

LINEARNA ALGEBRA 2020/21
13. VAJE: 28. 12. 2020

1. Naj bo p praštevilo. Vzemimo $x, y \in \mathbb{Z}_p[x, y]$ pokaži, da je $(x + y)^p = x^p + y^p$. Po
Poišči primer, ko p ni praštevilo in enakost ne velja.
2. Določi vse homomorfizme kolobarjev $\mathbb{Z}_6 \rightarrow \mathbb{Z}_{26}$.
3. Klasificiraj vektorske podprostore $\mathbb{R}^3$.
4. Ali je – vektorski podprostor v – ?
 - a.) $U = \left\{ \begin{bmatrix} a & \\ & -a \end{bmatrix} \mid a \in \mathbb{R} \right\}$ v $\mathbb{R}^{2 \times 2}$.
 - b.) $V = \left\{ \begin{bmatrix} a & 1 \\ & a \end{bmatrix} \mid a \in \mathbb{R} \right\}$ v $\mathbb{R}^{2 \times 2}$.
 - c.) $W = \{p \in \mathbb{R}_n[x] \mid p(x) = p(-x)\}$ v $\mathbb{R}_n[x]$.
 - d.) $W = \{p \in \mathbb{R}_n[x] \mid p \text{ ima vsaj eno realno ničlo}\}$ v $\mathbb{R}_n[x], n \geq 2$.
5. Pokaži, da je $\{(1, 2, 3, 4)^T, (-2, 1, 0, 1)^T, (1, 0, 1, 1)^T, (2, -1, 0, 3)^T\}$ baza $\mathbb{R}^4$.
6. Naj bo $U = \text{Lin}\{(2, 3, -1, 4)^T, (1, 2, 1, 2)^T, (4, 7, 1, 8)^T, (1, 1, -2, 2)^T\}$. Določi $\dim U$
in kakšno bazo.
7. Poišči vse baze $\mathbb{Z}_2$ -vektorskega prostora $\mathbb{Z}_2^3$ in $\mathbb{Z}_3$ -vektorskega prostora $\mathbb{Z}_3^3$.

1. Naj bo p praštevilo. Vzemimo $x, y \in \mathbb{Z}_p[x, y]$ pokaži, da je $(x + y)^p = x^p + y^p$. Po
Poišči primer, ko p ni praštevilo in enakost ne velja.

$$\mathbb{Z}_p = \{0, 1, 2, 3, 4, 5\}$$

$\mathbb{Z}_p[x, y]$ polinomi s spremenljivkama x, y in koeficienti v $\mathbb{Z}_p$
 $xy = yx$

$$(x + y)^p = \sum_{i=0}^p \binom{p}{i} x^i y^{p-i} \quad \leftarrow \text{za ta rezultat potrebujemo } xy = yx$$

$i \neq 0, p$ Pokazati želim, da $p \mid \binom{p}{i}$, če je $i \neq 0, p$
 $p! = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n} \cdot p^k$ $k=1$, če je $k > 1$ potem $p \mid (p-1)!$ $\leftarrow$ vsi praštevilski faktorji so manjši od p
 p je tvoj $(p-i)!i!$ - vsi praštevilski faktorji so manjši od p .

Lema
če je $\gcd(a, b) = 1$ in $a \mid b \cdot c$, potem $a \mid c$

Pokaz
 $xa + yb = 1$ $b \cdot c = k \cdot a$
 $xa \cdot c + yb \cdot c = c$ $c = (xc + yk) \cdot a$
 $\left(\begin{smallmatrix} xc \\ k \cdot a \end{smallmatrix} \right)$

Alternativno

Primajmo praštevilske razcepe.

$$(p-i)!i \mid p! \xrightarrow{\text{lema}} (p-i)!i! \mid (p-1)! \Rightarrow \frac{(p-1)!}{(p-i)!i!} \in \mathbb{Z} \Rightarrow p \mid \binom{p}{i}$$

$$\binom{p}{i} \equiv 0 \pmod{p} \rightarrow (x + y)^p = x^p + y^p$$

Za $\mathbb{Z}_4$ to ne velja!

$$(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4 \equiv x^4 + 2x^2y^2 + y^4 \pmod{4}$$

2. Določi vse homomorfizme kolobarjev $\mathbb{Z}_6 \rightarrow \mathbb{Z}_{26}$.

R_1, R_2 kolobarja

$$f: R_1 \rightarrow R_2$$

$$\left. \begin{aligned} f(x+y) &= f(x) + f(y) \\ f(x \cdot y) &= f(x) \cdot f(y) \end{aligned} \right\} \text{homomorfizem}$$

(Nekateri avtorji zahtevajo tudi $f(1)=1$)

homomorfizem kolobarjev je
tudi homomorfizem ab. grup.

$$f: \mathbb{Z}_6 \rightarrow \mathbb{Z}_{26}$$

Naj bo f netrivialen homomorfizem. $f(1)=13$ (glej Vaje 11 udloga 7)

$$f(1) = f(1 \cdot 1) = f(1) \cdot f(1) = 13 \cdot 13 = 169 = 26 \cdot 6 + 13 \equiv 13 \pmod{26}$$

$$f(n \cdot m) = n \cdot m \cdot f(1) = n \cdot m \cdot f(1) \cdot f(1) = n \cdot f(1) \cdot m \cdot f(1) = f(n) \cdot f(m).$$

Primer grupnega homomorfizma $f: \mathbb{Z}_5 \rightarrow \mathbb{Z}_5$, ki ni homomorfizem kolobarjev

$$f(0)=0, f(1)=4, f(2)=3, f(3)=2, f(4)=1$$

$$4 = f(1) = f(1 \cdot 1) = f(1) \cdot f(1) = 4 \cdot 4 = 16 \equiv 1 \pmod{5} \quad 4 \not\equiv 1 \pmod{5}$$

Vektorski prostori

F -polje (komutativni obseg)
(asociativni) skalor $\neq$ enoto, kjer je vsak neničen element obrnljiv

V -vektorsko polje nad F

$(V, +)$ - abelova grupa

$\cdot : (F \times V) \rightarrow V$ skalarno množenje

i) $\alpha(v+w) = \alpha v + \alpha w \quad \forall \alpha \in F, \forall v, w \in V$

ii) $(\alpha+\beta)(v) = \alpha v + \beta v \quad \forall \alpha, \beta \in F, v \in V$

iii) $(\alpha\beta)v = \alpha(\beta v) \quad \forall \alpha, \beta \in F, v \in V$

iv) $1 \cdot v = v$

Primeri :

$$F^n = \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \mid x_i \in F \right\}$$

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{bmatrix}$$

$$\alpha \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \alpha x_1 \\ \vdots \\ \alpha x_n \end{bmatrix}$$

$F[x]$ - polinomi

$\vdots$

V v.p. in $U \subseteq V$. U je vektorski podprostor, če je :

$\bullet \forall u_1, u_2 \in U \Rightarrow u_1 + u_2 \in U$

$\bullet \forall u \in U \forall \alpha \in F \Rightarrow \alpha u \in U$

3. Klasificiraj vektorske podprostore $\mathbb{R}^3$.

$\bullet \dim U = 0$

$U = \{0\}$

$\bullet \dim U = 1$

$\downarrow$ elementarne baze
 U ima bazo uoči 1 $b \in V$

$U = \{ \alpha \cdot b \mid \alpha \in F \}$

$\rightarrow$ podprostori dimenzije 1 so premice, ki potekajo skozi izhodišče.

• $\dim V = 2$

V ima bazo z dvema elementoma b_1, b_2

$$V = \{ \alpha b_1 + \beta b_2 \mid \alpha, \beta \in \mathbb{R} \}$$

→ ravnina, ki vsebuje izhodišče

• $\dim V = 3$

$$V = \mathbb{R}^3 - \text{vektorski prostor}$$

4. Ali je – vektorski podprostor v – ?

a.) $U = \left\{ \begin{bmatrix} a \\ -a \end{bmatrix} \mid a \in \mathbb{R} \right\} \subset \mathbb{R}^{2 \times 2}.$

b.) $V = \left\{ \begin{bmatrix} a & 1 \\ a \end{bmatrix} \mid a \in \mathbb{R} \right\} \subset \mathbb{R}^{2 \times 2}.$

c.) $W = \{ p \in \mathbb{R}_n[x] \mid p(x) = p(-x) \} \subset \mathbb{R}_n[x].$

d.) $W = \{ p \in \mathbb{R}_n[x] \mid p \text{ ima vsaj eno realno ničlo} \} \subset \mathbb{R}_n[x], n \geq 2.$

a) $U \subseteq \mathbb{R}^{2 \times 2} (= M_2(\mathbb{R}))$

U je podprostor

$$\begin{bmatrix} a \\ -a \end{bmatrix} + \begin{bmatrix} b \\ -b \end{bmatrix} = \begin{bmatrix} a+b \\ -(a+b) \end{bmatrix}$$

$$\alpha \begin{bmatrix} a \\ -a \end{bmatrix} = \begin{bmatrix} \alpha a \\ -\alpha a \end{bmatrix}$$

Alternativno

$$U = \left\{ \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \mid x_1 + x_4 = 0, x_2 = x_3 = 0 \right\}$$

$U \rightarrow$ prostor rešitev homogenega sistema lin. enačb.

b) Ni podprostor

$$\begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix} + \begin{bmatrix} b & 1 \\ 0 & b \end{bmatrix} = \begin{bmatrix} a+b & 2 \\ 0 & a+b \end{bmatrix} \notin V$$

$$F_n[X] = \left\{ \sum_{i=0}^n a_i x^i \mid a_i \in F \right\}$$

polinomi stopnje največ n .

c) $\mathcal{W}$ je podprostor

$$\alpha p(x) = \left(\alpha \sum a_i x^i = \sum a_i (-1)^i x^i \right) = \alpha p(-x)$$

$p, q \in \mathcal{W}$

$$(p+q)(x) = p(x) + q(x) = p(-x) + q(-x) = (p+q)(-x)$$

d) $\mathcal{N}$ je podprostor

$$\alpha \cdot 0 \in \mathcal{N} \quad p(0) = 0 \quad \alpha p(0) = \alpha \cdot 0 = 0 \quad \checkmark$$

$$(x-1) \in \mathcal{N} \quad -x \in \mathcal{N} \quad (x-1) - x = -1 \notin \mathcal{N}$$

Baze

$B \subseteq V$ je baza, če je I III ogrodje in linearno neodvisna.

$$\text{I)} \quad \forall x \in V \quad \exists b_1, \dots, b_n \in B \quad \alpha_1, \dots, \alpha_n \in F \quad x = \sum_{i=1}^n \alpha_i b_i$$

$$\text{II)} \quad \forall \{b_1, \dots, b_n\} \subseteq B \quad \sum_{i=1}^n \alpha_i b_i = 0 \Rightarrow \alpha_i = 0 \quad \forall i=1, \dots, n$$

za vsako končno podmnožico.

Če je $B = \{b_1, \dots, b_n\}$ končna množica se stvari malo poenostavijo

$$\text{I)} \quad \forall x \in V \quad \exists \alpha_1, \dots, \alpha_n \quad x = \sum \alpha_i b_i$$

$$\text{II)} \quad \sum_{i=1}^n \alpha_i b_i = 0 \Rightarrow \alpha_i = 0 \quad \forall i=1, \dots, n$$

Če sta B_1, B_2 bazi V , potem je $|B_1| = |B_2|$. $\dim V = |B|$, kjer je B poljubna baza.

5. Pokaži, da je $\{(1, 2, 3, 4)^T, (-2, 1, 0, 1)^T, (1, 0, 1, 1)^T, (2, -1, 0, 3)^T\}$ baza $\mathbb{R}^4$.

i) če je X ogradje v.p. V , potem je $|X| \geq \dim V$

ii) če je X lin. neodvisna, potem je $|X| \leq \dim V$

• Če sta izpolnjeni dva pogoja, potem je tudi tretji:

1) X je ogradje 2) X je baza 3) $|X| = \dim V$

• Recimo, da poznamo kakšno bazo B . Če želimo preveriti, da je X ogradje, potem je dovolj, da vsake bazni element $b \in B$ izrazimo kot lin. kombinacijo elementov iz X .

$$\mathbb{R}^4 \text{ ima bazo } \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = e_1, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = e_2, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = e_3, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = e_4$$

Želimo pokazati, da obstajajo α_{ij} , da bo $\sum_{j=1}^4 \alpha_{ij} v_j = e_i$

Matrični zapis

$$\forall i: \begin{bmatrix} v_1 & v_2 & v_3 & v_4 \end{bmatrix} \begin{bmatrix} \alpha_{1i} \\ \alpha_{2i} \\ \alpha_{3i} \\ \alpha_{4i} \end{bmatrix} = e_i \quad \text{ali} \quad \begin{bmatrix} v_1 & v_2 & v_3 & v_4 \end{bmatrix} \begin{bmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} & \alpha_{14} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} & \alpha_{34} \\ \alpha_{41} & \alpha_{42} & \alpha_{43} & \alpha_{44} \end{bmatrix} = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{bmatrix}$$

Zanimu nas ali ima $[v_1 \ v_2 \ v_3 \ v_4]$ inverz!

$$\det \begin{bmatrix} 1 & -2 & 1 & 2 \\ 2 & 1 & 0 & -1 \\ 3 & 0 & 1 & 0 \\ 4 & 1 & 1 & 3 \end{bmatrix} = \det \begin{bmatrix} 1 & -2 & 1 & 0 \\ 2 & 1 & 0 & 0 \\ 3 & 0 & 1 & 0 \\ 4 & 1 & 1 & 4 \end{bmatrix} = 4 \cdot \det \begin{bmatrix} 1 & -2 & 1 \\ 2 & 1 & 0 \\ 3 & 0 & 1 \end{bmatrix}$$

$$= 4 \det \begin{bmatrix} 0 & -2 & 1 \\ 2 & 1 & 1 \\ 2 & 0 & 0 \end{bmatrix} = 8 \cdot \det \begin{bmatrix} -2 & 1 \\ 1 & 1 \end{bmatrix} = 8 \cdot \det \begin{bmatrix} -3 & 0 \\ 1 & 1 \end{bmatrix}$$

$$= -3 \cdot 8 \neq 0.$$

$[v_1, v_2, v_3, v_4]$ ima invert $\Rightarrow e_1, e_2, e_3, e_4$ so lin kombinacije v_1, v_2, v_3, v_4
 $\{v_1, v_2, v_3, v_4\}$ je ograjba $|\{v_1, v_2, v_3, v_4\}| = 4 \Rightarrow$ so baza
 (Tudi lin. neodvisnost dobimo iz $\det([v_1, v_2, v_3, v_4]) \neq 0$.)

6. Naj bo $U = \text{Lin}\{(2, 3, -1, 4)^T, (1, 2, 1, 2)^T, (4, 7, 1, 8)^T, (1, 1, -2, 2)^T\}$. Določi $\dim U$ in kakšno bazo. $v_1 \quad v_2 \quad v_3 \quad v_4$

V -vp. $X \subseteq V$ poljubna množica
 $U = \text{Lin } X = \left\{ \sum_{i=1}^n d_i x_i \mid d_i \in F, x_i \in X \right\}$
 linearna ograjba - najmanjši vektorski podprostor, ki vsebuje X .

X je vedno ograjba $\text{Lin } X$. Iz ograjbe lahko vedno reberemo bazo. Možniko lažje je najti poljubno bazo.

Naj bo $A = [v_1, \dots, v_n]$, $\{v_1, \dots, v_n\} = X$, potem je $\{A \begin{bmatrix} d_1 \\ \vdots \\ d_n \end{bmatrix} \mid d_i \in F\} = \text{Lin } X$
 $\parallel$ P -obrnjena $n \times n$ matrika
 $\{AP \begin{bmatrix} d_1 \\ \vdots \\ d_n \end{bmatrix} \mid d_i \in F\}$
 Stolpci AP so še vedno ograjba

Želimo najti takšno obrnjeno $n \times n$ matriko P , da bodo začetni stolpci matrike AP linearno neodvisni, ostali pa ničelni. (Gauss po stolpcih $\rightarrow$ ker nam je bolj domač Gauss po vrsticah A transponiramo in delamo po vrsticah)

$$\begin{bmatrix} 2 & 3 & -1 & 4 \\ 1 & 2 & 1 & 2 \\ 4 & 7 & 1 & 8 \\ 1 & 1 & -2 & 2 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 2 & 1 & 2 \\ 2 & 3 & -1 & 4 \\ 4 & 7 & 1 & 8 \\ 1 & 1 & -2 & 2 \end{bmatrix} \rightsquigarrow$$

$$\begin{bmatrix} 1 & 2 & 1 & 2 \\ 0 & -1 & -3 & 0 \\ 0 & -1 & -3 & 0 \\ 0 & -1 & -3 & 0 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 2 & 1 & 2 \\ 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \left\{ \begin{bmatrix} 1 \\ 2 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 3 \\ 0 \end{bmatrix} \right\} \text{ je}$$

ograjba U + je lin neodvisno $\Rightarrow$ je baza!

$$\dim U = 2$$

Kasneje bomo videli, da je $\dim U = \text{rang } A$.

max. št. lin. neodvisnih stolpcev (vrstic) A