (vrstni red pri komponiranju ni pomemben) in so do vrstnega reda natančno enolično določeni.



teh nam niti ni treba pisati

Cikel reda 2 imenujemo transpozicija. $\tau = (a_1, a_2)$

$\tau \circ \tau = id$

Trditev: Vsak cikel je kompozitum (produkt) samih transpozicij.

Dokaz: $\sigma = (a_1, a_2, \dots, a_k) \Rightarrow$

$\Rightarrow \sigma = (a_1, a_k) \dots (a_1, a_4)(a_1, a_3)(a_1, a_2)$ ∎

! Če uporabimo še prejšnjo trditev, je vsaka permutacija kompozitum samih transpozicij.

Naj bo $\sigma = (a_1, \dots, a_k) \in S_n$ cikel dolžine k.

$$\text{znak } s(\sigma) = \begin{cases} 1; & k \text{ je liho št.} \\ -1; & k \text{ je sodo št.} \end{cases}$$

τ transpozicija $\Rightarrow s(\tau) = -1 \qquad s(id) = 1$

Glej zvezek z zadnje strani za nadaljevanje.

$\pi \in S_n$ poljubna permutacija

$\pi = \sigma_1 \sigma_2 \dots \sigma_m$ (paroma disjunktni cikli)

$s(\pi) \overset{def.}{=} s(\sigma_1) \cdot s(\sigma_2) \cdot \dots \cdot s(\sigma_m)$

Ali so identitete zraven je vseeno.

S tem je $s(\pi)$ enoličnо določen.

Trditev: Za vsako permutacijo π in transpozicijo τ velja: $s(\tau\pi) = -s(\pi)$

Ideja dokaza:

1) Razcepimo π na paroma disjunktne cikle.
=> Trditev zadošča dokazati za primer, ko je π cikel ali produkt dveh ciklov.

2) π je cikel; $\pi = (a_1, \dots, a_j, \dots, a_k)$
$\tau = (a_1, a_j)$

3) π je produkt dveh ciklov;
$\pi = (a_1, \dots, a_k)(b_1, \dots, b_\ell)$
$\tau = (a_1, b_1)$

Trditev: $\pi \in S_n$, τ transpozicija $\tau \in S_n$
Potem je $s(\tau\pi) = -s(\pi)$

Dokaz: $\pi = \sigma_1 \sigma_2 \dots \sigma_m$ disjunktni cikli
$s(\pi) = s(\sigma_1) s(\sigma_2) \dots s(\sigma_m)$ ↖ komutirajo

I. elementa iz τ sta v enem samem ciklu izmed $\sigma_1, \dots, \sigma_m$; npr. σ_1

$\tau\sigma_1 = ?$ $\quad \tau = (a_1, a_j)$

$\sigma_1 = (a_1 \dots a_j \dots a_k)$

$$(a_1 a_j)(a_1 \dots a_j \dots a_k) = (a_j \dots a_k)(a_1 \dots a_{j-1}) = (a_1 \dots a_{j-1})(a_j \dots a_k)$$

$\tau\pi = (a_1 \dots a_{j-1})(a_j \dots a_k)\sigma_2 \dots \sigma_m$ disjunktni cikli

$(-1)^{j}$ $\quad (-1)^{k-j+2}$

$s(\tau\pi) = s((a_1 \dots a_{j-1}))\, s((a_j \dots a_k))\, s(\sigma_2) \dots s(\sigma_m)$

$s(\tau\pi) = (-1)^k s(\sigma_2) \dots s(\sigma_m)$

$s(\pi) = (-1)^{k+1} s(\sigma_2) \dots s(\sigma_m)$

$= s(\sigma_1)$

$\Rightarrow s(\tau\pi) = -s(\pi)$

II. elementa iz τ sta vsak v svojem ciklu izmed $\sigma_1, \dots, \sigma_m$, npr. σ_1 in σ_2

$\tau = (a_1, b_1)$

$\sigma_1 = (a_1, \dots, a_j)$

$\sigma_2 = (b_1, \dots, b_k)$

$\tau\sigma_1\sigma_2 = (a_1, b_1)(a_1, \dots, a_j)(b_1, \dots, b_k) =$

$= (a_1, \dots, a_j, b_1, \dots, b_k)$

$s(\tau\sigma_1\sigma_2) = (-1)^{j+k+1}$

$s(\sigma_1\sigma_2) = s(\sigma_1)\cdot s(\sigma_2) = (-1)^{j+1}(-1)^{k+1} = (-1)^{j+k}$ (+2)

$\Rightarrow s(\tau\sigma_1\sigma_2) = -s(\sigma_1\sigma_2) \Rightarrow s(\tau\pi) = -s(\pi)$

Posledica: Naj bo $\pi \in S_n$ produkt transpozicij $\pi = \tau_1\tau_2\dots\tau_k$. Potem je $s(\pi) = (-1)^k$

Dokaz. Po trditvi je $s(\pi) = s(\tau_1\tau_2\dots\tau_k) =$
$= (-1)s(\tau_2\dots\tau_k) = (-1)(-1)s(\tau_3\dots\tau_k) =$
$= \dots = (-1)^k$ ∎

$s(\pi) = 1$, π je soda permutacija
$s(\pi) = -1$, π je liha permutacija

Produkt sodih permutacij je soda permutacija.

$\pi = \tau_1\dots\tau_k \Rightarrow \pi^{-1} = \tau_k\tau_{k-1}\dots\tau_1$

$\Rightarrow$ Inverz sode permutacije je soda permutacija.

Torej je množica sodih permutacij reda n podgrupa grupe S_n. (imenujemo jo alternirajoča grupa reda n - znak: A_n)

$A_n = \{\pi \in S_n : s(\pi) = 1\}$

Ima $\frac{n!}{2}$ elementov. (za $n > 1$)

Abelove grupe

(= komutativne grupe)

$(G, +)$ ← znak za operacijo v Abelovi grupi

0 - nevtralni element

$a \in G$, $-a$ nasprotni element (= inverz)

$a + (-a) = (-a) + a = 0$

Abelova: $a + b = b + a \quad \forall a, b \in G$

$$\underbrace{a + a + \ldots + a}_{n \in \mathbb{N}} \equiv na$$

$$\underbrace{(-a) + (-a) + \ldots + (-a)}_{n \in \mathbb{N}} \equiv -na$$

iz $\mathbb{Z} \rightarrow 0a \equiv 0 \leftarrow$ iz G

$\mathbb{Z} \times G \longrightarrow G$ množenje s celim številom

$(n, a) \longmapsto na$, $n \in \mathbb{Z}$, $a \in G$

$a + (-b) \equiv a - b$

Primer: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$

$H \subseteq G$ Abelova grupa

H podgrupa

$a \sim b \overset{\text{def.}}{\iff} a - b \in H$ ← ni nujno, da je grupa Abelova

$\sim$ je ekvivalenčna rel. v G

1. refl. $a \sim a$? $0 \in H$ - velja!

dokazujemo, da je ~ ekvivalenčna relacija

2. simetričnost

$a \sim b \Rightarrow b \sim a$?

$a - b \in H \Rightarrow b - a \in H$?

H zaprta za invertiranje!

$a - b \in H \Rightarrow \underbrace{-(a-b)}_{b-a} \in H$

3. tranzitivnost

$(a \sim b,\ b \sim c) \Rightarrow a \sim c$?

$\left.\begin{array}{l} a - b \in H \\ b - c \in H \end{array}\right\} \Rightarrow a - c \in H$?

$a - c = \underbrace{(a-b)}_{\in H} + \underbrace{(b-c)}_{\in H} \in H$

(zaprtost H za seštevanje!)

Ali je relacija ~ usklajena s seštevanjem?

$\left.\begin{array}{l} x \sim a \\ y \sim b \end{array}\right\} \Rightarrow x + y \sim a + b$ (usklajenost)

$\left.\begin{array}{l} x - a \in H \\ y - b \in H \end{array}\right\} \Rightarrow (x+y) - (a+b) \in H$ (?)

uporabimo komutativnost

$(x+y) - (a+b) = \underbrace{(x-a)}_{\in H} + \underbrace{(y-b)}_{\in H} \in H$ ✓

(zaprtost H za seštevanje)

Zaradi usklajenosti lahko seštevanje prenesemo na kvocientno množico $G/_\sim$.

$G/_\sim \equiv G/_H \qquad G/_H = \{[a] : a \in G\}$

$(G/H, +)$ seštevanje $+$ uvedemo s predpisom

$$[a] + [b] = [a+b]$$

$+$ je operacija na G/H (zaradi usklajenosti ...)

Velja: $(G/H, +)$ je Abelova grupa

1) asociativnost seštevanja v G/H sledi iz asociativnosti seštevanja v G

2) nevtralni el. v G/H je $[0]$

3) $[a] \in G/H$

nasprotni (inverzni) el. tega elementa je $[-a]$

4) komutativnost: $[a] + [b] = [a+b]$

$$[b] + [a] = [b+a]$$

Primer: $(G, +) = (\mathbb{Z}, +)$

$$H = n\mathbb{Z} \equiv \{ n \cdot k : k \in \mathbb{Z} \}, \quad n \in \mathbb{N}$$

$$n\mathbb{Z} = \{ \ldots, -2n, -n, 0, n, 2n, \ldots \}$$

podgrupa

$$\mathbb{Z}/_{n\mathbb{Z}} \equiv \mathbb{Z}_n$$

$$[m] = \{ x \in \mathbb{Z} : x \sim m \}$$

$$x - m \in n\mathbb{Z} \qquad n \mid x - m$$

= množica celih števil, ki pri deljenju z n dajejo isti ostanek kot m

k ostanek pri deljenju m z n

$\Rightarrow [m] = [k]$

$\{[0], [1], \dots, [n-1]\} = \mathbb{Z}_n$

$\{ 0, 1, \dots, n-1 \}$

ura koti (stopinjski)

$\mathbb{Z}_n$ je grupa ostankov pri deljenju z n

$n = 5$ $\{0, 1, 2, 3, 4\}$

$3+4 = 2$ $2+3 = 0$

Kolobar

Množica K skupaj z operacijama $+$ (seštevanje) in $\cdot$ (množenje) je kolobar, kadar velja:

(1) $(K, +)$ je Abelova grupa

(2) $(K, \cdot)$ je polgrupa (= množenje je asociativno)

(3) $a(b+c) = ab + ac$

$(a+b)c = ac + bc$ $\forall a, b, c \in K$

distributivnost (z leve in desne)

distributivnostna zakona

K je komutativen, kadar velja $ab = ba$ $\forall a, b \in K$

K ima enoto (ali enico), kadar ima $(K, \cdot)$ enoto; $(e \in K)$ $1 \in K$

$ea = ae = a$ $\forall a \in K$

$1a = a1 = a$ -ll-

Kolobar $(K, +, \cdot)$ je obseg, kadar je $K \setminus \{0\}$ grupa. Enota v tej grupi $1 \in K \setminus \{0\}$.

$\{0,1\}$ je najmanjši obseg

$\mathbb{Z}_2$

Primeri: $(\mathbb{Z},+,\cdot)$ običajni operaciji
= komutativen kolobar z enoto 1

$(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$

$K = F(M,\mathbb{R})$, $M \neq \emptyset$

$f \in F(M,\mathbb{R})$, tj. $f : M \to \mathbb{R}$

$(f+g)(x) = f(x) + g(x)$, $f,g \in K$, $x \in M$

$(f \cdot g)(x) = f(x) \cdot g(x)$, -"-

$(K,+,\cdot)$ je komutativen kolobar z enoto

$K = \mathbb{R}^3$, $+$: po komponentah

$(x,y,z)\cdot(a,b,c) = (xa,\ xb+yc,\ zc)$

$(K,+,\cdot)$ je kolobar

K ima enoto! $1 = (1,0,1)$

$(1,1,0)\cdot(0,1,1) = (0,2,0)$

$(0,1,1)\cdot(1,1,0) = (0,0,0)$

$\Downarrow$

K ni komutativen

$(\mathbb{Z}_n,+,\cdot)$ kolobar ostankov pri deljenju z n $(n \in \mathbb{N})$

$\{0,1,\dots,n-1\}$

$\mathbb{Z}_6$; $4\cdot 2 = 2$, $5^2 = 1$, $2\cdot 3 = 0$

2, 3 - delitelja niča

$\mathbb{Z}_n$ - kateri elementi so delitelji niča?

Nekaj preprostih lastnosti kolobarja:

(1)	$0 \cdot a = a \cdot 0 = 0 \quad \forall a \in K$
(2)	$(-a)b = -ab$
	$(-a)(-b) = a \cdot b$

Dokaz (1): $0 \cdot a = x$

$$x + x = 0 \cdot a + 0 \cdot a = \underbrace{(0+0)}_{0} \cdot a = 0 \cdot a = x$$

(distributivnost)

$$x + x = x \mid + (-x)$$

$$x = 0 \quad \Rightarrow \quad 0 \cdot a = 0$$

Podobno: $a \cdot 0 = 0$

Dokaz (2):

$$(-a) \cdot b + a \cdot b = (-a + a) \cdot b = 0 \cdot b \overset{(1)}{=} 0$$

(distributivnostni zakon)

$$\Rightarrow (-a) \cdot b = -a \cdot b$$

$(K, +, \cdot)$ obseg

1 - enica (enota)

$(K \setminus \{0\}, \cdot)$ grupa

$a \in K, \ a \neq 0 \Rightarrow \exists a^{-1} \in K$

$(a \cdot a^{-1} = a^{-1} \cdot a = 1)$

Velja: $ab = ac \ldots a \neq 0 \Rightarrow b = c$ ("krajšanje")

$$a^{-1} \cdot \mid \ ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac)$$

$$(a^{-1} \cdot a)b \qquad (a^{-1} \cdot a) \cdot c$$

$$\Rightarrow \underbrace{1 \cdot b}_{b} = \underbrace{1 \cdot c}_{c}$$

Obseg nima deliteljev ničla:

$ab = 0$
$a \neq 0,\ b \neq 0$
a del. ničla

$a^{-1}(ab) = a^{-1} \cdot 0 = 0$ (inverz za množenje)
$(a^{-1}a)\,b = 1 \cdot b = b$

$\mathbb{Z}_p$ - p praštevilo ; $\mathbb{Z}_p$ je obseg ni deliteljev ničla

$f : K_1 \longrightarrow K_2$ homomorfizem
$f(a+b) = f(a) + f(b)$
$f(a \cdot b) = f(a) \cdot f(b)$

Vektorski prostor

Vektorski prostor V nad obsegom O je Abelova grupa $(V, +)$ skupaj z zunanjo operacijo $O \times V \to V$. ($(\alpha, v) \longmapsto \alpha v$, množenje s skalarjem), ki ustreza pogojem:

(1) $(\alpha + \beta)v = \alpha v + \beta v$; $\alpha, \beta \in O$, $v \in V$
(2) $\alpha(u+v) = \alpha u + \alpha v$; $\alpha \in O$, $u, v \in V$
(3) $\alpha(\beta v) = (\alpha\beta)v$; $\alpha, \beta \in O$, $v \in V$
(4) $1 \cdot v = v$; $1 \in O$ (enica), $v \in V$

↖ tega pogoja lahko tudi ne bi bilo ???

Primeri vekt. prostorov

$\mathbb{R}^3$: seštevanje in množenje s skalarji - po komponentah

$\mathbb{R}^2$, $\mathbb{R}$ (vsi nad obsegom $\mathbb{R}$)

$\mathcal{U} = \mathbb{R}$ → realen vekt. prostor
$\mathcal{U} = \mathbb{C}$ → kompleksen vekt. prostor

$\mathcal{O}$ obseg (običajno komutativen)

$\mathcal{O}^n = \{ (\alpha_1, \alpha_2, \dots, \alpha_n) : \alpha_i \in \mathcal{O} \ \forall i \}$

operacije definiramo po komponentah:

$(\alpha_1, \alpha_2, \dots, \alpha_n) + (\beta_1, \beta_2, \dots, \beta_n) = (\alpha_1+\beta_1, \alpha_2+\beta_2, \dots, \alpha_n+\beta_n)$

$\gamma(\alpha_1, \alpha_2, \dots, \alpha_n) = (\gamma\alpha_1, \gamma\alpha_2, \dots, \gamma\alpha_n)$

$\mathcal{O}^n$ je s temi operacijami vekt. prostor nad obsegom $\mathcal{O}$

V vektorski prostor nad $\mathcal{O}$:

$(V, +)$ Abelova grupa

$\alpha, \beta \in \mathcal{O}$

$x, y \in V$

$\alpha(x+y) = \alpha x + \alpha y$

$(\alpha+\beta)x = \alpha x + \beta x$

$\alpha(\beta x) = (\alpha\beta)x$

$1 \cdot x = x$

V ravnina v $\mathbb{R}^3$, ki vsebuje izhodišče 0

V je realen vekt. prostor

operacije vzamemo iz $\mathbb{R}^3$

Podobno velja za vsako premico ($\subset \mathbb{R}^3$), ki vsebuje 0.

Trivialni (ničelni) prostor $V = \{0\}$.

$V = F(M, \mathbb{R})$; $M \neq \emptyset$

$f \in V \overset{def.}{\iff} f : M \to \mathbb{R}$

seštevanje in množenje s skalarjem - po točkah:

$(f+g)(x) = f(x) + g(x) \qquad x \in M$

$(\alpha \cdot f)(x) = \alpha \cdot f(x) \qquad \alpha \in \mathbb{R}, x \in M$

$f, g \in V$

V je realen vektorski prostor.

Lastnosti (nekaj najosnovnejših):

(1) $0 \cdot x = 0 \quad \forall x \in V$

(0 NV 0; 0 NV V)

(2) $\alpha \cdot 0 = 0 \quad \forall \alpha \in \mathbb{O}$

(0 NV V)

(3) $(-1)x = -x \quad \forall x \in V$

(4) $\alpha \cdot x = 0 \Rightarrow \alpha = 0$ ali $x = 0$
$(\alpha \in \mathbb{O},\ x \in V)$

Dokaz:

(1) $0 \cdot x = y$

$y + y = \overbrace{0+0}^{0} \cdot x = 0 \cdot x + 0 \cdot x = 0 \cdot x = y$

$\Rightarrow y = 0$ ∎

(2) $\alpha \cdot 0 = z$

$z + z = \alpha \cdot \overbrace{0+0}^{0} = \alpha \cdot 0 + \alpha \cdot 0 = \alpha \cdot 0 = z$

$\Rightarrow z = 0$ ∎

(3) $x + (-1) \cdot x = 1 \cdot x + (-1) \cdot x = \underbrace{(1 + (-1))}_{0} x \overset{(1)}{=} 0$

$\Rightarrow (-1)x = -x$ ∎

(4) $\alpha \cdot x = 0, \quad \alpha \in \mathbb{O} \setminus \{0\} \Rightarrow \exists\, \alpha^{-1} \in \mathbb{O}$ in

$\alpha^{-1}(\alpha \cdot x) = \alpha^{-1} \cdot 0 \overset{(2)}{=} 0$

$\| $

$\underbrace{(\alpha^{-1} \cdot \alpha)}_{1} x = 1 \cdot x = x$ Torej $x = 0$. ∎

Vektorski podprostor

V vektorski prostor nad $\mathbb{O}$

$U \subseteq V$; Kdaj je U za „operacije iz V" vektorski prostor?

Veljati mora:

(1) $x, y \in U \Rightarrow x+y \in U$ (U zaprta za seštevanje)

(2) $x \in U \Rightarrow \alpha \cdot x \in U$ (U zaprta za množenje s skalarji)

Ti dve lastnosti zadoščata!

Le še: $x \in U \Rightarrow -x \in U$ ($-x = (-1)x \in U$, če $x \in U$)

(glej 2) (2)

Neprazna podmnožica $U \subseteq V$ je **vektorski podprostor** (vektorski podprostor V), kadar veljata za U lastnosti (1) in (2).

Tedaj je U sam zase vektorski prostor nad istim obsegom kot V.

Primeri: V vektorski prostor nad $\mathbb{O}$;

Trivialni podprostor $\{0\}$ je vektorski podprostor.

V je vektorski podprostor v. p. V.

Ravnina (oz. premica) „skozi" 0 je vektorski podprostor $\mathbb{R}^3$.

$V = F(M, \mathbb{R})$

$N \subseteq M$ $\quad U = \{f \in V : f(x) = 0 \ \forall x \in N\}$

je vektorski podprostor v. p. V.

Vekt. podprostor vsebuje vektor 0.

$U \subseteq V$; U v. podpr. $\quad \overset{''}{0}$

$U \neq \emptyset$, $\exists x \in U \overset{(2)}{\Rightarrow} 0 \cdot x \in U$

Presek v. podprostorov danega v.p. je vekt. podprostor.

Naj bo $M \subseteq V$, M podmnožica, V v.p. nad $\mathbb{O}$

Lin M = presek vseh v. podprostorov v. p. V, ki vsebujejo M

(1) Lin M je v. podprostor (v V)

(2) Lin M je vsebovan v vsakem v. podprostoru (v.p. V), ki vsebuje M (je „najmanjši" med njimi)

Imena: Lin M = linearna ogrinjača (lupina) množice M (v v.p. V)

Primeri: (1) $M = \{v\} \subset \mathbb{R}^3$, $v \neq 0$;

Lin M = premica, ki vsebuje v (in 0)

(2) $M = \{u, v\} \subset \mathbb{R}^3$, u, v lin. neodvisna

Lin M = ravnina, ki vsebuje u, v (in 0)

(3) $M = \emptyset$; $\quad$ Lin M $= \{0\}$

V v.p. nad $\mathbb{O}$, $U \subseteq V$, U v. podprostor

$u_1, u_2, u_3, \ldots, u_k \in U$ $\quad$ $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{O}$

$\Rightarrow \underbrace{\alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_k u_k}_{\text{linearna kombinacija } u_1, u_2, \ldots, u_k} \in U$

$\emptyset \neq M \subseteq V$, $v_1, v_2, \ldots, v_k \in M$

$\Rightarrow \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_k v_k \in \mathcal{L}in\, M$

Trditev $M \subseteq V$, $M \neq 0$

Potem je $\mathcal{L}in\, M$ množica vseh linearnih kombinacij vektorjev iz M.

Dokaz: Zadošča videti, da je množica vseh linearnih kombinacij vektorjev iz M vektorski podprostor.

(1) zaprtost za seštevanje (OČITNO), (2) zaprtost za množenje s skalarji (SKORAJ OČITNO)

(2) $\beta(\alpha_1 v_1 + \ldots + \alpha_k v_k) = (\beta\alpha_1)v_1 + \ldots + (\beta\alpha_k)v_k$

$v_1, \ldots, v_k \in M$

V_1, V_2 vektorska podprostora $\subseteq V$

$v \in \mathcal{L}in\,(V_1 \cup V_2) = ?$

$v = x + y$, $x \in V_1$, $y \in V_2$

velja tudi obratno:

$x \in V_1, y \in V_2 \Rightarrow x + y \in \mathcal{L}in\,(V_1 \cup V_2)$

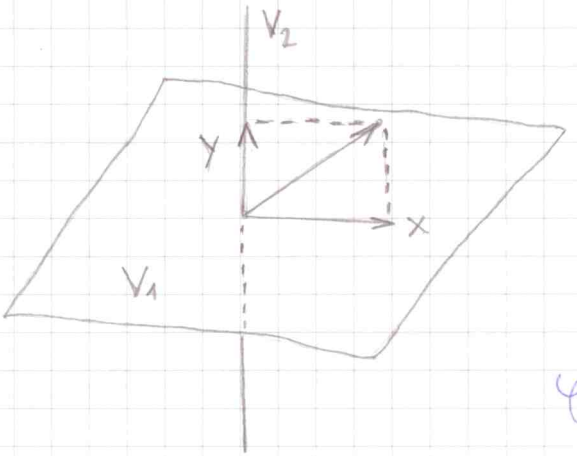
Torej velja $\boxed{\mathcal{L}in\,(V_1 \cup V_2) = V_1 + V_2}$ = vsota podprostorov

$\equiv \{ x + y : x \in V_1, y \in V_2 \}$

Vsota vektorskih podprostorov $V_1 + V_2$ je najmanjši vektorski podprostor v V, ki vsebuje V_1 in V_2.

Splošneje: $V_1 + V_2 + \ldots + V_k = \mathcal{L}in\,(\bigcup_{i=1}^{k} V_i)$

$V_1 \cup V_2 \cup \ldots \cup V_k$



V_1, V_2 vektorska podprostora

Vsota V_1+V_2 je direktna (prema), kadar velja $V_1 \cap V_2 = \{0\}$

Oznaka: $V_1 \oplus V_2$

Trditev: Vsota V_1+V_2 je direktna natanko takrat, kadar se da vsak $v \in V_1+V_2$ na en sam način zapisati v obliki $v = x+y$, $x \in V_1$, $y \in V_2$.
(x, y sta enolično določena)

Dokaz. $V_1 \oplus V_2 \Rightarrow v = x+y$, $x \in V_1$, $y \in V_2$

$v \in V_1+V_2$

enoličnost: $v = x'+y'$, $x' \in V_1$, $y' \in V_2$

$\Rightarrow x'+y' = x+y$

$x-x' = y'-y$ – ta element leži v $V_1 \cap V_2 = \{0\}$

$x \in V_1$, $y \in V_2$

$\Rightarrow x-x' = y'-y = 0$

$\Rightarrow x' = x$, $y' = y$

(2) enoličnost $\Rightarrow$ direktna vsota

Trdimo, da je $V_1 \cap V_2 = \{0\}$ ...

$z \in V_1 \cap V_2$

$z = z + 0 = 0 + z$

$z \in V_1$, $0 \in V_2$, $0 \in V_1$, $z \in V_2$

Torej $V_1 \cap V_2 = \{0\}$.

enoličnost $\Rightarrow z = 0$.

Preslistaj nazaj na oznako 11.12.2007 (1)

11.12.2007 (1)

V v. p. nad $\mathbb{O}$

$V_1, V_2, \dots, V_m$ v. podprostori $(\subseteq V)$

Def. V je direktna vsota podpr. $V_1, \dots, V_m$, kadar za vsak $v \in V$ obstajajo natanko določeni vektorji $v_1, \dots, v_m \in V$, tako da velja

$$v = v_1 + \dots + v_m, \quad v_i \in V_i, \quad i = 1, \dots, m$$

Primer $\mathbb{R}^3 = \underbrace{\mathbb{R}\vec{i}}_{x\text{-os}} \oplus \underbrace{\mathbb{R}\vec{j}}_{y\text{-os}} \oplus \underbrace{\mathbb{R}\vec{k}}_{z\text{-os}}$

Označka za dir. vsoto:

$V_1 \oplus V_2 \oplus \dots \oplus V_m$

$(V = V_1 \oplus V_2 \oplus \dots \oplus V_m)$

Kvocientni vektorski prostor

v. p. $V \supseteq U$ v. podprostor

$v_1 \sim v_2 \overset{\text{def.}}{\iff} v_1 - v_2 \in U$

($\sim$ je ekvivalenčna relacija)

$V/_\sim \equiv V/U$ (= kvoc. grupa za sešt.)

$[v] \in V/U, \quad v \in V$

$[v] = v + U \quad (\text{ali } U + v)$

sešt.: $[v_1] + [v_2] = [v_1 + v_2]$

množ. s skal.: $\alpha[v] = [\alpha v], \alpha \in \mathbb{O}, v \in V$

(je dobro def.)

$[v'] = [v] \overset{(2)}{\Rightarrow} [\alpha v'] = [\alpha v]$

Pojdi nekaj strani naprej na oznako 11.12.2007 (2)

$[v] = [v'] \Rightarrow v \sim v' \Rightarrow v - v' \in U \Rightarrow$
$\Rightarrow \alpha(v - v') \in U \Rightarrow \alpha v \sim \alpha v' \Rightarrow [\alpha v] = [\alpha v']$

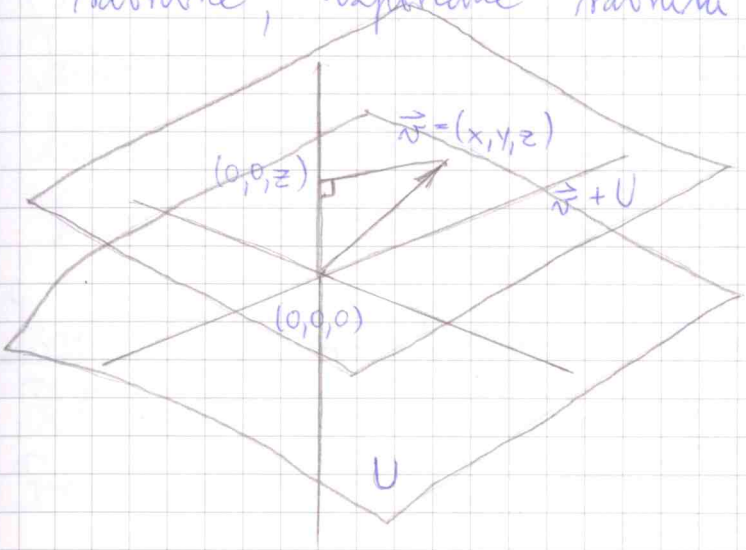
S tema dvema operacijama V/U postane vektorski prostor (nad $\mathbb{O}$).

Primer: $V = \mathbb{R}^3$ $U = \mathbb{R}^2 \times \{0\}$ (ravnina $z = 0$)

$V/U = ?$ $[v] = v + U$

$[(x, y, z)] = \{(a, b, z) : a, b \in \mathbb{R}\}$

Ekvivalenčni razredi (torej el. iz V/U) so ravnine, vzporedne ravnini $z = 0$.



$[(x, y, z)] = [(0, 0, z)]$

Homomorfizmi vekt. prostorov

U, V vekt. prostora nad $\mathbb{O}$

Def. Presl. $A : V \to U$ je *homomorfizem v. p.* (oz. *linearna*), kadar velja:

(1) $A(x+y) = Ax + Ay$ (*aditivnost*);
(2) $A(\alpha x) = \alpha Ax$ (*homogenost*);

$x, y \in V$ $\alpha \in \mathbb{O}$

$A: V \to U$ linearna

Velja $A0 = 0$ (sledi iz (1) in iz (2) $\alpha = 0$)

* $A(x-y) = Ax - Ay$
* $A(-z) = -A(z)$ $(\alpha = -1)$

(• in aditivnost) $\Rightarrow$ (*)

$A(\alpha x + \beta y) \overset{(1)}{=} A(\alpha x) + A(\beta y) \overset{(2)}{=}$
$\overset{(2)}{=} \alpha Ax + \beta Ay$

A ohrani linearno kombinacijo

$$A(\alpha_1 v_1 + \ldots + \alpha_m v_m) = \alpha_1 A v_1 + \ldots + \alpha_m A v_m$$

$\alpha_i \in O$, $v_i \in V$ $(\forall i)$

$A: V \to U$ linearna

ker $A = \{ v \in V : Av = 0 \}$ jedro

im $A = \{ Av : v \in V \}$ slika / image

ker A je podprostor domene V

im A je " kodomene U

zaprtost za sešt. in množ. s skal.

(le za jedro):

(1) $v_1, v_2 \in \ker A \Rightarrow A(v_1 + v_2) = Av_1 + Av_2 = 0$
($Av_1 = 0$, $Av_2 = 0$)

$\Rightarrow v_1 + v_2 \in \ker A$

(2) $v \in \ker A \Rightarrow A(\alpha v) = \alpha Av = 0$
($Av = 0$)

$\Rightarrow \alpha v \in \ker A$

$\mathcal{A}$ surjekcija $\Leftrightarrow$ $\operatorname{im}\mathcal{A} = U$

$\mathcal{A}$ injekcija $\Leftrightarrow$ $\ker\mathcal{A} = \{0\}$

($\Rightarrow$): $\mathcal{A}0 = 0 \Rightarrow 0 \in \ker\mathcal{A}$

$\mathcal{A}$ injekcija, $v \in \ker\mathcal{A}$ $\Rightarrow$ $v = 0$ Torej $\ker\mathcal{A} = \{0\}$.

($\Leftarrow$): $v_1, v_2 \in V$, $\mathcal{A}v_1 = \mathcal{A}v_2 \Rightarrow$

$\Rightarrow \mathcal{A}(v_1 - v_2) = \mathcal{A}v_1 - \mathcal{A}v_2 = 0$

$\Rightarrow v_1 - v_2 \in \ker\mathcal{A} = \{0\} \Rightarrow v_1 - v_2 = 0$

$\Rightarrow v_1 = v_2$ Torej je $\mathcal{A}$ injektivna.

Izomorfizem v.p. je bijektiven homomorfizem, torej bijektivna linearna preslikava (linearna bijekcija).
Inverz izomorfizma je izomorfizem.

Izrek: Naj bo $\mathcal{A}: V \to U$ linearna
Potem sta vekt. prostora $V/\ker\mathcal{A}$ in $\operatorname{im}\mathcal{A}$ izomorfna.
Preslikava $\Phi: V/\ker\mathcal{A} \to \operatorname{im}\mathcal{A}$,
definirana s predpisom $\Phi([v]) = \mathcal{A}v$, je izomorfizem.

Dokaz: Φ je dobro definirana

$[v'] = [v] \Rightarrow v' \sim v \Rightarrow v' - v \in \ker\mathcal{A} \Rightarrow$

$\Rightarrow \mathcal{A}(v' - v) = 0 \Rightarrow \mathcal{A}v' = \mathcal{A}v$.

$\mathcal{A}v' - \mathcal{A}v$

Φ je homomorfizem (je linearna):

$\Phi([v_1] + [v_2]) = \Phi([v_1 + v_2]) = \mathcal{A}(v_1 + v_2) =$

$= \mathcal{A}v_1 + \mathcal{A}v_2 = \Phi([v_1]) + \Phi([v_2])$ (adit.)

$\Phi(\alpha[v]) = \Phi([\alpha v]) = \mathcal{A}(\alpha v) = \alpha \mathcal{A}v = \alpha \Phi([v])$ (homogenost)

Φ je bijekcija:

(1) Φ je surjekcija - razvidno iz definicije Φ

(2) Φ je injekcija: $\Phi([v_1]) = \Phi([v_2]) \Rightarrow$

$\Rightarrow \mathcal{A}v_1 = \mathcal{A}v_2 \Rightarrow \mathcal{A}(v_1 - v_2) = \mathcal{A}v_1 - \mathcal{A}v_2 = 0$

$\Rightarrow v_1 - v_2 \in \ker \mathcal{A} \Rightarrow v_1 \sim v_2 \Rightarrow$

$\Rightarrow [v_1] = [v_2]$. □

$\mathcal{A}: V \to U$ linearna $\Rightarrow V/\ker \mathcal{A}$ in $\operatorname{im} \mathcal{A}$ sta izomorfna

Primer: $V = U = \mathbb{R}^3$

$\mathcal{A}: \mathbb{R}^3 \to \mathbb{R}^3$

$\mathcal{A}(x, y, z) = (0, 0, z)$

$\mathcal{A}$ - pravokotna projekcija na z-os

$\ker \mathcal{A}$ = ravnina $z = 0$ $(= V_1)$

$\operatorname{im} \mathcal{A}$ = z-os $(= V_2)$

$V/V_1 \cong V_2$ (↑ znak za izomorfnost)

velja: $V_1 \oplus V_2 = V$

V, U vektorska prostora nad $\mathbb{O}$ ($\mathbb{O}$ je komutativen)

$\mathcal{L}(V, U)$ - množ. vseh lin. preslikav $V \to U$

vpeljemo seštevanje („po točkah"):

$\mathcal{A}, \mathcal{B} \in \mathcal{L}(V, U)$

$(\mathcal{A}+\mathcal{B})v = \mathcal{A}v + \mathcal{B}v \quad \forall\, v \in V$

množ. s skalarji („po točkah"):

$(\alpha\mathcal{A})v = \alpha(\mathcal{A}v) \quad \forall\, \alpha \in \mathbb{O} \;\forall\, v \in V$

$\mathcal{L}(U,V)$ je s tema operacijama vekt. prostor (nad $\mathbb{O}$)

Ničelni element je ničelna preslikava $\mathcal{O}$, ki slika po pravilu $\mathcal{O}v = 0 \quad \forall\, v \in V$.

Nasprotni element: $(-\mathcal{A})v = -\mathcal{A}v \quad \forall\, v \in V$

(oznaka za preslikavo)

$\mathcal{L}(V) \equiv \mathcal{L}(V,V)$

↑ prostor endomorfizmov vektorskega prostora V

Množenje v $\mathcal{L}(V)$ ≡ komponiranje

$(\mathcal{A}\mathcal{B})v = \mathcal{A}(\mathcal{B}v) \qquad \mathcal{A},\mathcal{B} \in \mathcal{L}(V),\ v \in V$

$(\mathcal{L}(V), +, \cdot)$ je kolobar

$\mathcal{L}(V)$ je vektorski prostor nad $\mathbb{O}$ in $(\alpha\mathcal{A})\mathcal{B} = \mathcal{A}(\alpha\mathcal{B}) = \alpha(\mathcal{A}\mathcal{B})$ $(\forall\, \alpha \in \mathbb{O})$

} $\mathcal{L}(V)$ je algebra nad obsegom $\mathbb{O}$

Def: **Algebra** A nad obsegom (komutativnim) $\mathbb{O}$ je vektorski prostor nad $\mathbb{O}$, ki je za množenje in seštevanje tudi kolobar, hkrati pa velja pogoj

$(\alpha a)b = a(\alpha b) = \alpha(ab)$

za $\forall\, \alpha \in \mathbb{O}$ in $\forall\, a, b \in A$.

Primer 1: $\mathcal{L}(V)$ je nekomutativna algebra ...

Primer 2: $F(M, \mathbb{R})$ vektorski prostor realnih

funkcij $M \to \mathbb{R}$ (nad $\mathbb{R}$) z množenjem (def. po točkah) je komutativna algebra.

$f, g \in F(M, \mathbb{R})$

$(f+g)(x) = f(x) + g(x)$ $\quad (f \cdot g)(x) = f(x) \cdot g(x)$

$(\alpha f)(x) = \alpha f(x)$ $\quad x \in M, \ \alpha \in \mathbb{R}$

Vse algebre imajo enoto (za množenje; navaja se na kolobar).

(1) enota je id_V

(2) enota je funkcija $x \longmapsto 1 \quad \forall x \in M$