

LINEÁRNA ALGEBRA A GEOMETRIA

PRVÝ ROČNÍK, ZIMNÝ SEMESTER

Fakulta matematiky, fyziky a informatiky
Univerzita Komenského

OBSAH

I. Zobrazenia medzi množinami	2
II. Okruh, teleso, pole	9
III. Vektorové priestory	11
IV. Systémy lineárnych rovníc	14
V. Lineárna závislosť a nezávislosť vektorov	16
VI. Lineárne a direktné súčty	20
VII. Matice	22
VIII. Lineárne zobrazenie	26
IX. Systémy lineárnych rovníc 2	33
X. Euklidovský vektorový priestor	43

REFERENCIE

1. M.Hejný, V.Zaťko, P.Kršňák, *Geometria 1*, SPN, Bratislava, 1985.
2. T.Katriňák, M.Gavalec, E.Gedeonová, J.Smítal, *Algebra a teoretická aritmetika*, Univerzita Komenského, Bratislava, 1999.
3. G.Birkhoff, S.MacLane, *Prehľad modernej algebry*, ALFA, Bratislava, 1979.
4. A.I.Kostrikin, Y.I.Manin, *Linear Algebra and Geometry*, Gordon & Breach, New York, 1989.
5. A.K.Faddejev, J.S.Sominskij, *Zbierka úloh z vyššej algebry*, ALFA, Bratislava, 1968.
6. I.V.Proskurjakov, *Problems in Linear Algebra*, Mir, Moscow, 1978.
7. A.I.Kostrikin, *Exercises in Algebra; A Collection of Exercises in Algebra; Linear Algebra and Geometry*, Gordon & Breach, New York, 1996.

I. ZOBRAZENIA MEDZI MNOŽINAMI

Definícia 1.1. Nech A, B sú množiny. Zobrazenie z A do B je predpis, ktorý každému prvku z A priradí práve jeden prvok z B . Ak tento predpis označíme f , tak hovoríme $f : A \rightarrow B$. $f(a) = b$ znamená, že sme priradili prvku $a \in A$ $b \in B$. a je tzv. *vzor* prvku b . $f : a \rightarrow b$. $f(A)$ = obraz zobrazenia f . $Im(f)$ je obraz množiny A pri zobrazení $Im(f) = \{y \in B \mid \exists x \in A : f(x) = y\}$

Definícia 1.2. Zobrazenia $f : A \rightarrow B$, $g : A \rightarrow B$ sa rovnajú ($f = g$), ak pre $\forall a \in A$ je $f(a) = g(a)$. $f, g : \mathbb{N} \rightarrow \mathbb{N}$; $f(x) = x + x$; $g(x) = 2x$

Definícia 1.3. Nech $f : A \rightarrow B$ je zobrazenie a nech $A' \subset A$. Predpis, ktorý každému prvku $a \in A'$ priradí $f(a)$ sa nazýva *zúženie* zobrazenia f na podmnožinu A' . Označenie: $f|_{A'} : A' \rightarrow B$ a $f|_{A'}(x) = f(x)$

Definícia 1.4. $f : A \rightarrow B$ sa nazýva *surjektívne* ak $f(A) = B$. Zobrazenie $f : A \rightarrow B$ je surjektívne $\iff \forall y \in B \exists x \in A : f(x) = y$.

Definícia 1.5. Zobrazenie $f : A \rightarrow B$ sa nazýva *injektívne* ak z toho, že $f(a) = f(a')$ vyplýva, že $a = a'$

Definícia 1.6. Zobrazenie $f : A \rightarrow B$ sa nazýva *bijekcia* ak je surjektívne aj injektívne.

Definícia 1.7. Nech $f : A \rightarrow B$, $g : B \rightarrow C$ sú dve zobrazenia, potom predpis $x \in A \rightarrow g(f(x))$ definuje zobrazenie $A \rightarrow C$ označíme ho $g \circ f : A \rightarrow C$, $g \circ f(x) = g(f(x))$ pre $\forall x \in A$. Zobrazenie $g \circ f : A \rightarrow C$ sa nazýva zobrazenie *zložené* z f a g resp. *kompozícia* zobrazení f a g .

Tvrdenie 1.1.

- 1.) Ak $f : A \rightarrow B$, $g : B \rightarrow C$ sú injekcie, tak aj $g \circ f : A \rightarrow C$ je injekcia.
- 2.) Ak $f : A \rightarrow B$, $g : B \rightarrow C$ sú surjekcie, tak aj $g \circ f : A \rightarrow C$ je surjekcia.

Dôkaz. Predpokladajme, že $g \circ f(a) = g \circ f(a')$. Chceme ukázať, že $a = a'$. Ale $g(f(a)) = g(f(a'))$, lebo g je injektívne. Z toho: $f(a) = f(a')$. Ale aj f je injektívne $\Rightarrow a = a'$. □

Tvrdenie 1.2. Ak $f : A \rightarrow B$, $g : B \rightarrow C$, $h : C \rightarrow D$ sú zobrazenia, tak $h \circ (g \circ f) = (h \circ g) \circ f$. To je tzv. *asociatívnosť skladania zobrazení*.

Dôkaz. $h \circ (g \circ f)(x) = h((g \circ f)(x)) = h(g(f(x)))$;
 $(h \circ g) \circ f(x) = (h \circ g)(f(x)) = h(g(f(x))) : \forall x \in A$ □

Veta 1.1 a Definícia 1.8. Nech $f : A \rightarrow B$ je bijekcia. Potom existuje zobrazenie $B \rightarrow A$, ktoré každému prvku $b \in B$ priradí len jediný prvok $a \in A$, pre ktorý $f(a) = b$. Toto je *inverzné zobrazenie* k f , označíme ho f^{-1} . Teda $f^{-1}(b) = a \iff f(a) = b$. Zobrazenie $f^{-1} : B \rightarrow A$ je tiež bijektívne a platí: $f^{-1} \circ f = id_A$, $f \circ f^{-1} = id_B$.

Dôkaz.

- 1.) f^{-1} je injekcia: nech $a = f^{-1}(b) = f^{-1}(b')$ Potom $f(a) = b$ a $f(a) = b' \Rightarrow b = b'$. f^{-1} je injekcia.
- 2.) f^{-1} je surjekcia: ľubovoľné $a \in A$, $f^{-1}(f(a)) = a$, f^{-1} je bijekcia. □

Tvrdenie 1.3. Ak $f : A \rightarrow B$, $g : B \rightarrow A$ sú zobrazenia také, že $g \circ f = id_A$, tak f je injekcia a g je surjekcia.

Dôkaz.

f je injekcia: Predpokladajme, že $f(a) = f(a') \Rightarrow g(f(a)) = g(f(a')) = (g \circ f)(a') = id_A(a') = a'$.

g je surjekcia: ľubovoľné $a \in A \Rightarrow f(a) \in B$, $a = g(f(a)) \Rightarrow f(a)$ je vzor k prvku a pri zobrazení g . □

Veta 1.2. Zobrazenie $f : A \rightarrow B$ je bijektívne $\Leftrightarrow$ keď existuje $g : B \rightarrow A$ také, že $g \circ f = id_A$ a $f \circ g = id_B$

Dôkaz. Predpokladajme, že f je bijektívne. Potom vieme, že $\exists f^{-1} : B \rightarrow A$ s tým, že $f^{-1} \circ f = id_A$. Predpokladajme, že $\exists g : B \rightarrow A : g \circ f = id_A$ a $f \circ g = id_B$. Z tvrdenia 1.3 dostávame, že f je injektívne aj surjektívne $\Rightarrow$ bijektívne. □

Binárne operácie.

Definícia 1.9. Binárna operácia na množine $M \neq \emptyset$ je zobrazenie $M \times M \rightarrow M$. Binárne operácie označujeme rôznymi spôsobmi. Obraz dvojice $(a, b) \in M \times M$ potom označujeme obyčajne $a + b = +(a, b) \dots$

Definícia 1.10. Nech $*$: $M \times M \rightarrow M$ je binárna operácia na M . Prvok $e \in M$ taký, že $m * e = m = e * m$ pre $\forall m \in M$ sa nazýva *neutrálny prvok* operácie $*$.

Pozn.. Binárna operácia nemusí mať neutrálny prvok.

Tvrdenie 1.4. Ak binárna operácia $*$: $M \times M \rightarrow M$ má neutrálny prvok, tak ho má jediný.

Dôkaz. Keby $e_1, e_2 \in M$ boli neutrálne, tak $e_1 = e_1 * e_2 = e_2 \Rightarrow e_1 = e_2$. □

Definícia 1.11. Nech $*$: $M \times M \rightarrow M$ je binárna operácia a nech má neutrálny prvok $e \in M$. Ak pre nejaké $x \in M : \exists y \in M$ také, že $x * y = y * x = e$, tak y sa volá *inverzný prvok* k x .

Označenie. Inverzný prvok k prvku x z predchádzajúcej definície označíme x^{-1} .

Definícia 1.12. Binárna operácia je *asociatívna*, ak pre všetky $a, b, c \in M$ máme: $a * (b * c) = (a * b) * c$

Tvrdenie 1.5. Nech $\bullet$: $M \times M \rightarrow M$ je asociatívna binárna operácia a nech $e \in M$ je neutr. prvok tejto operácie. Potom ak pre $x \in M$ existuje inverzný prvok, tak je jediný.

Dôkaz. Nech pre $x \in M$ by inverzné prvky boli dva: $a \in M, b \in M$. Teda: $ax = xa = e$, $bx = xb = e$. Chceme ukázať, že $a = b$. Takto: $a = ae = a(bx) = (ax)b = eb = b$. □

Definícia 1.13. Nech $G \neq \emptyset$ je množina a nech $*$: $G \times G \rightarrow G$ je binárna operácia na G s týmito vlastnosťami:

- 1.) binárna operácia $*$ je asociatívna
- 2.) v G existuje neutrálny prvok operácie $*$, označíme ho e , teda pre každé $x \in G$: $e * x = x * e = x$
- 3.) $\forall x \in G$ existuje v G inverzný prvok, vieme už, že to je jediný prvok $x^{-1} \in G$ taký, že $x * x^{-1} = x^{-1} * x = e$.

Potom hovoríme, že dvojica $(G, *)$ je *grupa*. (alebo G s operáciou $*$ je grupa). Ak je operácia $*$ jasná, niekedy hovoríme, že G je grupa.

Príklad. Nech $m \in \mathbb{N}$ je pevne zvolené. Označme $\mathbb{Z}_m$ množinu zvyškov po delení celých čísel číslom m . Teda $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$. Definujme pre $x, y \in \mathbb{Z}_m$:

$x \oplus y$ je zvyšok po vydelení $x + y$ číslom m . Potom $\oplus$ je binárna operácia na $\mathbb{Z}_m$. Je asociatívna, neutrálny prvok je 0, inverzný prvok k $x \in \mathbb{Z}_m$ je zvyšok po vydelení čísla $m - x$ číslom m . $(\mathbb{Z}_m, \oplus)$ je grupa.

Definícia 1.14. Binárna operácia $*$: $M \times M \rightarrow M$ na množine $M \neq \emptyset$ je *komutatívna*, ak pre $\forall a, b \in M$: $a*b = b*a$. Ak túto vlastnosť nemá tak je nekomutatívna.

Definícia 1.15. Ak $(G, *)$ je grupa a operácia $*$ je komutatívna, tak grupa G sa nazýva komutatívna (alebo tiež abelovská).

Príklady.

1.) $(\mathbb{R} \setminus \{0\}, \cdot)$ je komutatívna grupa.

2.) $G = \{e\}$, $e*e = e$ to je tzv. triviálna grupa.

3.) $(\mathbb{Z}, +)$, $(\mathbb{Z}_m, \oplus)$ sú komutatívne grupy.

4.) Nech $M \neq \emptyset$ je množina. Označme $S_M :=$ množinu všetkých bijekcií $M \rightarrow M$. Skladanie zobrazení definuje binárnu operáciu $*$ na S_M , t.j. $f*g = g \circ f$ pre $\forall f, g \in S_M$. Potom $(S_M, *)$ je grupa. Nie je komutatívna.

5.) Ak M z 4.) je $M = \{1, 2, \dots, n\}$ čo je vlastne S_M ? $S_{\{1, 2, \dots, n\}}$ je vlastne množina permutácií prvkov $1, 2, \dots, n$ množiny $\{1, 2, \dots, n\}$. Permutáciu

$f: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ môžeme prehľadne zapísať ako $f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$

Napr. pre $S_{\{1, 2, 3\}}$ je $(S_{\{1, 2, 3\}}, *)$ grupa, ktorá má 6 prvkov.

Napr.: $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ kým $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

$S_{\{1, 2, 3\}}$ je komutatívna grupa.

Veta 1.3. Nech $(G, \bullet)$ je grupa. Potom:

1.) $(x^{-1})^{-1} = x$ pre $\forall x \in G$

2.) $(x \bullet y)^{-1} = y^{-1} \bullet x^{-1}$ pre $\forall x, y \in G$

Dôkaz.

1.) $(x^{-1})^{-1}$ je inverzný prvok k x^{-1} . Ale máme $x \bullet x^{-1} = x^{-1} \bullet x = 1$ a teda inverzný prvok k x^{-1} je x . Pretože inverzný prvok je jediný máme: $(x^{-1})^{-1} = x$.

2.) Rátajme $(x \bullet y) \bullet (y^{-1} \bullet x^{-1}) = x \bullet (y \bullet y^{-1}) \bullet x^{-1} = x \bullet 1 \bullet x^{-1} = 1$

Podobne $(y^{-1} \bullet x^{-1}) \bullet (x \bullet y) = y^{-1} \bullet (x^{-1} \bullet x) \bullet y = y^{-1} \bullet 1 \bullet y = 1 \Rightarrow 2.$

□

Podgrupa.

Definícia 1.16. Nech $(G, \bullet)$ je grupa. Nech $U \neq \emptyset$ je podmnožina v G s binárnou operáciou $*$: $U \times U \rightarrow U$ takou, že pre každé $x, y \in U$ platí $x*y = x \bullet y$. Ak $(U, *)$ je grupa, tak hovoríme, že $(U, *)$ je *podgrupa* grupy $(G, \bullet)$. Voľnejšie tiež hovoríme, že grupa U je podgrupou grupy G . Teda ak $(U, *)$ je podgrupou v $(G, \bullet)$ tak zobrazenie $\bullet|_{U \times U}: U \times U \rightarrow G$ je vlastne U teda (trochu nepresne) môžeme povedať, že v tejto situácii je binárna operácia $*$ podgrupy U zúžením binárnej operácie $\bullet$ grupy G .

Veta 1.4. (kritérium podgrupy). Nech $U \neq \emptyset$ je podmnožina množiny G , pričom nech $(G, \bullet)$ je grupa. Potom U je podgrupou grupy G práve vtedy, keď platí ktorákoľvek z nasledujúcich dvoch ekvivalentných podmienok:

(I): pre $\forall x, y \in U$ je $x \bullet y^{-1} \in U$

(II): pre $\forall x, y \in U$ je $x \bullet y \in U$ a $y^{-1} \in U$.

Dôkaz. U je podgrupa potom $(I) \wedge (II)$

Najskôr ukážeme, že $(U, *)$ je podgrupa v $(G, \bullet)$. Označme 1_U neutrálny prvok grupy U , 1 je neutrálny prvok grupy G . Máme: $1_U * 1_U = 1_U = \boxed{1_U \bullet 1_U = 1_U \bullet 1}$. Vynásobením rovnosti $\boxed{}$ zľava prvkom 1_U^{-1} dostávame: $1_U = 1$. Teraz pre ľubovoľný prvok $y \in U$ označme y_U^{-1} k nemu inverzný prvok v podgrupe $(U, *)$. (y^{-1} je inverzný prvok k y v grupe $(G, \bullet)$). Máme: $y_U * y_U^{-1} = y_U \bullet y_U^{-1} = 1_U = 1 = y_U^{-1} * y_U = y_U^{-1} \bullet y_U$. Teda z toho, čo je podčiarknuté vidíme, že k y je v G inverzný prvok y_U^{-1} . Ale tiež je to y^{-1} . Keďže inverzný prvok k prvku grupy je práve jeden, dostávame: $y_U^{-1} = y^{-1}$. Teda pre $x, y \in U$ máme aj $x, y^{-1} \in U$. Pretože $(U, *)$ je podgrupa, máme $x*y^{-1} = x \bullet y^{-1} \in U$. To je práve (I). Analogicky sa dokáže, že ak $(U, *)$ je podgrupa,

tak platí (II).

Teraz predpokladajme, že je splnená podmienka (I). Chceme ukázať, že potom $(U, *)$ je podgrupa. Pretože $U \neq \emptyset$ máme ďalej prvok $a \in U$. Z (I) potom dostávame, že $a \bullet a^{-1} = 1 \in U$. Ďalej, ak $y \in U$ je ľubovoľné, tak z podmienky (I) vyplýva $1 \bullet y^{-1} = y^{-1} \in U$. Teraz pre ľubovoľné $x, y \in U$ bude tiež $x, y^{-1} \in U$. Z (I) potom máme, že aj $x \bullet (y^{-1})^{-1} = x \bullet y \in U$. Ináč povedané, predpis $x * y = x \bullet y$ pre ľubovoľné $(x, y) \in U \times U$ definuje binárnu operáciu $* : U \times U \rightarrow U$. Operácia $*$ je asociatívna (lebo $\bullet$ je taká), neutrálny prvok je, inverzný prvok $y_U^{-1} = y^{-1}$, teda $(U, *)$ je grupa. Je to podgrupa v $(G, \bullet)$. □

Homomorfizmy grúp.

Definícia 1.17. Nech $(G, \bullet), (H, *)$ sú grupy. *Homomorfizmus* z $(G, \bullet)$ do $(H, *)$ je zobrazenie $f : G \rightarrow H$ také, že $f(x \bullet y) = f(x) * f(y)$ pre všetky $x, y \in G$.

Veta 1.5. Nech $f : (G, \bullet) \rightarrow (H, *)$ je homomorfizmus grúp. Potom

- 1.) $f(1) = 1$.
- 2.) $f(x^{-1}) = (f(x))^{-1}$.

Dôkaz.

- 1.) $1 * f(1) = f(1 \bullet 1) = f(1) * f(1) \Leftrightarrow f^{-1}(1) * 1 * f(1) = f^{-1}(1) * f(1) * f(1) \Leftrightarrow f(1) = 1$
- 2.) Nech $x \in G$ je ľubovoľné. Potom $x * x^{-1} = x^{-1} * x = 1$. Pretože f je homomorfizmus a platí $f(1) = 1$ máme, že $f(x \bullet x^{-1}) = f(x) * f(x^{-1}) = f(x^{-1}) * f(x) = f(1) = 1$ z čoho $(f(x))^{-1} = f(x^{-1})$. □

Veta 1.6. Nech $f : (G, \bullet) \rightarrow (H, *)$ je homomorfizmus grúp. Ak $S \neq \emptyset$ je podgrupa grupy G tak $f(S)$ je podgrupa grupy H .

Dôkaz. Pretože S je podgrupa vieme, že $1 \in S$. Potom $f(1) = 1 \in S$, teda $f(S) \neq \emptyset$. Ďalej overíme (napr.) podmienku (I) z kritéria podgrupy pre $f(S)$. Nech $x, y \in f(S)$ sú ľubovoľné. Teda $x = f(a)$ a $y = f(b)$ pre $a, b \in S$. Potom $y^{-1} = (f(b))^{-1} = f(b^{-1})$ z predchádzajúcej vety. Z toho $x * y^{-1} = f(a) * f(b^{-1}) = f(a \bullet b^{-1}) \in f(S)$ totiž $a \bullet b^{-1} \in S$ keďže $a, b \in S$ a S je podgrupa. Podmienka (I) je splnená a teda $f(S)$ je podgrupa. □

Definícia 1.18. Majme zobrazenie $f : M \rightarrow N$ a nech $A \subset N$. Vzor množiny A pri zobrazení f označíme $f^{-1}(A)$ pritom $f^{-1}(A) = \{x \in M; f(x) \in A\}$

Veta 1.7. Nech $f : (G, \bullet) \rightarrow (H, \bullet)$ je homomorfizmus grúp a nech $S \subset H$ je podgrupa grupy H . Potom $f^{-1}(S)$ je podgrupa grupy G .

Dôkaz. Vieme, že $f(1) = 1$ pritom $1 \in S$, lebo S je podgrupa. Teda $1 \in f^{-1}(S)$ a preto $f^{-1}(S) \neq \emptyset$. Teraz použijeme kritérium podgrupy. Nech $x, y \in f^{-1}(S)$ sú ľubovoľné. Chceme ukázať, že $x \bullet y^{-1} \in f^{-1}(S)$. Takto: pretože $x, y \in f^{-1}(S)$ máme $f(x) \in S$, $f(y) \in S$. Pretože S je podgrupa, potom aj $f(x) \bullet (f(y))^{-1} \in S$. Pritom však vieme, že $f(y^{-1}) = (f(y))^{-1}$. Teda máme $f(x) \bullet f(y^{-1}) \in S \Rightarrow f(x \bullet y^{-1}) \in S$. To znamená, že $x \bullet y^{-1} \in f^{-1}(S)$. □

Definícia 1.19. Nech $f : (G, \bullet) \rightarrow (H, \bullet)$ je homomorfizmus grúp. Vieme, že $\{1\} \subset H$ je podgrupa grupy H . Podgrupu $f^{-1}(\{1\})$ grupy G nazývame *jadro* homomorfizmu f , označuje sa $\text{Ker}(f)$. Teda $\text{Ker}(f) = \{x \in G; f(x) = 1\}$

Veta 1.8. Nech $f : (G, \bullet) \rightarrow (H, \bullet)$ je homomorfizmus grúp. Potom f je injektia $\Leftrightarrow \text{Ker}(f) = \{1\}$

Dôkaz.

$\Rightarrow$: Nech f je injektívne zobrazenie. Chceme ukázať, že $\text{Ker}(f) = \{1\}$. Takto:

máme $f(1)=1$, a teda zrejme $\{1\} \subset \text{Ker}(f)$. Ak $x \in \text{Ker}(f)$, tak $f(x)=1=f(1)$. Z injektívnosti f vyplýva, že $x=1$. Teda tiež $\text{Ker}(f) \subset \{1\}$. Vcelku: $\text{Ker}(f)=\{1\}$.

$\boxed{\Leftarrow}$: Predpokladajme, že $\text{Ker}(f) = 1$. Chceme ukázať, že f je injektívne. Takto: nech $f(x) = f(y)$ pre dáke $x, y \in G$. Potrebujeme ukázať, že $x = y$. Z toho, že $f(x)=f(y)$ dostávame $f(x) \bullet (f(y))^{-1} = 1$. Ale vieme, že $f(y^{-1}) = (f(y))^{-1}$. Teda platí: $f(x) \bullet f(y^{-1}) = 1$. Pretože f je homomorfizmus, z toho dostaneme: $f(x \bullet y^{-1}) = 1$. Teda: $x \bullet y^{-1} \in \text{Ker}(f) = \{1\}$. To znamená, že $x \bullet y^{-1} = 1$. Z toho dostaneme, že $x = y$. □

Definícia 1.20. Injektívny homomorfizmus grúp sa nazýva *monomorfizmus*.

Surjektívny homomorfizmus grúp sa nazýva *epimorfizmus*. Homomorfizmus grúp, ktorý je bijektívny sa volá *izomorfizmus*. Ak $(G, \bullet)$ a $(H, \bullet)$ sú grupy a existuje izomorfizmus $f : (G, \bullet) \rightarrow (H, \bullet)$ tak hovoríme, že grupy G a H sú izomorfné. Vtedy stručne píšeme: $f : G \xrightarrow{\cong} H$, alebo $G \cong H$.

Veta 1.9. Nech $f : (G, \bullet) \rightarrow (H, \bullet)$ je izomorfizmus grúp. Potom aj inverzné zobrazenie $f^{-1} : (H, \bullet) \rightarrow (G, \bullet)$ je izomorfizmus grúp.

Dôkaz. Vieme, že $f^{-1} : H \rightarrow G$ existuje a že je bijekcia. Ešte treba ukázať, že f^{-1} je aj homomorfizmus grúp. Takto: nech $x, y \in H$ sú ľubovoľné. Potom existujú jednoznačne určené $a, b \in G$ také, že $f(a)=x$, $f(b)=y$. Keďže f je homomorfizmus máme $f(a) \bullet f(b) = f(a \bullet b) = x \bullet y$; z toho: $f^{-1}(x \bullet y) = a \bullet b = f^{-1}(x) \bullet f^{-1}(y)$. □

Veta 1.10. Zloženie dvoch homomorfizmov grúp je znova homomorfizmus grúp. Zloženie dvoch izomorfizmov grúp je znova izomorfizmus.

Dôkaz. Nech $f : (G, \bullet) \rightarrow (H, \bullet)$, $t : (T, \bullet) \rightarrow (S, \bullet)$ sú homomorfizmy grúp. Potom pre $\forall x, y \in G$ je $t \circ f(x \bullet y) = t(f(x \bullet y)) = t(f(x) \bullet f(y)) = t(f(x)) \bullet t(f(y)) = (t \circ f(x)) \bullet (t \circ f(y))$. □

Relácie na množinách a faktorové grupy komutatívnych grúp.

Definícia 1.21. Relácia na množine $M \neq \emptyset$ je hocijaká podmnožina $R \subset M \times M$.

Definícia 1.22. Relácia R na množine $M \neq \emptyset$ sa volá *relácia ekvivalencie* ak má tieto vlastnosti:

- 1.) $(x, x) \in R \quad \forall x \in M$ (reflexívnosť relácie R)
- 2.) ak $(x, y) \in R$ tak aj $(y, x) \in R$ (symetrickosť)
- 3.) ak $(x, y) \in R$ a $(y, z) \in R$ tak aj $(x, z) \in R$ (tranzitívnosť)

Definícia 1.23. Nech $\sim$ je relácia ekvivalencie na množine $M \neq \emptyset$. Potom pre ľubovoľné $y \in M$ označíme $[y] = \{x \in M; x \sim y\}$. $[y]$ sa volá *trieda ekvivalencie* určená (reprezentovaná) prvkom y , y sa volá *reprezentant* triedy ekvivalencie $[y]$.

Veta 1.11. Nech $\sim$ je relácia ekvivalencie na množine $M \neq \emptyset$ a nech $[y]$ pre $y \in M$ znamená triedu reprezentovanú prvkom y . Potom:

- 1.) $[y] \neq \emptyset \quad \forall y \in M$
- 2.) $[x] = [y] \Leftrightarrow x \sim y \quad \forall x, y \in M$
- 3.) ak $[x] \neq [y]$, tak $[x] \cap [y] = \emptyset$
- 4.) $\bigcup_{x \in M} [x] = M$

Dôkaz.

1.) $y \sim y$ a vtedy $y \in M$.

2.) $\boxed{\Leftarrow}$: Nech $x \sim y$. Chceme ukázať, že $[x] = [y]$. Nech $a \in [x]$. Potom $a \sim x$, ale $x \sim y$, preto $a \sim y$, a teda $a \in [y]$. Teda $[x] \subset [y]$. Analogicky sa dokáže $[y] \subset [x]$, teda $[x] = [y]$.

$\boxed{\Rightarrow}$: Predpokladajme, že $[x] = [y]$. Potom $x \in [x] = [y]$, teda $x \in [y]$, preto $x \sim y$.

3.) Predpokladajme, že $[x] \cap [y] \neq \emptyset$. Teda existuje $a \in [x] \cap [y]$. Potom $a \sim x$ a $a \sim y$,

teda $x \sim y$.

4.) Je zrejmé, že $\bigcup_{x \in M} [x] \subset M$. Nech teraz $x \in M$. Potom $x \in [x]$, teda $x \in \bigcup_{x \in M} [x]$, ukázali sme tiež, že $M \subset \bigcup_{x \in M} [x]$. Teda $M = \bigcup_{x \in M} [x]$. □

Veta 1.12. *Nech $(G, +)$ je komutatívna grupa a nech H je jej podgrupa. Definujeme reláciu $\sim$ na G takto: pre $x, y \in G$ platí $x \sim y \Leftrightarrow x - y \in H$. Potom $\sim$ je relácia ekvivalencie.*

Dôkaz.

Reflexívnosť: $x - x = 0 \in H$, teda $x \sim x \forall x \in G$

Symetrickosť: nech $x \sim y$. Potom $x - y \in H$. Ale H je podgrupa a preto aj $-(x - y) \in H$ teda $y \sim x$.

Tranzitívnosť: nech $x \sim y$ a $y \sim z$. Potom: $x - y \in H$ a $y - z \in H$. Pretože H je podgrupa máme, že $(x - y) + (y - z) \in H$. Teda $x \sim z$. □

Označenie. Množinu tried ekvivalencie na grupe G vzhľadom na reláciu ekvivalencie $\sim$ z predchádzajúcej vety označíme G/H (G podľa H)

Tvrdenie 1.5. *Nech pre $[x] \in G/H$ a $[y] \in G/H$ je $[x] \oplus [y] = [x + y]$. Potom $\oplus : G/H \times G/H \rightarrow G/H$ je dobre definované zobrazenie a teda $\oplus$ je binárna operácia na množine G/H .*

Dôkaz. Treba ukázať, že $[x + y]$ nezávisí od výberu reprezentant tried $[x]$ resp. $[y]$. Nech $[x] = [a]$, $[y] = [b]$. Chceme ukázať, že $[a + b] = [x + y]$. Takto: z toho, že $[x] = [a]$, $[y] = [b]$ vieme, že $x \sim a$, $y \sim b$. Teda $x - a \in H$, $y - b \in H$. Pretože H je podgrupa grupy G , máme tiež $(x - a) + (y - b) \in H \Leftrightarrow (x + y) - (a + b) \in H$. Z toho $x + y \sim a + b$, teda $[x + y] = [a + b]$. □

Veta 1.13 a Definícia 1.24. *Nech G je komutatívna grupa a H je jej podgrupa. Na množine G/H definujeme binárnu operáciu $\oplus$ ako v predchádzajúcom tvrdení. Potom $(G/H; \oplus)$ je komutatívna grupa. Táto grupa sa volá faktorová grupa grupy G podľa podgrupy H .*

Dôkaz. $G/H \neq \emptyset$, lebo $[0] \in G/H$.

Asociatívnosť operácie $\oplus$: $[x] \oplus ([y] \oplus [z]) = [x + (y + z)] = [(x + y) + z] = [x + y] \oplus [z] = ([x] \oplus [y]) \oplus [z]$, pre každé $[x], [y], [z] \in G/H$.

Existencia neutrálneho prvku: Pre každé $[x] \in G/H$ máme $[x] \oplus [0] = [x + 0] = [x] = [0 + x] = [0] \oplus [x]$, teda $[0]$ je neutrálny prvok operácie $\oplus$.

Existencia inverzného prvku: Nech $[x] \in G/H$ je ľubovoľné, potom $[x] \oplus [-x] = [x - x] = [0] = [-x] \oplus [x]$, teda inverzný prvok k $[x] \in G/H$ je $[-x] \in G/H$.

$(G/H, \oplus)$ je komutatívna grupa: $[x] \oplus [y] = [x + y] = [y + x] = [y] \oplus [x]$. □

Príklad. Nech $m \in \mathbb{N}$ je pevne zvolené. Zoberme $G = \mathbb{Z}$ s operáciou sčítovania a $H = m\mathbb{Z}$. $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \dots, [m-1]\}$, $[x] \oplus [y] = [x + y] \forall x, y \in \mathbb{Z}$, $(\mathbb{Z}/m\mathbb{Z}, \oplus)$ je komutatívna grupa.

Tvrdenie 1.6. *Nech $H \neq \{0\}$ je podgrupa grupy $(\mathbb{Z}, +)$. Potom $\exists m \in \mathbb{N}$ také, že $H = m\mathbb{Z}$.*

Dôkaz.

Nech m je najmenšie celé číslo patriace do H . Potom aj $k \cdot m = \overbrace{m + \dots + m}^{k-\text{krát}} \in H$ pre $\forall k \in \mathbb{N} \setminus \{0\}$. Pretože H je podgrupa, máme tiež $k \cdot m \in H$ pre $\forall k \in \mathbb{Z}$. Teda $m\mathbb{Z} \subset H$.

Ešte ukážeme, že $H \subset m\mathbb{Z}$. Nech $x \in H$ je ľubovoľný kladný prvok z H , ukážeme, že $x \in m\mathbb{Z}$ (to stačí). Vieme, že $x = q \cdot m + r$, pre jednoznačne určené q, r pričom $0 \leq r < m$. Z toho: $r = x - q \cdot m \in H$. Keby $r > 0$, tak by r bolo kladné číslo z H , menšie ako najmenší kladný prvok z H – to je nemožné. Preto $r = 0$, a teda $x = q \cdot m$ t.j. $x \in m\mathbb{Z}$. Tým sme ukázali, že aj $H \subset m\mathbb{Z}$. Vcelku: $H = m\mathbb{Z}$. □

Veta 1.14. (o faktorovom izomorfizme): Nech $(G, +)$ a $(H, +)$ sú komutatívne grupy a nech $f : G \rightarrow H$ je homomorfizmus grúp. Potom $G/Ker(f) \cong Im(f)$. Špeciálne, ak f je epimorfizmus, tak $G/Ker(f) \cong H$.

Dôkaz. Predpis, ktorý ľubovoľnému $[x] \in G/Ker(f)$ priradí $f(x) \in Im(f) = f(G)$, dobre definuje zobrazenie $\bar{f} : G/Ker(f) \rightarrow Im(f)$. Treba ukázať, že ak $[x] = [a]$, tak aj $f(x) = f(a)$. Takto: ak $[x] = [a]$, tak $x \sim a$, teda $x - a \in Ker(f)$. Z toho $f(x - a) = 0 \in H$ t.j. $f(x) - f(a) = 0$, a teda $f(x) = f(a)$. Ukázali sme, že $\bar{f} : G/Ker(f) \rightarrow Im(f)$; $\bar{f}([x]) = f(x)$ je dobre definované zobrazenie. $\bar{f}$ je aj homomorfizmus grúp: $\bar{f}([x] + [y]) = \bar{f}([x + y]) = f(x + y) = f(x) + f(y) = \bar{f}([x]) + \bar{f}([y])$ pre všetky $[x], [y] \in G/Ker(f)$. $\bar{f}$ je monomorfizmus grúp: Nech $\bar{f}([x]) = \bar{f}([y])$. Potom $f(x) = f(y)$, a teda $f(x) - f(y) = 0$, t.j. $f(x - y) = 0$ t.j. $x - y \in Ker(f)$. Teda $x \sim y$, preto $[x] = [y]$. $\bar{f}$ je epimorfizmus grúp: pre ľubovoľné $b \in Im(f)$ máme $x \in G : f(x) = b$. Potom $\bar{f}([x]) = f(x) = b \Rightarrow \bar{f}$ je izomorfizmus grúp. □

Príklad. $m \in \mathbb{N}$ pevne zvolené. Zobrazenie $\varphi_m : \mathbb{Z} \rightarrow \mathbb{Z}_m$. $\varphi_m(x) =$ zvyšok po vydelení x číslom m . φ_m je epimorfizmus z grupy $(\mathbb{Z}, +)$ na $(\mathbb{Z}_m, \oplus)$. $Ker(\varphi_m) = \{x \in \mathbb{Z}; m|x\} = m\mathbb{Z}$. Z vety o faktorovom izomorfizme: $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$.

II. OKRUH, TELESO, POLE

Definícia 2.1. Nech R je množina v ktorej sú aspoň dva prvky. Nech sú na R definované dve binárne operácie: $+$: $R \times R \rightarrow R$ ("sčítovanie") a $\bullet$: $R \times R \rightarrow R$ ("násobenie"). Hovoríme, že $(R, +, \bullet)$ je *okruh*, ak:

- 1.) $(R, +)$ je komutatívna grupa.
- 2.) $\bullet$ je asociatívna: $x \bullet (y \bullet z) = (x \bullet y) \bullet z \quad \forall x, y, z \in R$
- 3.) $\bullet$ je distributívna vzhľadom na sčítovanie: $x \bullet (y + z) = x \bullet y + x \bullet z$
 $(x + y) \bullet z = x \bullet z + y \bullet z$ Ak $\bullet$ je komutatívna, potom $(R, +, \bullet)$ s vlastnosťami 1.), 2.), 3.) je komutatívny okruh. Ak $\bullet$ má neutrálny prvok, hovoríme o okruhu s 1, $(R, +, \bullet, 1)$.

Definícia 2.2. Okruh $(R, +, \bullet)$, v ktorom operácia $\bullet$ je komutatívna sa volá *komutatívny okruh*.

Definícia 2.3. Nech $(R, +, \bullet)$ je okruh s 1, ak $\bullet|_{R^*}$, kde $R^* = R \setminus \{0\}$ nadobúda hodnoty v R , t.j. ak $\bullet|_{R^*}$ definuje binárnu operáciu v R^* , a R^* s touto operáciou je grupa, tak $(R, +, \bullet, 1)$ sa nazýva *teleso*. Komutatívny okruh, ktorý je telesom sa nazýva *pole*.

Veta 2.1. Nech $(R, +, \cdot)$ je ľubovoľný okruh. Potom v ňom platia tieto pravidlá pre rátanie:

- 1.) $0 \cdot x = x \cdot 0$ pre $\forall x \in R$
- 2.) $(-x) \cdot y = x \cdot (-y) = -(x \cdot y)$ pre $\forall x, y \in R$
- 3.) Ak R má 1, tak $1 \neq 0$.
- 4.) Ak R je teleso, tak z toho, že $x \cdot y = 0$ vyplýva, že $x = 0 \vee y = 0$.
- 5.) Ak R je teleso, tak $x^2 = 1 \Leftrightarrow x = 1 \vee x = -1$.

Dôkaz.

- 1.) $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x \Leftrightarrow 0 = 0 \cdot x$.
- 2.) $(x + (-x)) \cdot y = 0 \cdot y = 0$
 $x \cdot y + (-x) \cdot y = 0 \Leftrightarrow -(x \cdot y) = (-x) \cdot y$.
- 3.) Pretože R má aspoň 2 prvky, existuje $x \in R, x \neq 0$. Ak R má 1, tak $x \cdot 0 = 0$ podľa 1.) a $x \cdot 1 = 1$, keďže $x \neq 0 \Rightarrow 1 \neq 0$.
- 4.) Ak $x \neq 0$ a $y \neq 0$, tak treba dokázať $x \cdot y \neq 0$. Takto: $x \neq 0, y \neq 0$, tak $x \in R^*$ a $y \in R^*$, ale R^* je grupa (vzhľadom na $\cdot|_{R^*}$) a preto $x \cdot y \in R^*$ t.j. $x \cdot y \neq 0$.
- 5.) $\Rightarrow$: Predpokladajme, že $x^2 = 1$. Teda $x^2 - 1 = 0$, t.j. $(x - 1)(x + 1) = 0 \stackrel{4.}{\Rightarrow} x + 1 = 0 \vee x - 1 = 0 \Leftrightarrow x = -1 \vee x = 1$.
 $\Leftarrow$ Pomocou 2.).

□

Lema 2.1.

Nech $p, q \in \mathbb{N}$. Potom množina $\{p \cdot x + q \cdot y \in \mathbb{Z}; x, y \in \mathbb{Z}\}$ je podgrupou v $(\mathbb{Z}, +)$, pričom $\{p \cdot x + q \cdot y \in \mathbb{Z}; x, y \in \mathbb{Z}\} = r\mathbb{Z}$, kde r je najväčší spoločný deliteľ čísel p, q .

Dôkaz. $\{p \cdot x + q \cdot y \in \mathbb{Z}\} \neq \emptyset$. Kritérium podgrupy: $p \cdot x + q \cdot y - (p \cdot x' + q \cdot y') = p \cdot (x - x') + q \cdot (y - y') \in \{p \cdot x + q \cdot y; x, y \in \mathbb{Z}\}$. V $(\mathbb{Z}, +)$ sú všetky podgrupy tvaru: $k\mathbb{Z}$, (pre nejaké $k \in \mathbb{N}$). Teda $\{p \cdot x + q \cdot y; x, y \in \mathbb{Z}\} = r\mathbb{Z}$. Treba ešte ukázať, že r je najväčší spoločný deliteľ čísel p, q . $p \in \{p \cdot x + q \cdot y; x, y \in \mathbb{Z}\}$, $p = r \cdot k$, teda $r|p$. $q \in \{p \cdot x + q \cdot y; x, y \in \mathbb{Z}\}$, $q = r \cdot l$, teda $r|q$. Nech c je nejaký spoločný deliteľ čísel p, q . Chceme ukázať, že $c|r$. Ak $c|p$ a $c|q$, tak $c|p \cdot x + q \cdot y$ pre $\forall x, y \in \mathbb{Z}$, a teda c je deliteľom každého prvku z $\{p \cdot x + q \cdot y; x, y \in \mathbb{Z}\} = r\mathbb{Z}$, teda $c|r$ t.j. $c|r$.

□

Veta 2.2. Nech $m \in \mathbb{N}, m \geq 2$. Potom $(\mathbb{Z}/m\mathbb{Z}, \oplus, \odot)$ je pole $\Leftrightarrow m$ je prvočíslo.

Dôkaz.

$\Rightarrow$: Predpokladajme, že $\mathbb{Z}/m\mathbb{Z}$ je pole. (To znamená, že nenulové prvky tvoria grupu.) Keby m nebolo prvočíslo, tak by $m = m_1 \cdot m_2$, kde $m_1, m_2 \in \mathbb{N}, 1 < m_1 < m$

$1 < m_2 < m$. Potom $[m_1] \neq 0, [m_2] \neq 0$, ale $[m_1] \cdot [m_2] = [m_1 \cdot m_2] = [m] = [0] = 0$. Je to spor s tým, že $(\mathbb{Z}/m\mathbb{Z})^*$ je grupa.

$\boxed{\Leftarrow}$: Predpokladajme, že m je prvočíslo. Chceme ukázať, že $(\mathbb{Z}/m\mathbb{Z}, \odot)$ je grupa. Na to stačí ukázať, že pre ľubovoľné nenulové $0 \neq x \in \mathbb{Z}/m\mathbb{Z}$ existuje v $(\mathbb{Z}/m\mathbb{Z})^*$ inverzný prvok vzhľadom na násobenie. Takto: pre $[x] \in (\mathbb{Z}/m\mathbb{Z})^*$ máme $m \nmid x$, z toho: najväčší spoločný deliteľ m, x je 1. Potom z *Lemy* 2.1 vieme, že $1 = a \cdot x + b \cdot y$ pre dáke $a, b \in \mathbb{Z}$. Z toho $[1] = 1 = [a \cdot x + b \cdot y] = [a \cdot x] + [b \cdot y] = [a] \cdot [x] + [0] \Leftrightarrow [1] = [a] \odot [x]$ t.j. inverzný prvok k $[x]$ vzhľadom na násobenie je $[a] \in (\mathbb{Z}/m\mathbb{Z})^*$.

□

III. VEKTOROVÉ PRIESTORY

Definícia 3.1. Nech $V \neq \emptyset$ je množina, jej prvky budeme označovať: $\vec{a}, \dots, \vec{x}$. Nech R je pole. Nech na V je definovaná binárna operácia $+: V \times V \rightarrow V$ (budeme jej hovoriť sčítovanie prvkov z V) a nech okrem toho je dané zobrazenie $R \times V \rightarrow V$: $(\alpha, \vec{x}) \mapsto \alpha \cdot \vec{x}$ (hovoríme mu násobenie prvkov z V prvkami z R .) V sa nazýva *vektorový priestor* nad poľom R ak spĺňa axiómy:

- 1.) $(V, +)$ je komutatívna grupa.
- 2.) $\alpha(\vec{x} + \vec{y}) = \alpha\vec{x} + \alpha\vec{y}$ pre všetky $\alpha \in R, \vec{x}, \vec{y} \in V$.
- 3.) $(\alpha + \beta)\vec{x} = \alpha\vec{x} + \beta\vec{x}$ pre $\forall \alpha, \beta \in R$ a $\forall \vec{x} \in V$
- 4.) $\alpha(\beta\vec{x}) = (\alpha\beta)\vec{x}$ pre $\forall \alpha, \beta \in R, \forall \vec{x} \in V$.
- 5.) $1 \cdot \vec{x} = \vec{x}$, pre $\forall \vec{x} \in V$.

Ak V je vektorový priestor, prvky z V sa volajú *vektory*, prvky z R sa volajú *skaláry*.

Poznámka.

Neutrálly prvok vo vektorovom priestore $(V, +)$ sa nazýva *nulový vektor*, ozn.: $\vec{0}$. Ak $\alpha \in R, \vec{x} \in V$, tak $\alpha \cdot \vec{x}$ nazývame α -násobok vektora $\vec{x} \in V$.

Veta 3.1. Nech V je vektorový priestor nad poľom R . Potom $\forall \vec{x} \in V, \forall \alpha \in R$:

- 1.) $\vec{0} \cdot \vec{x} = \vec{0}$.
- 2.) $(-1) \cdot \vec{x} = -\vec{x}$.
- 3.) $\alpha \cdot \vec{0} = \vec{0}$

Dôkaz.

- 1.) $\vec{x} = 1 \cdot \vec{x} = (1 + \vec{0})\vec{x} = 1\vec{x} + \vec{0}\vec{x} = \vec{x} + \vec{0}\vec{x} \Leftrightarrow \vec{0}\vec{x} = \vec{0}$.
- 2.) $(1 + (-1))\vec{x} = \vec{0}\vec{x} = \vec{0}$. $1\vec{x} + (-1)\vec{x} = \vec{x} + (-1)\vec{x}$. Teda $\vec{x} + (-1)\vec{x} = \vec{0}$, z čoho $-\vec{x} = (-1)\vec{x}$.
- 3.) $\alpha\vec{0} = \alpha(\vec{x} + (-\vec{x})) = \alpha(1\vec{x} + (-1)\vec{x}) = \alpha(1 + (-1))\vec{x} = \alpha\vec{0} = \vec{0}\vec{x} = \vec{0}$.

□

Definícia 3.2. Nech V je vektorový priestor nad poľom R a nech $D \neq \emptyset$ je podmnožina vo V . D je *vektorový podpriestor* priestoru V , ak D je vektorový priestor nad R , pričom sčítovanie v D a násobenie prvkov z D skalármi z R je zúžením sčítovania vo V resp. násobenia prvkov z V skalármi z R .

Veta 3.2. (*kritérium podpriestoru*):

Nech V je vektorový priestor nad poľom R a nech $D \neq \emptyset, D \subset V$. D je vektorový podpriestor priestoru V práve vtedy, keď je splnená hociktorá z týchto dvoch ekvivalentných podmienok:

- (I.) $\forall \vec{x}, \vec{y} \in D : \vec{x} + \vec{y} \in D$ a pre ľubovoľné $\alpha \in R, \vec{x} \in D$ je $\alpha\vec{x} \in D$.
- (II.) $\forall \vec{x}, \vec{y} \in D$ a $\forall \alpha, \beta \in R$ je $\alpha\vec{x} + \beta\vec{y} \in D$.

Dôkaz. Predpokladajme, že D je vektorový podpriestor. Potom (I) je splnená (z definície vektorového podpriestoru). Teraz predpokladajme, že je splnená (I).

$+$ z V je zúžené na D definuje na D binárnu operáciu $+$. Podľa (I) : $\vec{0}\vec{x} = \vec{0}$ patrí do D . $\vec{0}$ je neutrálly prvok operácie $+$ na D . Pre $\vec{x} \in D$ podľa (I) tiež $(-1)\vec{x} = -\vec{x} \in D$. $+$ je asociatívne, komutatívne, vcelku $(D, +)$ je komutatívna grupa. Okrem toho z (I) vyplýva, že máme definované zobrazenie $R \times D \rightarrow D$. Operácia $+$ a násobenie prvkov z D prvkami z R majú potrebné vlastnosti (zdedené z V); D je teda vektorový podpriestor priestoru V . Na ukončenie dôkazu vety stačí ukázať (I) $\Leftrightarrow$ (II).

Nech platí (I), nech $\alpha, \beta \in R$ a $\vec{x}, \vec{y} \in D$. Potom $\alpha\vec{x} \in D$ a $\beta\vec{y} \in D \xrightarrow{(I)} \alpha\vec{x} + \beta\vec{y} \in D$. Teda (I) $\Rightarrow$ (II). Nech platí (II). Potom pre $\forall \vec{x}, \vec{y} \in D$ máme, že $1\vec{x} + 1\vec{y} = \vec{x} + \vec{y} \in D$. Pre ľubovoľné $\alpha \in R$ a ľubovoľné $\vec{x} \in D$, podľa (II) : $\alpha\vec{x} + \vec{0}\vec{x} = \alpha\vec{x} \in D$ tj. aj (II) $\Rightarrow$ (I). □

Veta 3.3. Nech S, T sú vektorové podpriestory vektorového priestoru V nad poľom R . Potom $S \cap T$ je takisto vektorový podpriestor priestoru V .

Dôkaz. $S \cap T \neq \emptyset$, lebo $\vec{0} \in S \cap T$. Ukážeme, že $S \cap T$ spĺňa podmienku (II). Nech $\alpha, \beta \in R$, pre $\forall \vec{x}, \vec{y} \in S \cap T$ sú ľubovoľné. Potom $\alpha\vec{x} + \beta\vec{y} \in S$ a $\alpha\vec{x} + \beta\vec{y} \in T \Rightarrow \Rightarrow \alpha\vec{x} + \beta\vec{y} \in S \cap T$. Čiže S aj T spĺňajú podmienku (II). $\square$

Veta 3.4. *Nech $\{S_\alpha, \alpha \in A\}$ (A indexová množina.) je ľubovoľný systém vektorových podpriestorov vektorového priestoru V nad poľom R . Potom $\bigcap_{\alpha \in A} S_\alpha$ je vektorový podpriestor priestoru V .*

Dôkaz. Podobne ako vo Vete 3.3. $\square$

Definícia 3.3. Nech V je vektorový priestor nad poľom R a nech $A \neq \emptyset$ je podmnožina vo V . *Najmenší vektorový podpriestor priestoru V obsahujúci A je vektorový podpriestor S taký, že:*

1.) $A \subset S$.

2.) Ak T je vektorový podpriestor vo V taký, že $A \subset T$, tak $S \subset T$.

Veta 3.5. *Nech V je vektorový priestor nad poľom R a nech A je podmnožina vo V . Potom najmenší vektorový podpriestor vo V obsahujúci A existuje a je jediný.*

Dôkaz.

Jednoznačnosť: Nech by S a T boli najmenšie podpriestory obsahujúce A . Potom $T \subset S$ a $S \subset T$, teda $S = T$.

Existencia: Nech φ je systém všetkých vektorových podpriestorov obsahujúcich A . $\varphi \neq \emptyset$, lebo $V \in \varphi$. Potom $\bigcap_{S \in \varphi} S$ je najmenší podpriestor vo V obsahujúci A , lebo:

$\forall S \in \varphi$ máme $A \subset S$, a preto $A \subset \bigcap_{S \in \varphi} S$, t.j. je splnená aj podmienka 2.) z Def 3.3.

Teda $S_A = \bigcap_{S \in \varphi} S$. $\square$

Definícia 3.4. Nech $\vec{x}_1, \dots, \vec{x}_k$ sú vektory z vektorového priestoru V nad poľom R , nech $\alpha_1, \dots, \alpha_k \in R$. Potom $\alpha_1 \cdot \vec{x}_1 + \dots + \alpha_k \cdot \vec{x}_k$ sa nazýva *lineárna kombinácia* vektorov $\vec{x}_1, \dots, \vec{x}_k$ s koeficientmi $\alpha_1, \dots, \alpha_k$. Ak $\alpha_1 = \dots = \alpha_k = 0$, táto lineárna kombinácia sa nazýva triviálna (a je to $\vec{0}$). Ak niektoré $\alpha_i \neq 0$, tak lineárna kombinácia je netriviálna.

Veta 3.6. *Nech $\vec{x}_1, \dots, \vec{x}_k$ sú vektory z vektorového priestoru V nad R . Potom $M = \{\alpha_1\vec{x}_1 + \dots + \alpha_k\vec{x}_k \in V, \alpha_i \in R\}$ je vektorový podpriestor vo V .*

Dôkaz. Daná množina je neprázdna, lebo $\vec{0} \in M$. Ďalej kritérium vektorového podpriestoru. Nech $\alpha, \beta \in R$, $\alpha_1\vec{x}_1 + \dots + \alpha_k\vec{x}_k, \beta_1\vec{x}_1 + \dots + \beta_k\vec{x}_k$ sú z tej množiny. Potom $\alpha \cdot \sum_{i=1}^k \alpha_i \vec{x}_i + \beta \cdot \sum_{i=1}^k \beta_i \vec{x}_i = \sum_{i=1}^k (\alpha\alpha_i + \beta\beta_i) \vec{x}_i \in M$, lebo $\alpha\alpha_i + \beta\beta_i \in R$. $\square$

Označenie. V situácii z predchádzajúcej vety označíme: $[\vec{x}_1, \dots, \vec{x}_k] = \{\alpha_1\vec{x}_1 + \dots + \alpha_k\vec{x}_k \in V; \alpha_i \in R\}$.

Veta 3.7. *Nech $\vec{x}_1, \dots, \vec{x}_k$ sú vektory z vektorového priestoru V nad R a nech $T \subset V$ je vektorového podpriestor taký, že $\{\vec{x}_1, \dots, \vec{x}_k\} \subset T$. Potom aj $[\vec{x}_1, \dots, \vec{x}_k] \subset T$.*

Dôkaz. Indukcia vzhľadom na maximálny počet nenulových koeficientov lineárnej kombinácie vektorov $\vec{x}_1, \dots, \vec{x}_k$. Ak lineárna kombinácia $\alpha_1\vec{x}_1 + \dots + \alpha_k\vec{x}_k$ má maximálny počet nenulových koeficientov, tak patrí do T , lebo je to buď $\vec{0}$, alebo

nenulový násobok spomedzi $\vec{x}_1, \dots, \vec{x}_k$, v každom prípade táto lineárna kombinácia patrí do T . Predpokladajme, že každá lineárna kombinácia vektorov $\vec{x}_1, \dots, \vec{x}_k$ s maximálne $s-1$ ($\leq k-1$) nenulovými koeficientmi patrí do T . Nech $\beta_1\vec{x}_1 + \dots + \beta_s\vec{x}_s$ je lineárna kombinácia s maximálne s nenulovými koeficientmi. Potom $\beta_1\vec{x}_1 + \dots + \beta_s\vec{x}_s = (\beta_1\vec{x}_1 + \dots + \beta_{s-1}\vec{x}_{s-1}) + \beta_s\vec{x}_s \in T$; T je vektorový podpriestor. $\square$

Veta 3.8.

Nech V je vektorový priestor nad R a nech $\{\vec{x}_1, \dots, \vec{x}_k\}$ je ľubovoľná konečná podmnožina vo V . Potom najmenší vektorový podpriestor je $S_{\{\vec{x}_1, \dots, \vec{x}_k\}} = [\vec{x}_1, \dots, \vec{x}_k]$.

Dôkaz. Stačí ukázať, že $[\vec{x}_1, \dots, \vec{x}_k]$ má obidve vlastnosti najmenšieho vektorového podpriestoru obsahujúceho množinu $\{\vec{x}_1, \dots, \vec{x}_k\}$.

1. $\{\vec{x}_1, \dots, \vec{x}_k\} \subset [\vec{x}_1, \dots, \vec{x}_k]$.
2. Ak $T \subset V$ je ľubovoľný podpriestor vo V obsahujúci $\{\vec{x}_1, \dots, \vec{x}_k\}$, tak $[\vec{x}_1, \dots, \vec{x}_k] \subset T$ platí podľa Vety 3.7. Z jednoznačnej určenosti vlastnosťami 1.), 2.) vyplýva, že naozaj $S_{\{\vec{x}_1, \dots, \vec{x}_k\}} = [\vec{x}_1, \dots, \vec{x}_k]$. $\square$

Definícia 3.5. Nech V je vektorový priestor nad R a nech $\{\vec{x}_1, \dots, \vec{x}_k\} \subset V$. Potom vektorový priestor $[\vec{x}_1, \dots, \vec{x}_k] \subset V$ sa nazýva *lineárny (vektorový) obal množiny* $\{\vec{x}_1, \dots, \vec{x}_k\}$. Vektory $\vec{x}_1, \dots, \vec{x}_k$ sa nazývajú *generátory* vektorového priestoru $[\vec{x}_1, \dots, \vec{x}_k]$.

Veta 3.9. Nech V je vektorový priestor nad R a nech $[\vec{x}_1, \dots, \vec{x}_k, \vec{a}] \in V$. Potom $[\vec{x}_1, \dots, \vec{x}_k, \vec{a}] = [\vec{x}_1, \dots, \vec{x}_k]$ práve vtedy, keď $\vec{a}$ je lineárna kombinácia vektorov $\vec{x}_1, \dots, \vec{x}_k$.

Dôkaz.

$\Rightarrow$: Predpokladajme, že $[\vec{x}_1, \dots, \vec{x}_k] = [\vec{x}_1, \dots, \vec{x}_k, \vec{a}]$. Potom

$[\vec{x}_1, \dots, \vec{x}_k, \vec{a}] \subset [\vec{x}_1, \dots, \vec{x}_k]$ teda $\vec{a}$ je lineárna kombinácia vektorov $\vec{x}_1, \dots, \vec{x}_k$.

$\Leftarrow$: Predpokladajme, že $\vec{a}$ je lineárnou kombináciou $\vec{x}_1, \dots, \vec{x}_k$. Chceme ukázať, že $[\vec{x}_1, \dots, \vec{x}_k] = [\vec{x}_1, \dots, \vec{x}_k, \vec{a}]$. Je zrejmé, že $\{\vec{x}_1, \dots, \vec{x}_k\} \subset [\vec{x}_1, \dots, \vec{x}_k, \vec{a}]$ a $[\vec{x}_1, \dots, \vec{x}_k] \subset [\vec{x}_1, \dots, \vec{x}_k, \vec{a}]$. Okrem toho, pretože $\vec{a}$ je lineárna kombinácia $\vec{x}_1, \dots, \vec{x}_k$ máme, že $\{\vec{x}_1, \dots, \vec{x}_k, \vec{a}\} \subset [\vec{x}_1, \dots, \vec{x}_k]$, teda $[\vec{x}_1, \dots, \vec{x}_k, \vec{a}] \subset [\vec{x}_1, \dots, \vec{x}_k]$. Vcelku: $[\vec{x}_1, \dots, \vec{x}_k, \vec{a}] = [\vec{x}_1, \dots, \vec{x}_k]$.

Z toho vyplýva, že najjednoduchší zápis lineárneho obalu $[\vec{y}_1, \dots, \vec{y}_k]$ dostaneme postupným vynechávaním tých vektorov, ktoré sú lineárnou kombináciou ostatných. $\square$

IV. SYSTÉMY LINEÁRNYCH ROVNÍC

Definícia 4.1. Systém rovníc S :

$$a_{11}x_1 + \cdots + a_{1n}x_n = b_1$$

$$\vdots$$

$$a_{s1}x_1 + \cdots + a_{sn}x_n = b_s$$

(všetky rovnice musia byť splnené súčasne) je systém s lineárnych rovníc s n neznámymi $x_1, \dots, x_n$, ak $a_{ij} \in R$ ($i \in [1, s], j \in [1, n]$) a $b_i \in R$, kde R je dané pole. Prvky poľa a_{ij} sa nazývajú *koefficienty*, $b_1, \dots, b_n$ sa nazývajú *absolútne členy* systému S .

Definícia 4.2. Usporiadaná n -tica $(r_1, \dots, r_n) \in R^n$ je *riešenie* systému S , ak $r_1, \dots, r_n$ po dosadení $x_i = r_i$ vyhovuje všetkým rovniciam S . Vyriešiť systém znamená nájsť všetky jeho riešenia. Ak žiadna n -tica z R^n nie je riešením systému S , hovoríme, že je *neriešiteľný*.

Definícia 4.3. Dva systémy lineárnych rovníc sú *ekvivalentné* ak majú tú istú množinu riešení. Vyriešiť daný lineárny systém potom znamená vyriešiť hocikaký s ním ekvivalentný systém.

Definícia 4.4. *Ekvivalentné úpravy* sú také, ktoré nemenia množinu riešení.

Veta 4.1. Nasledujúce úpravy sú ekvivalentné:

- 1.) *Vzájomná výmena dvoch rovníc systému.*
- 2.) *Vynásobenie ľubovoľnej rovnice v S prvkom $\alpha \neq 0$, $\alpha \in R$.*
- 3.) *Pripočítanie ľubovoľnej rovnici v S inej rovnici v S .*

Dôkaz. triviálny. □

Zámer pri riešení systému S . :

Pomocou ekvivalentných úprav ho prevedieme na jednoduchý ekvivalentný systém, ktorý už nie je problém vyriešiť.

Gaussova eliminačná metóda.

Predpokladajme, že niektorý z koeficientov pri x_1 v S je nenulový. Môžeme priamo predpokladať, že $a_{11} \neq 0$.

1. krok. Pomocou prvej rovnice vylúčime x_1 z druhej $\dots$, s -tej rovnice. Takto: k druhej rovnici prirátame $-(a_{11}^{-1}a_{21})$ -násobok prvej rovnice, $\dots$ atď, až k s -tej rovnici prirátame $-(a_{11}^{-1}a_{s1})$ -násobok prvej rovnice. Dostaneme ekvivalentný systém S^* tvaru:

$$a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1$$

$$\bar{a}_{22}x_2 + \cdots + \bar{a}_{2n}x_n = b_2$$

$$\vdots$$

$$\bar{a}_{s2}x_2 + \cdots + \bar{a}_{sn}x_n = b_n$$

V S^* môžu byť rovnice s ľavou aj pravou stranou nulovou, tie vynecháme. V S^* sa môže vyskytnúť rovnica s ľavou stranou nulovou, kým jej pravá strana je nenulová. Ak sa stane takéto niečo, potom systém S^* a teda aj S je *neriešiteľný*.

Po konečnom počte opakovaní prvého kroku dostaneme systém V tvaru:

$$c_{11}y_1 + c_{12}y_2 + \cdots + c_{1k}y_k + \cdots + c_{1n}y_n = d_1$$

$$c_{22}y_2 + \cdots + c_{2k}y_k + \cdots + c_{2n}y_n = d_2$$

$$\vdots$$

$$c_{kk}y_k + \cdots + c_{kn}y_n = d_k$$

kde $y_1, \dots, y_n$ vznikli (príp. viacnásobným) premenovaním neznámych $x_1, \dots, x_n$, pritom $k \leq s$ a $k \leq n$. Navyše $c_{11} \neq 0, \dots, c_{ii} \neq 0, \dots, c_{kk} \neq 0$. Ak $k=n$, tak V vyzerá takto:

$$\begin{aligned} c_{11}y_1 + \dots + c_{1n}y_n &= d_1 \\ c_{21}y_1 + \dots + c_{2n}y_n &= d_2 \\ &\vdots \\ c_{n-1,n-1}y_{n-1} + c_{n-1,n}y_n &= d_{n-1} \\ c_{nn}y_n &= d_n \end{aligned}$$

a teda vyrátame z poslednej rovnice $y_n = d_n c_{nn}^{-1}$, dosadíme do predposlednej, z nej vyrátame $y_{n-1}, \dots$ atď, až napokon y_1 . Vtedy V má práve jedno riešenie. Spätným premenovaním dostaneme tú jedninú n -ticu v R , ktorá je riešením systému S .

Ak $k < n$, tak $y_1, \dots, y_k$ sú viazané rovnicami systému V , kým neznáme $y_{k+1}, \dots, y_n$ považujeme za tzv. voľné neznáme (parametre), nadobúdajú ľubovoľné hodnoty z R . Zo systému V potom postupne, počnúc od poslednej rovnice, vyrátame $y_k, y_{k-1}, \dots, y_1$ pomocou parametrov $y_{k+1}, \dots, y_n$. Takto dostaneme všeobecné vyjadrenie riešenia systému V pomocou parametrov $y_{k+1}, \dots, y_n$. Spätným premenovaním neznámych dostaneme z toho všeobecné vyjadrenie riešenia systému S pomocou $n-k$ parametrov.

V. LINEÁRNA ZÁVISLOSŤ A NEZÁVISLOSŤ VEKTOROV

Definícia 5.1. Nech V je vektorový priestor nad R a nech $\vec{x}_1, \dots, \vec{x}_k \in V$ sú dané vektory. Hovoríme, že $\vec{x}_1, \dots, \vec{x}_k$ sú *lineárne závislé*, ak $\vec{0}$ sa dá vyjadriť ako netriviálna lineárna kombinácia vektorov $\vec{x}_1, \dots, \vec{x}_k$. Vektory $\vec{x}_1, \dots, \vec{x}_k$ sa nazývajú *lineárne nezávislé* ak nie sú lineárne závislé.

Veta 5.1. Nech $\vec{x}_1, \dots, \vec{x}_k$ sú navzájom rôzne nenulové vektory vektorového priestoru V nad R , nech $k \geq 2$. Potom platí: $\vec{x}_1, \dots, \vec{x}_k$ sú lineárne závislé $\Leftrightarrow$ niektorý z nich je lineárna kombinácia ostatných.

Dôkaz.

Predpokladajme, že $\vec{x}_1, \dots, \vec{x}_k$ sú lineárne závislé. Teda existujú $\alpha_1, \dots, \alpha_k \in R$ nie všetky nulové, také, že $\vec{0} = \sum_{i=1}^k \alpha_i \vec{x}_i$. Povedzme, že $\alpha_i \neq 0$, teda $\alpha_1 \vec{x}_1 + \dots + \alpha_i \vec{x}_i + \dots + \alpha_k \vec{x}_k = \vec{0}$. Z toho: $\alpha_i \vec{x}_i = -\alpha_1 \vec{x}_1 - \dots - \alpha_{i-1} \vec{x}_{i-1} - \alpha_{i+1} \vec{x}_{i+1} - \dots - \alpha_k \vec{x}_k$, teda: $\vec{x}_i = -\alpha_i^{-1} \cdot \sum_{j=1, j \neq i}^k \alpha_j \vec{x}_j$.

Opačne: Predpokladajme, že napr. $\vec{x}_i$ je lineárnou kombináciou ostatných.

Teda $\vec{x}_i = \sum_{j=1, j \neq i}^k \beta_j \vec{x}_j \Rightarrow \beta_1 \vec{x}_1 + \dots + \beta_{i-1} \vec{x}_{i-1} - \beta_i \vec{x}_i + \beta_{i+1} \vec{x}_{i+1} + \dots + \beta_k \vec{x}_k = \vec{0}$.

Teda $\vec{x}_1, \dots, \vec{x}_k$ sú lineárne závislé. □

Veta 5.2. Nech V je vektorový priestor nad R , nech $\{\vec{x}_1, \dots, \vec{x}_k\} \subset V - \{\vec{0}\}$. Potom $\vec{x}_1, \dots, \vec{x}_k$ sú lineárne závislé práve vtedy, keď niektorý z týchto vektorov je lineárnou kombináciou tých, čo sú napísané pred ním.

Dôkaz.

Predpokladajme, že $\vec{x}_1, \dots, \vec{x}_k$ sú lineárne závislé. Teda existujú $\alpha_1, \dots, \alpha_k \in R$ nie všetky nulové také, že $\vec{0} = \sum_{i=1}^k \alpha_i \vec{x}_i$. Nech j je najvyšší index taký, že $\alpha_j \neq 0$. Teda

$\vec{0} = \sum_{i=1}^j \alpha_i \vec{x}_i$, pričom $\alpha_j \neq 0$. Potom $j \geq 2$, lebo keby $j=1$, tak by sme mali $\alpha_1 \vec{x}_1 = \vec{0}$,

$\alpha_1 \neq 0$, teda $\vec{x}_1 = \vec{0}$ – spor.

Opačne: Nech niektorý z $\vec{x}_1, \dots, \vec{x}_k$ je lineárnou kombináciou tých, čo sú napísané pred ním. Potom je lineárnou kombináciou aj ostatných, lebo stačí tie, čo sú za ním zobrať s koeficientom 0. Z Vety 5.1 sú lineárne závislé. □

Dôsledok. Nech V je vektorový priestor nad R , nech $\{\vec{x}_1, \dots, \vec{x}_k\} \subset V - \{\vec{0}\}$. Potom $\vec{x}_1, \dots, \vec{x}_k$ sú lineárne závislé práve vtedy, keď existuje $j \in \{1, 2, \dots, k\}$, že $[\vec{x}_1, \dots, \vec{x}_k] = [\vec{x}_1, \dots, \vec{x}_{j-1}, \vec{x}_{j+1}, \dots, \vec{x}_k]$.

Dôkaz. Zrejímavý. □

Poznámka. Z dôsledku vyplýva návod na hľadanie najkratšieho zápisu lineárneho obalu. Ak $\vec{x}_1, \dots, \vec{x}_k$ sú lineárne nezávislé, tak zápis $[\vec{x}_1, \dots, \vec{x}_k]$ je najkratší. Ak $\vec{x}_1, \dots, \vec{x}_k$ sú lineárne závislé, tak niektorý z nich je lineárnou kombináciou ostatných, ten vynecháme, pričom lineárny obal zvyšných: $[\vec{x}_1, \dots, \vec{x}_k]$, ak tie zvyšné vektory sú lineárne nezávislé, tak sme skončili; ak sú lineárne závislé tak opakujeme predchádzajúci krok. Po konečnom počte krokov dostaneme vyjadrenie $[\vec{x}_1, \dots, \vec{x}_k]$ pomocou lineárne nezávislej podmnožiny množiny $\{\vec{x}_1, \dots, \vec{x}_k\}$.

Steinitzova veta. *Nech vektorový priestor $V \neq \{\vec{0}\}$, $V = [\vec{x}_1, \dots, \vec{x}_k]$. Nech $\{\vec{y}_1, \dots, \vec{y}_j\} \subset V$ je lineárne nezávislá podmnožina. Potom platia:*

1° $j \leq k$

2° Spomedzi $\vec{x}_1, \dots, \vec{x}_k$ existuje $k-j$ vektorov, ktoré spolu s $\vec{y}_1, \dots, \vec{y}_j$ generujú celý priestor V .

Dôkaz. Indukcia vzhľadom na j .

1° Pre $j=1$: $\vec{y}_1$ je lineárne nezávislý práve vtedy, keď $\vec{y}_1 \neq \vec{0}$, pretože $V \neq \{\vec{0}\}$, máme $j=1 \leq k$. Teda 1° platí. Máme $V = [\vec{x}_1, \dots, \vec{x}_k]$, ale $\vec{y}_1 \in V$ t.j. $\vec{y}_1$ je lineárna kombinácia $\vec{x}_1, \dots, \vec{x}_k$, teda množina $\{\vec{y}_1, \vec{x}_1, \dots, \vec{x}_k\}$ je lineárne závislá. Potom $V = [\vec{x}_1, \dots, \vec{x}_k] = [\vec{y}_1, \vec{x}_1, \dots, \vec{x}_k]$. Vektory $\vec{y}_1, \vec{x}_1, \dots, \vec{x}_k$ sú lineárne závislé, teda niektorý z nich je lineárna kombinácia tých, čo sú napísané pred ním. $\vec{y}_1$ to nemôže byť, teda je to niektorý spomedzi $\vec{x}_1, \dots, \vec{x}_k$. Povedzme, že to je $\vec{x}_k$. Potom $V = [\vec{x}_1, \dots, \vec{x}_k] = [\vec{y}_1, \vec{x}_1, \dots, \vec{x}_{k-1}]$. Tým sme overili, že platí 2°.

2° Predpokladajme, že veta platí pre $j=s-1$. Nech teraz $\{\vec{y}_1, \dots, \vec{y}_s\}$ je ľubovoľná lineárne nezávislá podmnožina vo V . Chceme ukázať, že veta platí aj pre $j=s$. Aj množina $\{\vec{y}_1, \dots, \vec{y}_{s-1}\}$ je lineárne nezávislá. Podľa indukčného predpokladu 1° platí: $s-1 \leq k$ a 2° $\vec{y}_1, \dots, \vec{y}_{s-1}$ sa dajú $k-(s-1)$ vektormi spomedzi $\vec{x}_1, \dots, \vec{x}_k$ doplniť tak, že spolu generujú celý priestor V . Povedzme, že tie "doplňujúce" vektory sú $\vec{x}_1, \dots, \vec{x}_{k-s+1}$. Teda $V = [\vec{x}_1, \dots, \vec{x}_k] = [\vec{y}_1, \dots, \vec{y}_{s-1}, \vec{x}_1, \dots, \vec{x}_{k-s+1}]$. Chceme ukázať, že $s \leq k$. Ukážeme, že $s-1 < k$. Keby $s-1=k$ tak by sme mali, že $V = [\vec{x}_1, \dots, \vec{x}_k] = [\vec{y}_1, \dots, \vec{y}_{s-1}]$. Ale $\vec{y}_s \in V$, teda by mal byť lineárnou kombináciou vektorov $\vec{y}_1, \dots, \vec{y}_{s-1}$, to je spor s tým, že $\vec{y}_1, \dots, \vec{y}_s$ sú lineárne nezávislé. Ďalej: $V = [\vec{x}_1, \dots, \vec{x}_k] = [\vec{y}_1, \dots, \vec{y}_s, \vec{x}_1, \dots, \vec{x}_{k-s+1}]$. Teraz $\vec{y}_s \in V$, teda $\vec{y}_s$ je lineárna kombinácia vektorov $\vec{y}_1, \dots, \vec{y}_{s-1}, \vec{x}_1, \dots, \vec{x}_{k-s+1}$. Teda $\vec{y}_1, \dots, \vec{y}_s, \vec{x}_1, \dots, \vec{x}_{k-s+1}$ sú lineárne závislé. Z vety vieme, že niektorý z nich je lineárna kombinácia tých, čo sú pred ním. Nemôže to byť žiadny spomedzi $\vec{y}_1, \dots, \vec{y}_s$, lebo sú lineárne nezávislé a teda je to niektorý spomedzi $\vec{x}_1, \dots, \vec{x}_{k-s+1}$, povedzme, že to je posledný $\vec{x}_{k-s+1}$. Ten môžeme vynechať a podľa vety 5.2: $V = [\vec{y}_1, \dots, \vec{y}_s, \vec{x}_1, \dots, \vec{x}_{k-s}]$. Teda aj 2° je pre $\vec{y}_1, \dots, \vec{y}_s$ v poriadku. □

Báza a dimenzia.

$V = [\vec{x}_1, \dots, \vec{x}_k]$. Dá sa každý vektorový priestor napísať ako lineárny obal konečnej množiny vektorov? (t.j. dá sa generovať konečnou množinou)
Odpoveď: NIE.

Príklad. $\mathbb{R}[t]$ všetky polynómy. $p(t) = \sum_{i=0}^{\infty} a_i t^i$ iba konečne veľa a_i je nenulový. $\mathbb{R}[t]$ je

vektorový priestor nad $\mathbb{R}$. Stupeň $\sum_{i=0}^{\infty} a_i t^i$ je s , ak $s \neq 0$, ale $a_{s+1}, \dots$ sú nuly. Keby existovali polynómy $q_1(t), \dots, q_k(t) \in \mathbb{R}[t]$ také, že $\mathbb{R}[t] = [q_1(t), \dots, q_k(t)]$, tak potom pre $n > \max\{\deg(q_1(t)), \dots, \deg(q_k(t))\}$ by polynóm $t^n \notin \mathbb{R}[t]$. Teda vektorový priestor $\mathbb{R}[t]$ sa nedá generovať konečnou množinou.

Definícia 5.2. Vektorový priestor V sa nazýva *konečne generovaný* ak existuje konečná množina $\{\vec{x}_1, \dots, \vec{x}_k\} \subset V$ taká, že $V = [\vec{x}_1, \dots, \vec{x}_k]$. Ak V nie je konečne generovaný, hovoríme, že je nekonečne generovaný.

Definícia 5.3. Nech $V \neq \{\vec{0}\}$ je konečne generovaný vektorový priestor nad R . Potom usporiadaná množina $(\vec{a}_1, \dots, \vec{a}_k)$ vektorov z V sa nazýva *báza* priestoru V , ak:

1°: $V = [\vec{a}_1, \dots, \vec{a}_k]$.

2°: $\vec{a}_1, \dots, \vec{a}_k$ sú lineárne nezávislé.

Veta 5.3. Každý konečne generovaný vektorový priestor $V \neq \{\vec{0}\}$ nad R má bázu.

Dôkaz. Keďže V je konečne generovaný, existuje konečná množina $\{\vec{x}_1, \dots, \vec{x}_p\} \subset V$, pre ktorú $[\vec{x}_1, \dots, \vec{x}_p] = V$. Ak $\vec{x}_1, \dots, \vec{x}_p$ sú lineárne nezávislé, tak tvoria bázu. Ak nie, tak niektorý z nich je lineárna kombinácia zvyšných, potom lineárny obal zvyšných $= V$. Ak tie zvyšné sú lineárne nezávislé, tak tieto tvoria bázu priestoru V , ak sú lineárne závislé, tak zas zopakujeme predchádzajúcu úvahu. Po konečnom počte krokov dostaneme podmnožinu množiny $\{\vec{x}_1, \dots, \vec{x}_p\}$, ktorá už je lineárne nezávislá a jej lineárny obal je celé V . Tá je báza priestoru V . $\square$

Príklad.

$\mathbb{R}^n$ má bázu: $[(1, 0, \dots, 0), (0, 1, \dots, 0), \dots, (0, 0, \dots, 1)] = [\vec{e}_1, \vec{e}_2, \dots, \vec{e}_n]$. To je tzv. štandardná báza v $\mathbb{R}^n$.

Veta 5.4. Všetky bázy nenulového konečne generovaného vektorového priestoru majú rovnaký počet prvkov.

Dôkaz. Nech $(\vec{a}_1, \dots, \vec{a}_s), (\vec{b}_1, \dots, \vec{b}_q)$ sú dve bázy takého vektorového priestoru. Potom zo Steinitzovej vety: $s \leq q$ a $q \leq s$ a teda $s = q$. $\square$

Definícia 5.4. Počet prvkov (ľubovoľnej) bázy konečne generovaného nenulového vektorového priestoru V nad R sa nazýva *dimenzia* priestoru V nad poľom R , ozn: $\dim_R(V)$ (alebo $\dim(V)$ ak je R jasné z kontextu).

Dimenzia nulového priestoru je 0. $\dim(\{\vec{0}\}) = 0$

Dimenzia priestoru, ktorý je nekonečne generovaný je ∞ . $\dim(V) = \infty$.

Príklady.

1. $\dim_{\mathbb{C}} \mathbb{C} = 1$
2. $\dim_{\mathbb{R}} \mathbb{C} = 2$
3. $\dim \mathbb{R}^n = n$
4. $\dim \mathbb{R}[t] = \infty$

Veta 5.5. Každú lineárne nezávislú množinu nenulového konečne generovaného vektorového priestoru môžeme doplniť na jeho bázu.

Dôkaz. Nech V je taký priestor, nech $\{\vec{y}_1, \dots, \vec{y}_j\} \subset V$ je lineárne nezávislá. Keďže V je konečne generovaný, existujú $\vec{x}_1, \dots, \vec{x}_k \in V$. $(\vec{x}_1, \dots, \vec{x}_k)$ je báza vo V . Zo Steinitzovej vety: $j \leq k$, $\vec{y}_1, \dots, \vec{y}_j$ sa dajú doplniť $k-j$ vektormi spomedzi $\vec{x}_1, \dots, \vec{x}_k$ tak, že týchto k vektorov generuje celé V . Tieto vektory však musia byť aj lineárne nezávislé. (Keby boli lineárne závislé, tak by V mal bázu s najviac $k-1$ prvkami. Spor s dimenziou.) Teda $\vec{y}_1, \dots, \vec{y}_j$ spolu s tými, doplnujúcimi vektormi tvoria bázu priestoru V . $\square$

Veta 5.6. Ak $\dim(V) = n$, tak $n+1$ vektorov z V je vždy lineárne závislých.

Dôkaz. $\dim(V) = n$, teda vo V existuje n -prvková báza $(\vec{a}_1, \dots, \vec{a}_n)$. Keby ľubovoľná $n+1$ -prvková množina lineárne nezávislá, tak podľa Steinitzovej vety by bolo $n+1 \leq n$, čo je spor. $\square$

Veta 5.7. Nech $\dim(V) = n$. Potom:

1. usporiadaná množina $(\vec{a}_1, \dots, \vec{a}_n)$ n vektorov z V je bázou vo V práve vtedy, keď $\{\vec{a}_1, \dots, \vec{a}_n\}$ je lineárne nezávislá.
2. $(\vec{a}_1, \dots, \vec{a}_n)$ je bázou vo V práve vtedy, keď $V = [\vec{a}_1, \dots, \vec{a}_n]$.

Dôkaz.

1. $\Rightarrow$: jasné.

$\Leftarrow$: Predpokladajme, že $\{\vec{a}_1, \dots, \vec{a}_n\}$ je lineárne nezávislá. Podľa vety 5.5 túto množinu môžeme doplniť $n-n=0$ vektormi z V na bázu vo V . t.j. už $(\vec{a}_1, \dots, \vec{a}_n)$ je báza.

2. $\Rightarrow$: jasné

$\Leftarrow$: Predpokladajme, že $V=[\vec{a}_1, \dots, \vec{a}_n]$. Chceme ukázať, že $\vec{a}_1, \dots, \vec{a}_n$ sú aj lineárne nezávislé. Keby boli lineárne závislé, postupným vynechávaním tých, ktoré sú lineárnou kombináciou zvyšných by sme dostali bázu, ktorá by mala najvyšš $n-1$ prvkov. Spor s tým, že $\dim(V)=n$. Teda všetky bázy majú n prvkov. $\square$

Veta 5.8 a Definícia 5.5. *Nech $V \neq \{\vec{0}\}$ je konečne generovaný vektorový priestor nad R . Potom množina $(\vec{a}_1, \dots, \vec{a}_n)$ je bázou vo V práve vtedy, keď každý vektor z V sa dá jediným spôsobom vyjadriť ako lineárna kombinácia vektorov $\vec{a}_1, \dots, \vec{a}_n$. Ak $(\vec{a}_1, \dots, \vec{a}_n)$ je báza vo V a pre $\vec{x} \in V$ máme $\vec{x} = x_1\vec{a}_1 + \dots + x_n\vec{a}_n$. Tak usporiadaná n -tica $(x_1, \dots, x_n) \in \mathbb{R}^n$ sa nazýva n -tica súradníc vektora $\vec{x}$ vzhľadom na bázu $(\vec{a}_1, \dots, \vec{a}_n)$.*

Dôkaz.

$\Rightarrow$: Predpokladajme, že $(\vec{a}_1, \dots, \vec{a}_n)$ je báza v priestore V . Teda $V=[\vec{a}_1, \dots, \vec{a}_n]$ t.j. pre ľubovoľný vektor $\vec{x} \in V$ $\exists x_1, \dots, x_n \in R$ také, že $\vec{x} = x_1\vec{a}_1 + \dots + x_n\vec{a}_n$. Keby $\vec{x} = x'_1\vec{a}_1 + \dots + x'_n\vec{a}_n$ bolo iné také vyjadrenie, tak $x_1\vec{a}_1 + \dots + x_n\vec{a}_n = x'_1\vec{a}_1 + \dots + x'_n\vec{a}_n \Leftrightarrow (x_1 - x'_1)\vec{a}_1 + \dots + (x_n - x'_n)\vec{a}_n = \vec{0}$. Ale $\vec{a}_1, \dots, \vec{a}_n$ tvoria bázu, sú aj lineárne nezávislé, preto $x_1 - x'_1 = 0, \dots, x_n - x'_n = 0 \Leftrightarrow x_i = x'_i$. čsmd.

$\Leftarrow$: Predpokladajme, že každý vektor z V sa dá jediným spôsobom vyjadriť ako lineárna kombinácia $\vec{a}_1, \dots, \vec{a}_n$. Teda $V \subset [\vec{a}_1, \dots, \vec{a}_n]$. Ešte ukážeme, že $\vec{a}_1, \dots, \vec{a}_n$ sú lineárne nezávislé. Nech $\alpha_1\vec{a}_1 + \dots + \alpha_n\vec{a}_n = \vec{0}$. Tiež: $0\vec{a}_1 + \dots + 0\vec{a}_n = \vec{0}$, keďže vyjadrenie 0 ako lineárna kombinácia vektorov $\vec{a}_1, \dots, \vec{a}_n$ je podľa predpokladu jediné, tak máme: $\alpha_1 = \dots = \alpha_n = 0$. $\square$

VI. LINEÁRNE A DIREKTNÉ SÚČTY VEKTOROVÝCH PRIESTOROV

Ak S, T sú vektorové podpriestory vektorového priestoru V , tak $S \cup T$ nemusí byť vektorový podpriestor vo V . Aký je najmenší podpriestor vo V , obsahujúci $S \cup T$?

Veta 6.1 a Definícia 6.1. *Nech $S, T \subset V$ sú vektorové podpriestory. Potom $\{\vec{s} + \vec{t} \in V, \vec{s} \in S, \vec{t} \in T\}$ je vektorový podpriestor vo V , nazýva sa lineárny súčet S a T , ozn. $S + T$.*

Dôkaz. $\vec{0} \in \{\vec{s} + \vec{t} \in V, \vec{s} \in S, \vec{t} \in T\} \neq \emptyset$, lebo $\vec{0} + \vec{0} = \vec{0}$. Ak $\vec{x}, \vec{y} \in \{\vec{s} + \vec{t}, \vec{s} \in S, \vec{t} \in T\}$, tak $\vec{x} = \vec{s}_1 + \vec{t}_1, \vec{y} = \vec{s}_2 + \vec{t}_2$, potom $\alpha\vec{x} + \beta\vec{y} = \alpha(\vec{s}_1 + \vec{t}_1) + \beta(\vec{s}_2 + \vec{t}_2) = \underbrace{(\alpha\vec{s}_1 + \beta\vec{s}_2)}_{\in S} + \underbrace{(\alpha\vec{t}_1 + \beta\vec{t}_2)}_{\in T}$,

teda $\alpha\vec{x} + \beta\vec{y} \in \{\vec{s} + \vec{t}, \vec{s} \in S, \vec{t} \in T\}$. □

Tvrdenie. $S + T$ je najmenší podpriestor obsahujúci $S \cup T$.

Lema 6.1. *Ak P je vektorový podpriestor konečne generovaného vektorového priestoru V , tak aj P je konečne generovaný.*

Dôkaz. : dú. □

Veta 6.2. *Predpokladajme, že V je konečne generovaný vektorový priestor nad R , nech S, T sú jeho podpriestory. Potom $\dim(S + T) = \dim(S) + \dim(T) - \dim(S \cap T)$.*

Dôkaz.

1. Predpokladajme, že $S \cap T = \{\vec{0}\}$. Nech $\vec{x}_1, \dots, \vec{x}_s$ je báza v S , $(\vec{y}_1, \dots, \vec{y}_t)$ je báza v T . Potom $S + T = [\vec{x}_1, \dots, \vec{x}_s, \vec{y}_1, \dots, \vec{y}_t]$. Navyše $(\vec{x}_1, \dots, \vec{x}_s, \vec{y}_1, \dots, \vec{y}_t)$ je báza v $S + T$. Stačí ukázať ich lineárna nezávislosť. Keby boli lineárne závislé, potom jeden z nich by bol lineárna kombináciou tých, čo sú pred ním. Nemôže byť žiadny z $\vec{x}_1, \dots, \vec{x}_s$, lebo tie tvoria bázu v S . Teda musí to byť dajaké $\vec{y}_i$: $\vec{y}_i = a_1\vec{x}_1 + \dots + a_s\vec{x}_s + b_1\vec{y}_1 + \dots + b_{i-1}\vec{y}_{i-1}$, z toho $\underbrace{\vec{y}_i - b_1\vec{y}_1 - \dots - b_{i-1}\vec{y}_{i-1}}_{\neq \vec{0}, \in T \cap S = \{\vec{0}\}, \text{ spor}} = a_1\vec{x}_1 +$

$+\dots + a_s\vec{x}_s$. $\dim(S + T) = s + t = \dim(S) + \dim(T)$.

2. $S \cap T \neq \{\vec{0}\}$: Nech $(\vec{z}_1, \dots, \vec{z}_r)$ je báza v $S \cap T$. $S \cap T$ je podpriestor v S aj v T . Podľa *Steinitzovej vety* doplníme $(\vec{z}_1, \dots, \vec{z}_r)$ na bázu $(\vec{z}_1, \dots, \vec{z}_r, \vec{x}_1, \dots, \vec{x}_s)$ v S resp. na bázu $(\vec{z}_1, \dots, \vec{z}_r, \vec{y}_1, \dots, \vec{y}_t)$ v T . Teda $\dim(S) = r + s, \dim(T) = r + t$. Máme $S + T = [\vec{z}_1, \dots, \vec{z}_r, \vec{x}_1, \dots, \vec{x}_s, \vec{y}_1, \dots, \vec{y}_t]$. Navyše $\vec{z}_1, \dots, \vec{z}_r, \vec{x}_1, \dots, \vec{x}_s, \vec{y}_1, \dots, \vec{y}_t$ sú lineárne nezávislé, teda tvoria bázu v $S + T$. Nech by boli lineárne závislé. Teda niektorý je lineárna kombinácia tých, čo sú pred ním. Nemôže to byť žiadny spomedzi $\vec{z}_1, \dots, \vec{z}_r, \vec{x}_1, \dots, \vec{x}_s$ lebo tvoria bázu v S . Teda existuje i :

$$(*) \quad \vec{y}_i = \gamma_1\vec{z}_1 + \dots + \gamma_r\vec{z}_r + \alpha_1\vec{x}_1 + \dots + \alpha_s\vec{x}_s + \beta_1\vec{y}_1 + \dots + \beta_{i-1}\vec{y}_{i-1}.$$

Z toho $\underbrace{\vec{y}_i - \beta_1\vec{y}_1 - \dots - \beta_{i-1}\vec{y}_{i-1}}_{\in T} = \underbrace{\gamma_1\vec{z}_1 + \dots + \gamma_r\vec{z}_r + \alpha_1\vec{x}_1 + \dots + \alpha_s\vec{x}_s}_{\in S} \in S \cap T \Rightarrow$

$\Rightarrow \gamma_1\vec{z}_1 + \dots + \gamma_r\vec{z}_r + \alpha_1\vec{x}_1 + \dots + \alpha_s\vec{x}_s = \delta_1\vec{z}_1 + \dots + \delta_r\vec{z}_r \Leftrightarrow (\gamma_1 - \delta_1)\vec{z}_1 + \dots + (\gamma_r - \delta_r)\vec{z}_r + \alpha_1\vec{x}_1 + \dots + \alpha_s\vec{x}_s = \vec{0}$. Z toho, že $\vec{z}_1, \dots, \vec{z}_r, \vec{x}_1, \dots, \vec{x}_s$ sú lineárne nezávislé máme, že $\alpha_1 = \dots = \alpha_s = 0$. Teda z (*): $\vec{y}_i = \gamma_1\vec{z}_1 + \dots + \gamma_r\vec{z}_r + \beta_1\vec{y}_1 + \dots + \beta_{i-1}\vec{y}_{i-1}$ spor s tým, že $(\vec{z}_1, \dots, \vec{z}_r, \vec{y}_1, \dots, \vec{y}_t)$ je báza. Teda naozaj $(\vec{z}_1, \dots, \vec{z}_r, \vec{y}_1, \dots, \vec{y}_t, \vec{x}_1, \dots, \vec{x}_s)$ je báza v $S + T$. Teda $\dim(S + T) = r + s + t = \dim(S) + r + t - r = \dim(S) + \dim(T) - \dim(S \cap T)$. □

Definícia 6.2. Ak S, T sú vektorové podpriestory priestoru V a $S \cap T = \{\vec{0}\}$, tak vektorový podpriestor $S + T$ sa nazýva *direktný súčet* vektorových podpriestorov S a T . ozn. $S \oplus T$.

Dôsledok formuly dimenzie: Ak S, T sú podpriestory konečne generovaného vektorového priestoru V a $S \cap T = \{\vec{0}\}$, tak $\dim(S \oplus T) = \dim(S) + \dim(T)$. Teraz vieme, že ak $(\vec{x}_1, \dots, \vec{x}_s)$ je báza v S , a $(\vec{y}_1, \dots, \vec{y}_t)$ je báza v T , tak $(\vec{x}_1, \dots, \vec{x}_s, \vec{y}_1, \dots, \vec{y}_t)$ je báza pre $(S \oplus T)$.

Veta 6.3. *Nech S, T, P sú vektorové podpriestory priestoru V . Potom P je direktným súčtom S a T ($P = S \oplus T$) práve vtedy, keď každý vektor z P sa dá jediným spôsobom vyjadriť ako súčet vektora z S a vektora z T .*

Dôkaz.

$\Rightarrow$: Predpokladajme, že $P = S \oplus T$. Potom je samozrejme pravda, že každý vektor z P je súčet vektora z S a vektora z T . Nech by existovali dve takéto vyjadrenia $\vec{x} \in P$: $\vec{x} = \vec{s}_1 + \vec{t}_1 = \vec{s}_2 + \vec{t}_2$, $\vec{s}_1, \vec{s}_2 \in S, \vec{t}_1, \vec{t}_2 \in T$. Potom $\vec{s}_2 - \vec{s}_1 = \vec{t}_1 - \vec{t}_2 \in (S \cap T) = \{\vec{0}\} \Rightarrow \vec{s}_1 = \vec{s}_2$ a $\vec{t}_1 = \vec{t}_2$.

$\Leftarrow$: Predpokladajme, že každý vektor z P má jediné vyjadrenie v tvare "vektor z S + vektor z T ". Teda $P = S + T$. Teraz nech $\vec{a} \in S \cap T$. Potom $\vec{a} = \underbrace{\vec{a}}_{\in S} + \underbrace{\vec{0}}_{\in T} = \underbrace{\vec{0}}_{\in S} + \underbrace{\vec{a}}_{\in T}$, keďže takéto vyjadrenie je jediné, máme $\vec{a} = \vec{0}$. Dokázali sme, že $S \cap T = \{\vec{0}\}$. Vcelku: $P = S \oplus T$.

□

VII. MATICE

Definícia 7.1. *Matica* typu $k \times s$ nad poľom R je tabuľka (obdĺžniková), v ktorej $k \cdot s$ prvkov z R rozmiestňujeme do k riadkov a s stĺpcov. Všeobecný zápis:

$$\begin{pmatrix} a_{11} & \cdots & a_{1s} \\ a_{21} & \cdots & a_{2s} \\ \vdots & \ddots & \vdots \\ a_{k1} & \cdots & a_{ks} \end{pmatrix}$$

$a_{ij} \in R$, i —riadkový index, j —stĺpcový index. Matice označujeme: $\mathbf{A}, \mathbf{B}, \dots$. Stručnejší všeobecný zápis: $\mathbf{A} = (a_{ij})_{k,s}$ alebo len $\mathbf{A} = (a_{ij})$ ak k, s je jasné z kontextu. Ak $\mathbf{A} = (a_{ij})_{k,s}$ kde $k=s$, tak $\mathbf{A}$ sa volá štvorcová matica stupňa k .

Jednotková matica stupňa n :

$$\mathbf{I}_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

Definícia 7.2. Dve matice toho istého typu nad tým istým poľom *sa rovnajú*, ak na všetkých zodpovedajúcich miestach majú rovnaké prvky. $\mathbf{A} = (a_{ij})_{k,s}$, $\mathbf{B} = (b_{uv})_{m,n}$ obidve nad $\mathbb{R}$. $\mathbf{A} = \mathbf{B}$ znamená, že $k=m$, $s=n$, $a_{ij} = b_{ij}$ pre všetky $i=1, \dots, k$ a $j=1, \dots, s$.

Označenie. Množina všetkých matíc typu $k \times s$ nad $\mathbb{R}$ označíme: $\mathfrak{M}_{k,s}(\mathbb{R})$.

Definícia 7.3. Ak $\mathbf{A}, \mathbf{B} \in \mathfrak{M}_{k,s}(\mathbb{R})$, tak definujeme ich súčet ako maticu, ktorú ozn. $\mathbf{A} + \mathbf{B}$; je typu $k \times s$; jej prvok i -teho riadku a j -teho stĺpca je súčet $a_{ij} + b_{ij}$.

Veta 7.1. $(\mathfrak{M}_{k,s}, +)$ je komutatívna grupa.

Dôkaz. Asociatívnosť operácie $+$ vyplýva z asociatívnosti operácie $+$ v poli $\mathbb{R}$. Neutrálny prvok je matica, ktorej všetky prvky sú $0 \in \mathbb{R}$ t.j. tzv. nulová matica. Inverzný prvok k matici $\mathbf{A} = (a_{ij})$ je matica $-\mathbf{A} = (-a_{ij})$. Komutatívnosť vyplýva z komutatívnosti operácie $+$ v poli $\mathbb{R}$.

□

Definícia 7.4. Pre $\alpha \in \mathbb{R}$, $\mathbf{A} = (a_{ij}) \in \mathfrak{M}_{k,s}(\mathbb{R})$ definujeme α -násobok matice $\mathbf{A}$ ako maticu, ktorú označíme $\alpha \mathbf{A} = (\alpha a_{ij}) \in \mathfrak{M}_{k,s}(\mathbb{R})$

Veta 7.2. $\mathfrak{M}_{k,s}(\mathbb{R})$ s vyššie definovaným sčítaním resp. násobením je vektorový priestor nad $\mathbb{R}$. $\alpha(\mathbf{A} + \mathbf{B}) = \alpha((a_{ij}) + (b_{ij})) = (\alpha(a_{ij}) + (\alpha(b_{ij}))) = \alpha(a_{ij}) + \alpha(b_{ij})$.

Tvrdenie 7.1. Ak definujeme $\mathbf{E}_{ij} \in \mathfrak{M}_{k,s}(\mathbb{R})$ ako maticu, ktorá má v i -tom riadku a j -tom stĺpci 1 a všetky ostatné prvky nulové, tak $\mathfrak{M}_{k,s}(\mathbb{R})$ je generovaný takýmito maticami $\mathbf{E}_{ij}$, $i=1, \dots, k$ $j=1, \dots, s$. Navyše $\mathbf{E}_{ij}$, $i=1, \dots, k$ $j=1, \dots, s$ sú lineárne nezávislé a teda tvoria bázu priestoru $\mathfrak{M}_{k,s}(\mathbb{R})$. Z toho: $\dim(\mathfrak{M}_{k,s}(\mathbb{R})) = k \cdot s$.

Dôkaz. Nech $\mathbf{A} = \begin{pmatrix} a_{11} & \cdots & a_{1s} \\ \vdots & \ddots & \vdots \\ a_{k1} & \cdots & a_{ks} \end{pmatrix} \in \mathfrak{M}_{k,s}(\mathbb{R})$. Potom $\mathbf{A} = \sum_{\substack{1 \leq i \leq k \\ 1 \leq j \leq s}} a_{ij} \mathbf{E}_{ij}$. Teda $\mathbf{E}_{ij}$ generujú $\mathfrak{M}_{k,s}(\mathbb{R})$. Nech $\begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1s} \\ \vdots & \ddots & \vdots \\ \alpha_{k1} & \cdots & \alpha_{ks} \end{pmatrix} = \sum_{\substack{1 \leq i \leq k \\ 1 \leq j \leq s}} \alpha_{ij} \mathbf{E}_{ij} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$ a teda $\alpha_{11} = \cdots = \alpha_{ks} = 0$.

□

Definícia 7.5. Nech $\mathbf{A}=(a_{ij})$ je matica typu $\mathfrak{M}_{k,s}(\mathbb{R})$. Riadky matice $\mathbf{A}$ chápme teraz ako prvky z $\mathbb{R}^s$. Označíme S_A vektorový podpriestor $\mathbb{R}^s$ generovaný riadkami matice $\mathbf{A}$. $S_A=[(a_{11}, \dots, a_{1s}), \dots, (a_{k1}, \dots, a_{ks})]$.

Definícia 7.6. *Elementárna riadková operácia* na matici je každá z týchto úprav (ERO):

1. Vzájomná výmena dvoch riadkov v matici.
2. Vynásobenie ľubovoľného riadku nenulovým skalárom.
3. Prirátanie ľubovoľného násobku riadku k inému riadku.

Definícia 7.7. Nech $\mathbf{A}, \mathbf{B} \in \mathfrak{M}_{k,s}(\mathbb{R})$. Hovoríme, že matica $\mathbf{B}$ je *riadkovo ekvivalentná* s $\mathbf{A}$ (píšeme $\mathbf{A} \approx \mathbf{B}$) ak $\mathbf{B}$ vznikne z $\mathbf{A}$ konečným počtom ERO.

Veta 7.3. *Relácia riadkovej ekvivalencie $\approx$ je relácia ekvivalencie na $\mathfrak{M}_{k,s}(\mathbb{R})$.*

Dôkaz.

1. *Reflexívnosť:* $\mathbf{A} \approx \mathbf{A}$ triviálne.
2. *Symetrickosť:* Nech $\mathbf{A} \approx \mathbf{B}$. Každá ERO sa dá vrátiť naspäť (má inverznú). $\mathbf{B} \approx \mathbf{A}$.
3. *Tranzitívnosť:* $\mathbf{A} \approx \mathbf{B}, \mathbf{B} \approx \mathbf{C} \Rightarrow \mathbf{A} \approx \mathbf{C}$ z definície jasné.

□

Veta 7.4. *Nech $\mathbf{A}, \mathbf{B} \in \mathfrak{M}_{k,s}(\mathbb{R})$. Ak $\mathbf{A} \approx \mathbf{B}$ tak $S_A = S_B$.*

Dôkaz. Stačí dokázať pre prípad, že matica $\mathbf{B}$ vznikla z $\mathbf{A}$ vykonaním práve jedinej ERO.

1. Nech $\mathbf{B}$ vznikla z $\mathbf{A}$ vzájomnou výmenou i -teho a j -teho riadku ($i \leq j$). Riadky v $\mathbf{A}$ označme $\vec{x}_1, \dots, \vec{x}_k$.

Teda $S_B = [\vec{x}_1, \dots, \vec{x}_{i-1}, \vec{x}_j, \vec{x}_{i+1}, \dots, \vec{x}_{j-1}, \vec{x}_i, \vec{x}_{j+1}, \dots, \vec{x}_k]$. Je jasné, že je to to isté ako lineárny obal $[\vec{x}_1, \dots, \vec{x}_k]$.

2. Nech $\mathbf{B}$ vznikla z $\mathbf{A}$ tak, že sme i -tý riadok $\vec{x}_i$ vynásobili $\alpha \neq 0$, $\alpha \in \mathbb{R}$. Teda $S_B = [\vec{x}_1, \dots, \alpha \vec{x}_i, \dots, \vec{x}_k]$. To je to isté ako $[\vec{x}_1, \dots, \vec{x}_i, \dots, \vec{x}_k] = S_A$.

3. $\mathbf{B}$ vznikla z $\mathbf{A}$ pripočítaním α -násobok prvého riadku k druhému. t.j. $\alpha \vec{x}_1 + \vec{x}_2$. Teda $S_B = [\vec{x}_1, \alpha \vec{x}_1 + \vec{x}_2, \vec{x}_3, \dots, \vec{x}_k]$. Ale $[\vec{x}_1, \alpha \vec{x}_1 + \vec{x}_2, \vec{x}_3, \dots, \vec{x}_k] = [\vec{x}_1, \dots, \vec{x}_k] = S_A$. Naozaj: inklúzia $\subset$ je zrejmá. Majme ľubovoľnú lineárnu kombináciu:
 $\alpha_1 \vec{x}_1 + \dots + \alpha_k \vec{x}_k = \alpha_1 \vec{x}_1 + \alpha_2 (\vec{x}_2 + \alpha \vec{x}_1) - \alpha \alpha_2 \vec{x}_1 + \alpha_3 \vec{x}_3 + \dots + \alpha_k \vec{x}_k = (\alpha_1 - \alpha \alpha_2) \vec{x}_1 + \alpha_2 (\vec{x}_2 + \alpha \vec{x}_1) + \alpha_3 \vec{x}_3 + \dots + \alpha_k \vec{x}_k \in [\vec{x}_1, \vec{x}_2 + \alpha \vec{x}_1, \dots, \vec{x}_k]$.

□

Otázka. Platí aj obrátené tvrdenie vo vete 7.4 ?

Odpoveď: Áno.

Definícia 7.8. Hovoríme, že matica $\mathbf{A}=(a_{ij}) \in \mathfrak{M}_{k,s}(\mathbb{R})$

je v *redukovanom trojuholníkovom tvare*, ak:

1. Prvý nenulový prvok (tzv. vedúci prvok) každého nenulového riadku je 1.
2. V stĺpci obsahujúcom vedúci prvok niektorého riadku sú ostatné prvky nulové.
3. Ak a_{ij} a a_{pq} sú vedúce prvky i -teho a p -teho riadku a pritom $i < p$, tak potom $j < q$.
4. Nulové riadky (ak existujú) sú pod všetkými nenulovými.

Príklad.

1. Matica $\begin{pmatrix} 1 & 2 & 3 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ nie je RTM (redukovaná trojuholníková matica).
2. Matica $\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ je RTM.

Poznámka. Ak $\mathbf{A}$ spĺňa len podmienky 3.,4. tak je to matica v tzv. trojuholníkovom tvare. Redukovaná trojuholníková matica typu $k \times k$ je buď nulová, alebo ak neobsahuje nulové riadky, tak je jednotková matica $\mathbf{I}_k$.

Veta 7.5. Nech $\mathbf{A} \in \mathfrak{M}_{k,s}(\mathbb{R})$ je RTM. Potom jej nenulové riadky sú lineárne nezávislé. (platí to už o trojuholníkových maticiach).

Dôkaz. Nech $\mathbf{A}$ je RTM a nech jej nenulové riadky sú $\vec{x}_1, \dots, \vec{x}_r \in R^s$. Vedúce prvky týchto riadkov nech sú v stĺpcoch $t_1 < t_2 < \dots < t_r$. Nech by boli $\vec{x}_1, \dots, \vec{x}_r$ lineárne závislé. Teda existuje $i \in \{1, \dots, r\} : \vec{x}_i = \alpha_1 \vec{x}_1 + \dots + \alpha_{i-1} \vec{x}_{i-1}$. Ale t_i -tá zložka v $\vec{x}_i$ je 1, kým $\vec{x}_1, \dots, \vec{x}_{i-1}$ majú t_i -tú zložku nulovú. Teda má platiť $1=0$ spor. $\square$

Príklad.

$$\begin{pmatrix} 1 & 2 & 3 & -1 \\ 1 & 1 & -1 & 1 \\ 2 & -1 & 1 & 0 \end{pmatrix} \approx \begin{pmatrix} 1 & 2 & 3 & -1 \\ 0 & -1 & -4 & 2 \\ 0 & -5 & -5 & 2 \end{pmatrix} \approx \begin{pmatrix} 1 & 2 & 3 & -1 \\ 0 & 1 & 4 & -2 \\ 0 & 0 & 15 & -8 \end{pmatrix} \approx$$

$$\approx \begin{pmatrix} 1 & 2 & 3 & -1 \\ 0 & 1 & 4 & -2 \\ 0 & 0 & 1 & -\frac{8}{15} \end{pmatrix} \approx \begin{pmatrix} 1 & 0 & 0 & \frac{1}{3} \\ 0 & 1 & 0 & \frac{2}{15} \\ 0 & 0 & 1 & -\frac{8}{15} \end{pmatrix}$$

Veta 7.6. Každá matica je riadkovo ekvivalentná s nejakou RTM-ou.

Dôkaz. Indukcia vzhľadom na počet riadkov v matici.

1° Ak $\mathbf{A}$ má jeden riadok, tak ak je nulový tak OK.

Keď nenulový: $(0, \dots, 0, c \neq 0, \dots) \approx (0, \dots, 0, 1, \dots)$ RTM.

2° Predpokladajme, že veta platí pre všetky matice, ktoré majú k riadkov. Nech $\mathbf{A}$ je matica, ktorá má $k+1$ riadkov. Ak $\mathbf{A}$ je nulová, tak OK. Nech $\mathbf{A} \neq 0$. Nech jej prvý

nenulový stĺpec je p -tý. $\mathbf{A} = \begin{pmatrix} 0 & \dots & 0 & \dots \\ \vdots & \ddots & \vdots & \dots \\ 0 & \dots & a_{ip} \neq 0 & \dots \\ \vdots & \ddots & \vdots & \dots \\ 0 & \dots & \dots & \dots \end{pmatrix}$. Je jasné, že $\mathbf{A} \approx \mathbf{B} = \begin{pmatrix} 0 & \dots & b_{1p} & \dots \\ \vdots & \ddots & \vdots & \dots \\ 0 & \dots & \dots & \dots \end{pmatrix} \approx$

$$\approx \begin{pmatrix} 0 & \dots & 1 & c_{1,p+1} & \dots & c_{1s} \\ 0 & \dots & 0 & c_{2,p+1} & \dots & c_{2s} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & c_{k+1,p+1} & \dots & c_{k+1,s} \end{pmatrix} = \mathbf{C}.$$
 Ozn. $\mathbf{C}' = \begin{pmatrix} c_{2,p+1} & \dots & c_{2s} \\ \vdots & \ddots & \vdots \\ c_{k+1,p+1} & \dots & c_{k+1,s} \end{pmatrix}$. Matica $\mathbf{C}'$ má

iba k riadkov, konečným počtom ERO sa upraví na RTM ozn. ju $\mathbf{D}'$. Teda:

$$\mathbf{D} = \begin{pmatrix} 0 & \dots & 0 & 1 & d_{1,p+1} & d_{1,p+2} & \dots & d_{1,s-1} & d_{1s} \\ 0 & \dots & 0 & 0 & d'_{2,p+1} & d'_{2,p+2} & \dots & d'_{2,s-1} & d'_{2s} \\ 0 & \dots & 0 & 0 & 0 & d'_{3,p+2} & \dots & d'_{3,s-1} & d'_{3s} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & 0 & 0 & \dots & d'_{k,s-1} & d'_{ks} \\ 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & d'_{k+1,s} \end{pmatrix}.$$

$\square$

Definícia 7.9. Nech $\mathbf{A} \in \mathfrak{M}_{k,s}(\mathbb{R})$. Potom číslo $\dim(S_A)$ sa nazýva *hodnota* matice $\mathbf{A}$, ozn. $h(\mathbf{A}) = \dim(S_A)$.

Platí. : $h(\mathbf{A})$ = počet lineárne nezávislých riadkov matice $\mathbf{A}$.

Tvrdenie 7.2. Ak $\mathbf{A} \approx \mathbf{B}$, tak $h(\mathbf{A}) = h(\mathbf{B})$.

Dôkaz. Keďže každú maticu $\mathbf{A}$ môžeme konečným počtom ERO upraviť na RTM $\mathbf{A}' \approx \mathbf{A}$, tak $h(\mathbf{A}) = h(\mathbf{A}')$ = počet nenulových riadkov v $\mathbf{A}'$. $\square$

Príklad. Výpočet hodnoty:

$$1. \mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ -1 & 1 & 2 \end{pmatrix} \approx \begin{pmatrix} 1 & 2 & 3 \\ 0 & 3 & 5 \end{pmatrix} \quad h(\mathbf{A}) = 2.$$

$$2. \mathbf{B} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 6 \end{pmatrix} \approx \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 0 \end{pmatrix} \quad h(\mathbf{B}) = 1.$$

Veta 7.7. *Nech $\mathbf{A}, \mathbf{B} \in \mathfrak{M}_{k,s}(R)$ sú RTM. Ak $S_A = S_B$, tak $\mathbf{A} = \mathbf{B}$.*

Dôkaz. Máme $h(\mathbf{A}) = h(\mathbf{B}) = r$. Nech $\vec{a}_1, \dots, \vec{a}_r$ resp. $\vec{b}_1, \dots, \vec{b}_r$ sú nenulové riadky v $\mathbf{A}$ resp. v $\mathbf{B}$. Nech teraz $s_1 < s_2 < \dots < s_r$ sú stĺpcové indexy vedúcich prvkov riadkov $\vec{a}_1, \dots, \vec{a}_r$, podobne nech $t_1 < t_2 < \dots < t_r$ sú stĺpcové indexy vedúcich prvkov riadkov $\vec{b}_1, \dots, \vec{b}_r$. Keďže $S_A = S_B$, máme $[\vec{a}_1, \dots, \vec{a}_r] = [\vec{b}_1, \dots, \vec{b}_r] \in \mathbb{R}^s$. Každé b_j má jediné vyjadrenie v tvare $\vec{b}_j = \alpha_1 \vec{a}_1 + \dots + \alpha_r \vec{a}_r$. Pre $\vec{b}_j$ nech q je najmenšie také, že $\alpha_q \neq 0$. Teda $\vec{b}_j = \alpha_q \vec{a}_q + \dots + \alpha_r \vec{a}_r$. b_j má prvú nenulovú zložku (t_j)-tú. Vektor vpravo má prvú nenulovú zložku ($=\alpha_q$) s_q -tú. Z rovnosti dostávame, že $1 = \alpha_q, t_j = s_q$. Pre $s_1 < s_2 < \dots < s_r, t_1 < t_2 < \dots < t_r$ máme, že každé s_i sa rovná dákemu t_v . To je možné iba tak, že $s_1 = t_1, \dots, s_r = t_r$. Teda máme, že $\vec{b}_j = \alpha_q \vec{a}_q + \alpha_{q+1} \vec{a}_{q+1} + \dots + \alpha_r \vec{a}_r$. V RTM sú v stĺpci obsahujúcom vedúci prvok riadku ostatné prvky 0, preto: $1 \cdot \alpha_{q+1} = 0 \Rightarrow \alpha_{q+1} = 0$. Podobne pre ostatné, t.j. $\alpha_{q+2} = \dots = \alpha_r = 0$. Teda pre $\forall q : \vec{b}_q = \vec{a}_q$. Záver $\mathbf{A} = \mathbf{B}$. □

Dôsledok. *Každá matica je riadkovo ekvivalentná s jedinou RTM.*

Dôkaz. Nech $\mathbf{A}$ je ľubovoľná matica. Vieme, že existuje RTM $\mathbf{A}'$: $\mathbf{A} \approx \mathbf{A}'$. Nech by aj $\mathbf{B}'$ bola RTM, $\mathbf{B}' \approx \mathbf{A}$. Potom $\mathbf{A}' \approx \mathbf{A} \approx \mathbf{B}'$, teda $\mathbf{A}' \approx \mathbf{B}'$, teda $S_{A'} = S_{B'}$. Z predchádzajúcej vety vieme, že $\mathbf{A}' = \mathbf{B}'$. □

Veta 7.8. *Nech $\mathbf{A}, \mathbf{B} \in \mathfrak{M}_{k,s}(R)$ sú ľubovoľné. Potom platí: $\mathbf{A} \approx \mathbf{B} \Leftrightarrow S_A = S_B$.*

Dôkaz.

$\Rightarrow$: Veta 7.7

$\Leftarrow$: Predpokladajme, že $S_A = S_B$. Nech $\mathbf{A}'$ je RTM taká, že $\mathbf{A} \approx \mathbf{A}'$. Nech $\mathbf{B}'$ je RTM taká, že $\mathbf{B} \approx \mathbf{B}'$. Potom $S_{A'} = S_A = S_B = S_{B'}$. Teda $S_{A'} = S_{B'}$. Ale $\mathbf{A}', \mathbf{B}'$ sú RTM, teda z Vety 7.7: $\mathbf{A}' = \mathbf{B}'$. $\mathbf{A} \approx \mathbf{A}' = \mathbf{B}' \approx \mathbf{B}$, teda $\mathbf{A} \approx \mathbf{B}$. □

Tvrdenie 7.4. *Nech $\mathbf{A}, \mathbf{B} \in \mathfrak{M}_{k,s}(R)$. Potom $\mathbf{A} \approx \mathbf{B} \Leftrightarrow \mathbf{A}, \mathbf{B}$ sa dajú konečným počtom ERO upraviť na tú istú RTM.*

Dôkaz.

$\Rightarrow$: Predpokladajme, že $\mathbf{A} \approx \mathbf{B}$. Nech $\mathbf{A}'$ je RTM, $\mathbf{B}'$ je RTM, $\mathbf{A} \approx \mathbf{A}'$ a $\mathbf{B} \approx \mathbf{B}'$. Potom $S_{A'} = S_A = S_B = S_{B'}$. Keďže $\mathbf{A}', \mathbf{B}'$ sú RTM, máme že $\mathbf{A}' = \mathbf{B}'$.

$\Leftarrow$: Predpokladajme, že $\mathbf{A}, \mathbf{B}$: $\mathbf{A} \approx \mathbf{A}'$, $\mathbf{B} \approx \mathbf{A}'$ kde $\mathbf{A}'$ je RTM. Z toho: $\mathbf{A} \approx \mathbf{A}' \approx \mathbf{B} \Leftrightarrow \mathbf{A} \approx \mathbf{B}$. □

Príklad. Rozhodnite, či reálne matice $\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$ a $\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ sú riadkovo ekvivalentné. $\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \approx \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \approx \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. $\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \approx \begin{pmatrix} 1 & -1 \\ 0 & -2 \end{pmatrix} \approx \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \approx \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Sú riadkovo ekvivalentné.

VIII. LINEÁRNE ZOBRAZENIE

Definícia 8.1.

Nech V, W sú vektorové priestory nad poľom $\mathbb{R}$. Potom *lineárne zobrazenie* z V do W je zobrazenie $f : V \rightarrow W$ také, že $f(\alpha\vec{x} + \beta\vec{y}) = \alpha f(\vec{x}) + \beta f(\vec{y})$ pre $\forall \alpha, \beta \in \mathbb{R}$ a $\forall \vec{x}, \vec{y} \in V$.

Tvrdenie 8.1. Ak $f : V \rightarrow W$ je lineárne zobrazenie, tak $f(\vec{0}) = \vec{0}$.

Dôkaz. $f(\vec{0}) = f(\vec{0} + \vec{0}) = f(\vec{0}) + f(\vec{0})$ z toho: $f(\vec{0}) = \vec{0}$. □

Príklady.

1. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$, $f(a, b) = (2a + b, a + b - 1, a + 2b)$ nie je lineárne zobrazenie, lebo $f(\vec{0}) = f(0, 0) = (0, -1, 0) \neq \vec{0}$.
2. $p_1 : \mathbb{R}^3 \rightarrow \mathbb{R}$, $f(x_1, x_2, x_3) = x_1$ je lineárne zobrazenie. (Nazýva sa projekcia na prvú zložku). $p_1(\alpha(x_1, x_2, x_3) + \beta(y_1, y_2, y_3)) = p_1(\alpha x_1 + \beta y_1, \alpha x_2 + \beta y_2, \alpha x_3 + \beta y_3) = \alpha x_1 + \beta y_1 = \alpha p_1(x_1, x_2, x_3) + \beta p_1(y_1, y_2, y_3)$.
3. $\mathcal{O} : V \rightarrow W$, $\mathcal{O}(\vec{v}) = \vec{0} \in W$ pre všetky $\vec{v} \in V$ je lineárne zobrazenie.
4. $id_V : V \rightarrow V$, $id_V(\vec{x}) = \vec{x}$ je lineárne zobrazenie.
5. $g : \mathbb{R}^2 \rightarrow \mathbb{R}^2$, $g(x, y) = (2x, 3x - y)$ je lineárne zobrazenie.

Veta 8.1. Nech $f : V \rightarrow W$ je lineárne zobrazenie.

1. Ak $S \subset V$ je vektorový podpriestor, tak $f(S) \subset W$ je vektorový podpriestor vo W . (Špeciálne: $Im(f) = f(V)$ je vektorový podpriestor vo W .)
2. Ak $P \subset W$ je vektorový podpriestor vo W , tak jeho vzor pri zobrazení f je vektorový podpriestor. t.j.: $f^{-1}(P) = \{\vec{a} \in V, f(\vec{a}) \in P\} \subset V$. (Špec. $f^{-1}(\{\vec{0}\}) = \{\vec{x} \in V, f(\vec{x}) = \vec{0}\} = Ker(f)$, t.j. jadro lineárneho zobrazenia je vektorový podpriestor vo V .)

Dôkaz.

1. $f(\vec{0}) = \vec{0} \in f(S) \Rightarrow f(S) \neq \emptyset$. Kritérium vektorového podpriestoru: Nech $\vec{a}, \vec{b} \in f(S)$, $\alpha, \beta \in \mathbb{R}$ chceme ukázať, že $\alpha\vec{a} + \beta\vec{b} \in f(S)$. Máme $\vec{a} = f(\vec{x}), \vec{b} = f(\vec{y})$ pre dáke $\vec{x}, \vec{y} \in S$. Potom $f(\underbrace{\alpha\vec{a} + \beta\vec{b}}_{\in S}) = \alpha f(\vec{x}) + \beta f(\vec{y}) = \alpha\vec{a} + \beta\vec{b}$. A teda $\alpha\vec{a} + \beta\vec{b} \in f(S)$. Ukázali sme, že

$f(S)$ je vektorový podpriestor.

2. $\vec{0} \in P$, pričom $f(\vec{0}) = \vec{0} \in P \Rightarrow \vec{0} \in f^{-1}(P)$, preto $f^{-1}(P) \neq \emptyset$. Použijeme kritérium vektorového podpriestoru: Nech $\vec{x}, \vec{y} \in f^{-1}(P)$, $\alpha, \beta \in \mathbb{R}$. Chceme ukázať, že $\alpha\vec{x} + \beta\vec{y} \in f^{-1}(P)$. Rátajme: $f(\alpha\vec{x} + \beta\vec{y}) = \underbrace{\alpha f(\vec{x})}_{\in P} + \underbrace{\beta f(\vec{y})}_{\in P}$, preto $\alpha\vec{x} + \beta\vec{y} \in f^{-1}(P)$. □

Veta 8.2. Lineárne zobrazenie $f : V \rightarrow W$ je injektívne $\Leftrightarrow Ker(f) = \{\vec{0}\}$. f je surjektívne $\Leftrightarrow Im(f) = W$.

Dôkaz. Podobne ako pre grupy. □

Definícia 8.2. Lineárne zobrazenie $f : V \rightarrow W$ sa nazýva *lineárny izomorfizmus* ak f je bijektívne. Ak pre dané vektorové priestory V, W existuje lineárny izomorfizmus $g : V \rightarrow W$, tak hovoríme, že vektorový priestor V je lineárne izomorfný s vektorovým priestorom W . Píšeme: $V \cong W$

Veta 8.3. Ak $f : V \rightarrow W$ je lineárny izomorfizmus, tak aj $f^{-1} : W \rightarrow V$ je lineárny izomorfizmus.

Dôkaz. Vieme, že $f^{-1} : W \rightarrow V$ existuje a je bijekcia. Chceme ukázať, že je aj lineárne. Nech $\vec{a}, \vec{b} \in W$, $\alpha, \beta \in \mathbb{R}$. Nech $\vec{x} \in V$ je ten jediný, pre ktorý $f(\vec{x}) = \vec{a}$, podobne

$\vec{y} \in V$ jediný, pre ktorý $f(\vec{y}) = \vec{b}$. Potom: $f(\alpha\vec{x} + \beta\vec{y}) = \alpha f(\vec{x}) + \beta f(\vec{y}) = \alpha\vec{a} + \beta\vec{b}$. Z toho: $f^{-1}(\alpha\vec{a} + \beta\vec{b}) = \alpha f^{-1}(\vec{a}) + \beta f^{-1}(\vec{b})$.

□

Poznámka. Teda ak $V \cong W$, tak aj $W \cong V$.

Veta 8.4. Ak $f : V \rightarrow W$, $g : W \rightarrow S$ sú lineárne zobrazenia, tak aj $g \circ f : V \rightarrow S$ je lineárne zobrazenie. Špeciálne zloženie dvoch lineárnych izomorfizmov je lineárny izomorfizmus.

Dôkaz. $g \circ f(\alpha\vec{x} + \beta\vec{y}) = g(\alpha f(\vec{x}) + \beta f(\vec{y})) = \alpha \cdot g \circ f(\vec{x}) + \beta \cdot g \circ f(\vec{y})$.

□

Príklad. V = vektorový priestor orientovaných úsečiek v O_{xy} so začiatkom v O . $f : V \rightarrow \mathbb{R}^2$. $f(\text{orient. úsečky}) = (1.\text{súr. konc.bodu}, 2.\text{súr.konc. bodu})$. $f : V \rightarrow \mathbb{R}^2$ je lineárny izomorfizmus.

Nech S je vektorový podpriestor priestoru $V(\mathbb{R})$. Už vieme, že V/S je komutatívna grupa, s operáciou $+$: $[\vec{x}] + [\vec{y}] = [\vec{x} + \vec{y}]$. Definujme zobrazenie $\mathbb{R} \times V/S \rightarrow V/S$, $(\alpha, [\vec{x}]) \mapsto \alpha[\vec{x}]$, kde $\alpha[\vec{x}] = [\alpha\vec{x}]$. Je to dobrá definícia, lebo ak $[\vec{x}] = [\vec{y}]$, tak vieme, že $\vec{x} - \vec{y} \in S$. Potom, keďže S je vektorový podpriestor, máme pre $\forall \alpha \in \mathbb{R}$: $\alpha(\vec{x} - \vec{y}) = \alpha\vec{x} - \alpha\vec{y} \in S$. Teda $[\alpha\vec{x}] = [\alpha\vec{y}]$. Potom V/S je vektorový podpriestor nad $\mathbb{R}$. (napr. overme $\alpha([\vec{x}] + [\vec{y}]) = \alpha[\vec{x} + \vec{y}] = [\alpha(\vec{x} + \vec{y})] = [\alpha\vec{x} + \alpha\vec{y}] = [\alpha\vec{x}] + [\alpha\vec{y}] = \alpha[\vec{x}] + \alpha[\vec{y}]$, podobne sa overia ostatné axiomy vektorový podpriestoru.)

Príklady.

1. $V/V = \{\vec{0}\}$
2. Nech $f : V \rightarrow W$ je lineárne zobrazenie. Vieme, že $\text{Ker}(f)$ je vektorový podpriestor vo V , máme priestor $V/\text{Ker}(f)$.

Definícia 8.3. Ak V je vektorový priestor nad R a $S \subset V$ je vektorový podpriestor, tak V/S sa nazýva *faktorový vektorový priestor*.

Veta 8.5. Nech V je konečne generovaný vektorový priestor nad R a nech $S \subset V$ je vektorový podpriestor. Potom $\dim(V/S) = \dim(V) - \dim(S)$.

Dôkaz.

Nech $(\vec{a}_1, \dots, \vec{a}_r)$ je báza v S . Doplňme ju na bázu $(\vec{a}_1, \dots, \vec{a}_r, \vec{b}_{r+1}, \dots, \vec{b}_n)$ priestoru V . Potom vektorový priestor V/S je generovaný vektormi $[\vec{b}_{r+1}], \dots, [\vec{b}_n]$. Pre ľubovoľný $[\vec{x}] \in V/S$. Máme $\vec{x} \in V$, teda $\vec{x} = \alpha_1\vec{a}_1 + \dots + \alpha_r\vec{a}_r + \beta_{r+1}\vec{b}_{r+1} + \dots + \beta_n\vec{b}_n$ pre $\alpha_i, \beta_i \in R$. Z toho: $[\vec{x}] = [\alpha_1\vec{a}_1] + \dots + [\alpha_r\vec{a}_r] + [\beta_{r+1}\vec{b}_{r+1}] + \dots + [\beta_n\vec{b}_n] = \alpha_1[\vec{a}_1] + \dots + \alpha_r[\vec{a}_r] + \beta_{r+1}[\vec{b}_{r+1}] + \dots + \beta_n[\vec{b}_n]$, teda $\vec{0} \in V/S$, $[\vec{x}] = \beta_{r+1}[\vec{b}_{r+1}] + \dots + \beta_n[\vec{b}_n]$. Teda $V/S \subset [\vec{b}_{r+1}], \dots, [\vec{b}_n]$, obrátená inklúzia je zrejma. Navyše $[\vec{b}_{r+1}], \dots, [\vec{b}_n] \in V/S$ sú lineárne nezávislé, lebo nech $\delta_{r+1}[\vec{b}_{r+1}] + \dots + \delta_n[\vec{b}_n] = \vec{0} \in V/S$. Potom $[\delta_{r+1}\vec{b}_{r+1} + \dots + \delta_n\vec{b}_n] = [\vec{0}]$, teda $\delta_{r+1}\vec{b}_{r+1} + \dots + \delta_n\vec{b}_n \in S$. Potom $\delta_{r+1}\vec{b}_{r+1} + \dots + \delta_n\vec{b}_n = \gamma_1\vec{a}_1 + \dots + \gamma_r\vec{a}_r$, z toho: $\delta_{r+1}\vec{b}_{r+1} + \dots + \delta_n\vec{b}_n - \gamma_1\vec{a}_1 - \dots - \gamma_r\vec{a}_r = \vec{0} \in V$. Ale $\vec{a}_1, \dots, \vec{a}_r, \vec{b}_{r+1}, \dots, \vec{b}_n$ sú nezávislé, preto $\delta_{r+1} = \dots = \delta_n = 0$. Ukázali sme, že $([\vec{b}_{r+1}], \dots, [\vec{b}_n])$ je báza vo V/S , teda $\dim(V/S) = n - r$.

□

Veta o faktorovom izomorfizme. Nech $f : V \rightarrow W$ je surjektívne lineárne zobrazenie. Potom $V/\text{Ker}(f) \cong W$.

Dôkaz. Definujme $\varphi : V/\text{Ker}(f) \rightarrow W$, $\varphi([\vec{x}]) = f(\vec{x})$. Z vety o faktorovom izomorfizme pre grupy vieme, že φ je dobre definovaný homomorfizmus abelovských grúp; tiež φ je bijekcia. Aby sme ukázali, že φ je aj lineárny izomorfizmus, stačí ukázať, že $\varphi(\alpha[\vec{x}])$ pre $\alpha \in R$, $[\vec{x}] \in V/\text{Ker}(f)$. Takto: $\varphi(\alpha[\vec{x}]) = \varphi([\alpha\vec{x}]) = f(\alpha\vec{x}) = \alpha f(\vec{x}) = \alpha\varphi([\vec{x}])$. Zistili sme, že φ je lineárny izomorfizmus medzi $V/\text{Ker}(f) \cong W$.

□

Príklad. $p_1 : \mathbb{R}^3 \rightarrow \mathbb{R}$, $p_1(x_1, x_2, x_3) = x_1$ je lineárne zobrazenie, je aj surjektívne. $\text{Ker}(p_1) = \{(x_1, x_2, x_3) \in \mathbb{R}^3, x_1 = 0\} = \{(0, x_2, x_3), x_2, x_3 \in \mathbb{R}\}$. Z vety: $\mathbb{R}^3 / \{(0, x_2, x_3) \in \mathbb{R}^3, x_2, x_3 \in \mathbb{R}\} \cong \mathbb{R}$

Veta 8.6. (základná veta o lineárnych zobrazeniach) *Nech V je konečne generovaný vektorový priestor nad poľom R a nech W je vektorový priestor nad R . Potom existuje jediné lineárne zobrazenie $f : V \rightarrow W$ také, že f zobrazí bázoové vektory $\vec{a}_1, \dots, \vec{a}_n$ priestoru V na predpísané obrazy $\vec{b}_1, \dots, \vec{b}_n \in W$, teda také, že $f(\vec{a}_1) = \vec{b}_1, \dots, f(\vec{a}_n) = \vec{b}_n$. Zobrazenie f funguje takto: ak $\vec{x} = \alpha_1 \vec{a}_1 + \dots + \alpha_n \vec{a}_n$, tak $f(\vec{x}) = \alpha_1 \vec{b}_1 + \dots + \alpha_n \vec{b}_n$.*

Dôkaz.

Jednoznačnosť: Ak také f existuje, tak jediné: nech by $f, g : V \rightarrow W$ boli dve také lineárne zobrazenia. Teda $f(\vec{a}_1) = \vec{b}_1, \dots, f(\vec{a}_n) = \vec{b}_n, g(\vec{a}_1) = \vec{b}_1, \dots, g(\vec{a}_n) = \vec{b}_n$. Ľubovoľný $x \in V$ má jednoznačné vyjadrenie: $\vec{x} = \alpha_1 \vec{a}_1 + \dots + \alpha_n \vec{a}_n$. Z lineárnosti f a g : $f(\vec{x}) = f(\alpha_1 \vec{a}_1 + \dots + \alpha_n \vec{a}_n) = \alpha_1 \vec{b}_1 + \dots + \alpha_n \vec{b}_n$ a $g(\vec{x}) = g(\alpha_1 \vec{a}_1 + \dots + \alpha_n \vec{a}_n) = \alpha_1 \vec{b}_1 + \dots + \alpha_n \vec{b}_n$. Teda $f = g$.

Existencia: Videli sme, že ak také f existuje, tak pre $\forall x \in V$, $\vec{x} = \alpha_1 \vec{a}_1 + \dots + \alpha_n \vec{a}_n$ musí byť $f(\vec{x}) = \alpha_1 \vec{b}_1 + \dots + \alpha_n \vec{b}_n$. Teda definujeme $f : V \rightarrow W$ takto: $f(\vec{x}) = \alpha_1 \vec{b}_1 + \dots + \alpha_n \vec{b}_n$, ak $\vec{x} = \alpha_1 \vec{a}_1 + \dots + \alpha_n \vec{a}_n$. Potom $f(\vec{a}_1) = \vec{b}_1, \dots, f(\vec{a}_n) = \vec{b}_n$; treba už len overiť lineárnosť $f : \vec{x}, \vec{y} \in V, \alpha, \beta \in R, \vec{x} = \alpha_1 \vec{a}_1 + \dots + \alpha_n \vec{a}_n, \vec{y} = \beta_1 \vec{a}_1 + \dots + \beta_n \vec{a}_n \Rightarrow f(\alpha \vec{x} + \beta \vec{y}) = f(\alpha(\alpha_1 \vec{a}_1 + \dots + \alpha_n \vec{a}_n) + \beta(\beta_1 \vec{a}_1 + \dots + \beta_n \vec{a}_n)) = f((\alpha\alpha_1 + \beta\beta_1)\vec{a}_1 + \dots + (\alpha\alpha_n + \beta\beta_n)\vec{a}_n) = (\alpha\alpha_1 + \beta\beta_1)\vec{b}_1 + \dots + (\alpha\alpha_n + \beta\beta_n)\vec{b}_n = \alpha(\alpha_1 \vec{b}_1 + \dots + \alpha_n \vec{b}_n) + \beta(\beta_1 \vec{b}_1 + \dots + \beta_n \vec{b}_n) = \alpha f(\vec{x}) + \beta f(\vec{y})$.

□

Lineárne zobrazenia $R^k \rightarrow R^s$, kde R je pole.

Definícia 8.4. Nech $f : R^k \rightarrow R^s$ je lineárne zobrazenie. Zo základnej vety o lineárnych zobrazeniach vieme, že f je úplne určené obrazmi bázoových vektorov. Špeciálne: obrazmi štandardných bázoových vektorov $\vec{e}_1, \dots, \vec{e}_k \in R^k$. Ak tieto obrazy (t.j. $f(\vec{e}_1), \dots, f(\vec{e}_k) \in R^s$) zapíšeme (poradie zachováme) do matice, tak dostaneme maticu typu $k \times s$ nad poľom R . Ozn.: $\mathbf{M}_f$. Matica $\mathbf{M}_f$ sa nazýva matica lineárneho zobrazenia f . $f(1, 0, \dots, 0) = (a_{11}, \dots, a_{1s}) \in R^s, \dots, f(0, 0, \dots, 1) = (a_{k1}, \dots, a_{ks}) \Rightarrow \mathbf{M}_f = \begin{pmatrix} a_{11} & \dots & a_{1s} \\ \vdots & \ddots & \vdots \\ a_{k1} & \dots & a_{ks} \end{pmatrix} \in \mathfrak{M}_{k,s}(R)$.

Príklad. $g : \mathbb{R}^2 \rightarrow \mathbb{R}^2, g(x_1, x_2) = (2x_1 - x_2, x_1 + x_2)$, $\mathbf{M}_g = \begin{pmatrix} g(1,0) \\ g(0,1) \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}$.

Definícia 8.5. Nech je daná matica $\mathbf{A} \in \mathfrak{M}_{k,s}(R)$. Potom zo základnej vety o lineárnych zobrazeniach vieme, že existuje jediné zobrazenie $R^k \rightarrow R^s$, ktoré $\vec{e}_1 \in R^k$ zobrazí na prvý riadok matice $\mathbf{A}$, atď, $\vec{e}_k$ na k -tý riadok matice $\mathbf{A}$. Toto lineárne zobrazenie označíme $f_A : R^k \rightarrow R^s$; nazýva sa lineárne zobrazenie patriace k matici $\mathbf{A}$.

Príklad.

$\mathbf{B} = \begin{pmatrix} 1 & -1 & 2 \\ 1 & 1 & 3 \end{pmatrix} \in M_{2,3}(\mathbb{R}), g_B : \mathbb{R}^3 \rightarrow \mathbb{R}^2, g_B(1, 0) = (1, -1, 2), g_B(0, 1) = (1, 1, 3)$.

$g_B(x_1, x_2) = g_B((1, 0)x_1 + (0, 1)x_2) = x_1(1, -1, 2) + x_2(1, 1, 3) = (x_1 + x_2, -x_1 + x_2, 2x_1 + 3x_2)$. Je jasné: $\mathbf{M}_{g_B} = \mathbf{B}$

Veta 8.7. Priradenie matice lineárnemu zobrazeniu $R^k \rightarrow R^s$ definuje bijektívnu korešpondenciu medzi množinou všetkých lineárnych zobrazení $R^k \rightarrow R^s$ a množinou matíc $\mathfrak{M}_{k,s}(R)$.

Dôkaz. Jasné!

□

Nech $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$, $g: \mathbb{R}^2 \rightarrow \mathbb{R}^3$ sú lineárne zobrazenia. Potom $g \circ f: \mathbb{R}^2 \rightarrow \mathbb{R}^3$ je tiež lineárne zobrazenie. Nech $\mathbf{M}_f = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ a $\mathbf{M}_g = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{pmatrix}$. Aký je vzťah medzi $\mathbf{M}_{g \circ f}$ na jednej strane a maticami $\mathbf{M}_g, \mathbf{M}_f$ na druhej strane?

$$\begin{aligned} \text{Rátame: } f(1,0) &= (a_{11}, a_{12}), f(0,1) = (a_{21}, a_{22}), g(1,0) = (b_{11}, b_{12}, b_{13}), g(0,1) = (b_{21}, \\ &b_{22}, b_{23}), g \circ f(1,0) = g(a_{11}(1,0) + a_{12}(0,1)) = a_{11}(b_{11}, b_{12}, b_{13}) + a_{12}(b_{21}, b_{22}, b_{23}) = \\ &= (a_{11}b_{11} + a_{12}b_{21}, a_{11}b_{12} + a_{12}b_{22}, a_{11}b_{13} + a_{12}b_{23}), g \circ f(0,1) = g(a_{21}(0,1) + a_{22}(0,1)) = \\ &= \dots = (a_{21}b_{11} + a_{22}b_{21}, a_{21}b_{12} + a_{22}b_{22}, a_{21}b_{13} + a_{22}b_{23}), \mathbf{M}_{g \circ f} = \mathbf{M}_f \cdot \mathbf{M}_g. \end{aligned}$$

Tvrdenie 8.2. Ak $f: R^k \rightarrow R^s$ je lineárne zobrazenie s maticou $\mathbf{M}_f = (a_{ij}) \in \mathfrak{M}_{k,s}(R)$ a $g: R^s \rightarrow R^t$ je lineárne zobrazenie s maticou $\mathbf{M}_g = (b_{ij}) \in \mathfrak{M}_{s,t}(R)$, tak lineárne zobrazenie $g \circ f: R^k \rightarrow R^t$ má maticu $\mathbf{M}_{g \circ f} \in \mathfrak{M}_{k,t}(R)$, ktorej prvok i -teho riadku a j -teho stĺpca dostaneme ako skalárny súčin i -teho riadku z $\mathbf{M}_f$ a j -teho stĺpca z $\mathbf{M}_g$.

Definícia 8.6. Nech $\mathbf{A} \in \mathfrak{M}_{k,s}(R)$, $\mathbf{B} \in \mathfrak{M}_{s,t}(R)$; potom *súčin matic* $\mathbf{A}$ a $\mathbf{B}$ ozn. $\mathbf{AB}$ sa definuje takto: $\mathbf{AB} = \mathbf{C} = (c_{ij}) \in \mathfrak{M}_{k,t}(R)$, kde $c_{ij} = a_{i1}b_{1j} + \dots + a_{is}b_{sj}$.

Tvrdenie 8.3. Ak $f : R^k \rightarrow R^s$ je lineárne zobrazenie s maticou $\mathbf{M}_f$ a $g : R^s \rightarrow R^t$ je lineárne zobrazenie s maticou $\mathbf{M}_g$, tak $\mathbf{M}_{g \circ f} = \mathbf{M}_f \cdot \mathbf{M}_g$

Príklad.

$$\begin{pmatrix} 1 & -2 & 3 \\ 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \end{pmatrix}$$

Niektoré vlastnosti súčinu matic.

1. $\mathbf{A} \in \mathfrak{M}_{k,s}(R)$ $\mathbf{I}_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \in \mathfrak{M}_{n,n}(R) \Rightarrow \mathbf{I}_k \mathbf{A} = \mathbf{A} = \mathbf{A} \mathbf{I}_s$ kde $\mathbf{I}_s = \mathbf{M}_{id(R^s)}$.
2. $\mathbf{A} \in \mathfrak{M}_{k,s}$, $\mathbf{B} \in \mathfrak{M}_{s,t}$, $\mathbf{C} \in \mathfrak{M}_{t,z}$ potom $(\mathbf{AB})\mathbf{C} = \mathbf{A}(\mathbf{BC})$. Dôkaz: $\mathbf{A} = \mathbf{M}_{f_A}$, $\mathbf{B} = \mathbf{M}_{f_B}$, $\mathbf{C} = \mathbf{M}_{f_C}$. Potom $\mathbf{A}(\mathbf{BC}) = \mathbf{M}_{f_A}(\mathbf{M}_{f_B}\mathbf{M}_{f_C}) = \mathbf{M}_{f_A}(\mathbf{M}_{f_C \circ f_B}) = \mathbf{M}_{(f_C \circ f_B) \circ f_A} = \mathbf{M}_{f_C(f_B \circ f_A)} = \mathbf{M}_{f_B \circ f_A} \mathbf{M}_{f_C} = (\mathbf{M}_{f_A} \mathbf{M}_{f_B}) \mathbf{M}_{f_C}$.
3. distributivita: $\mathbf{A}(\mathbf{B} + \mathbf{C}) = \mathbf{AB} + \mathbf{AC}$, keď to má zmysel, $(\mathbf{A} + \mathbf{B})\mathbf{C} = \mathbf{AC} + \mathbf{BC}$.
4. $\mathbf{AB} \neq \mathbf{BA}$ napr.: $\begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 3 \\ -2 & 0 \end{pmatrix}$, ale $\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 3 \\ -2 & -1 \end{pmatrix}$.
($\mathfrak{M}_{n,n}(R)$, +, $\bullet$, $1 = \mathbf{I}_n$) je okruh s 1.

Definícia 8.7. *Elementárna matica stupňa k patriaca k danej ERO je matica, ktorú z $\mathbf{I}_k$ dostaneme tak, že na $\mathbf{I}_k$ urobíme túto ERO.*

Príklad. ERO- prirátanie α -násobku druhého riadku k prvému. Prislúšná elementárna matica stupňa 3 je: $\mathbf{E} = \begin{pmatrix} 1 & \alpha & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Veta 8.8. *Nech $\mathbf{B} \in \mathfrak{M}_{k,s}(R)$ vznikne z $\mathbf{A} \in \mathfrak{M}_{k,s}(R)$ vykonaním práve jednej ERO. Potom ak $\mathbf{E}$ je elementárna matica stupňa k patriaca k tejto ERO, tak $\mathbf{B} = \mathbf{E}\mathbf{A}$.*

Dôkaz. Ak $\mathbf{C} \in \mathfrak{M}_{a,b}(R)$ je ľubovoľná matica, tak i -tý riadok matice $\mathbf{C}$ sa rovná

$$(0, \dots, 0, 1, 0, \dots, 0) \mathbf{C} = \vec{e}_i \mathbf{C}, (0, \dots, 0, 1, 0, \dots, 0) \cdot \begin{pmatrix} c_{11} & \cdots & c_{1b} \\ \vdots & \ddots & \vdots \\ c_{i1} & \cdots & c_{ib} \\ \vdots & \ddots & \vdots \\ c_{n1} & \cdots & c_{nb} \end{pmatrix} = (c_{i1}, \dots, c_{ib}).$$

$\mathbf{A}=(a_{ij})_{k,s}$. Nech napr. ERO spočíva v tom, že α -násobok j -teho riadku prirátame

k prvému. Teda: $\mathbf{B} = \begin{pmatrix} a_{11} + \alpha a_{j1} & \cdots & a_{1s} + \alpha a_{js} \\ a_{21} & \cdots & a_{2s} \\ \vdots & \ddots & \vdots \\ a_{k1} & \cdots & a_{ks} \end{pmatrix}$. Elementárna matica $\mathbf{E}$ vznikne z $\mathbf{I}_k$

vykonaním tej istej ERO. Teda riadky matice $\mathbf{E}$ budú $\vec{e}_1 + \alpha \vec{e}_j, \vec{e}_2, \dots, \vec{e}_k$. Prvý riadok v $\mathbf{EA}$ je $\vec{e}_1(\mathbf{EA}) = (\vec{e}_1 \mathbf{E})\mathbf{A} = (\vec{e}_1 + \alpha \vec{e}_j)\mathbf{A} = \vec{e}_1 \mathbf{A} + \alpha \vec{e}_j \mathbf{A} = (a_{11}, \dots, a_{1s}) + \alpha(a_{j1}, \dots, a_{js}) = (a_{11} + \alpha a_{j1}, \dots, a_{1s} + \alpha a_{js})$ = prvý riadok v $\mathbf{B}$. Druhý riadok v $\mathbf{EA}$ je $\vec{e}_2(\mathbf{EA}) = (\vec{e}_2 \mathbf{E})\mathbf{A} = \vec{e}_2 \mathbf{A} = (a_{21}, \dots, a_{2s})$ = druhý riadok v $\mathbf{B}$ podobne všetky ostatné. Teda $\mathbf{B} = \mathbf{EA}$.

□

Príklad. $\mathbf{A} = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \in \mathfrak{M}_{2,2}(\mathbb{R})$. K druhému riadku prirátame prvý.

$$\mathbf{B} = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \quad \mathbf{E} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \mathbf{EA} = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} = \mathbf{B}.$$

Tvrdenie 8.4. *Nech $\mathbf{A} \in \mathfrak{M}_{k,s}(R)$, nech $f_A : R^k \rightarrow R^s$ je lineárne zobrazenie matricou $\mathbf{A}$. Potom $f_{\mathbf{A}}(x_1, \dots, x_k) = (x_1, \dots, x_k) \cdot \mathbf{A}$ pre všetky $(x_1, \dots, x_k) \in R^k$. Pre lineárne zobrazenie $g : R^k \rightarrow R^s$ máme: $g(x_1, \dots, x_k) = (x_1, \dots, x_k) \cdot \mathbf{M}_g$ pre všetky $(x_1, \dots, x_k) \in R^k$.*

Dôkaz. Zo základnej vety o lineárnych zobrazeniach vieme, že g je úplne určené obrazmi: $\vec{e}_1, \dots, \vec{e}_k$. Predpis $h(x_1, \dots, x_k) = (x_1, \dots, x_k) \cdot \mathbf{M}_g$ definuje lineárne zobrazenie z $R^k \rightarrow R^s$. $h(\alpha(x_1, \dots, x_k) + \beta(y_1, \dots, y_k)) \cdot \mathbf{M}_g = \alpha(x_1, \dots, x_k) \cdot \mathbf{M}_g + \beta(y_1, \dots, y_k) \cdot \mathbf{M}_g = \alpha h(x_1, \dots, x_k) + \beta h(y_1, \dots, y_k)$. $g(\vec{e}_1) = 1$. riadok matice $\mathbf{M}_g$. $h(\vec{e}_1) = \vec{e}_1 \cdot \mathbf{M}_g = 1$. riadok v $\mathbf{M}_g$.

Všeobecne: $g(\vec{e}_i) = i$ -tý riadok v $\mathbf{M}_g$. $h(\vec{e}_i) = \vec{e}_i \mathbf{M}_g$ pre $i = 1, \dots, k$. Z toho: $h = g$, a teda $g(x_1, \dots, x_k) = (x_1, \dots, x_k) \cdot \mathbf{M}_g$.

□

Príklad. $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$, $f(x_1, x_2) = (-x_1 + x_2, -x_1)$, $\mathbf{M}_f = \begin{pmatrix} f(1,0) \\ f(0,1) \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$,

$$(x_1, x_2) \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} = (-x_1 + x_2, -x_1).$$

Poznámka. Prvky z R^k chápme ako riadky. Ale niekedy sa prvky z R^k chápu aj ako stĺpce. Potom pri takom chápaní sa matica lineárneho zobrazenia $f : R^k \rightarrow R^s$

definuje ako matica $\widetilde{\mathbf{M}}_f$ je typu $s \times k$ nad R , ktorej i -tý stĺpec je $f \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$.

$$g : R^k \rightarrow R^s, \quad g \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = g(x_1, \dots, x_k) = \widetilde{\mathbf{M}}_f \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix}.$$

Definícia 8.8. $\mathbf{A} = (a_{ij}) \in \mathfrak{M}_{k,s}(R)$ k nej *transponovaná* matica je matica $\mathbf{A}^T \in \mathfrak{M}_{s,k}(R)$ pričom $(a_{ij}^T) = a_{ji}$. Teda $\mathbf{A}^T$ dostaneme z $\mathbf{A}$ tak, že "vymeníme riadky za stĺpce".

$$\text{Príklad. } \mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \end{pmatrix} \quad \mathbf{A}^T = \begin{pmatrix} 1 & 2 \\ 2 & 4 \\ 3 & 5 \end{pmatrix}.$$

Tvrdenie 8.5. *Ak $\mathbf{A} = (a_{ij}) \in \mathfrak{M}_{k,s}$, $\mathbf{B} = (b_{ij}) \in \mathfrak{M}_{s,t}(R)$, tak $(\mathbf{AB})^T = \mathbf{B}^T \mathbf{A}^T$.*

Dôkaz. Prvok i -teho riadku a j -teho stĺpca v $\mathbf{B}^T \mathbf{A}^T$ je $\sum_{p=1}^s b_{ip}^T a_{pj}^T = \sum_{p=1}^s a_{jp} b_{pi}$.

Prvok z i -teho riadku a j -teho stĺpca v $(\mathbf{AB})^T$ = prvok j -teho riadku a i -teho stĺpca v $\mathbf{AB}$, teda $\sum_{p=1}^s a_{jp} b_{pi}$.

□

Poznámka. $(\mathbf{A}^T)^T = \mathbf{A}$.

Injektívnosť a surjektívnosť lineárnych zobrazení.

$f : V \rightarrow W$ vieme, že f je injektívne $\Leftrightarrow \text{Ker}(f) = \{\vec{0}\}$, f je surjektívne $\Leftrightarrow \text{Im}(f) = f(V) = W$.

Veta 8.9. *Nech $f : V \rightarrow W$ je lineárne zobrazenie a nech $(\vec{a}_1, \dots, \vec{a}_k)$ je báza vo V . Potom:*

1. f je injektívne $\Leftrightarrow f(\vec{a}_1, \dots, f(\vec{a}_n))$ sú lineárne nezávislé.
2. f je surjektívne $\Leftrightarrow [f(\vec{a}_1), \dots, f(\vec{a}_n)] = W$.

Dôkaz.

1. $\Rightarrow f$: je injektívne. Nech $\alpha_1 f(\vec{a}_1) + \dots + \alpha_n f(\vec{a}_n) = \vec{0}$. Chceme ukázať, že $\alpha_i = 0$. Z toho: $f(\alpha_1 \vec{a}_1 + \dots + \alpha_n \vec{a}_n) = f(\vec{0})$. Podľa predpokladu: $\alpha_1 \vec{a}_1 + \dots + \alpha_n \vec{a}_n = \vec{0}$, z lineárnej nezávislosti $\vec{a}_1, \dots, \vec{a}_n \Rightarrow \forall \alpha_i = 0$.
 $\Leftarrow$: Nech $\forall f(\vec{a}_i)$ sú lineárne nezávislé. Nech $\vec{x} \in \text{Ker}(f)$. Teda $f(\vec{x}) = \vec{0}$. Máme jednoznačne $\vec{x} = \beta_1 \vec{a}_1 + \dots + \beta_n \vec{a}_n$. Potom $f(\vec{x}) = \beta_1 f(\vec{a}_1) + \dots + \beta_n f(\vec{a}_n)$, keďže: $f(\vec{x}) = \vec{0} : f(\vec{a}_1), \dots, f(\vec{a}_n)$ sú lineárne nezávislé máme, že $\beta_1 = \dots = \beta_n = 0$ a teda $\vec{x} = \vec{0}$. Preto $\text{Ker}(f) = \{\vec{0}\}$, teda f je injektívne.
2. $\Rightarrow$: Predpokladajme, že f je surjektívne. Nech $\vec{y} \in W$ je ľubovoľný. Zo surjektívnosti: existuje $\vec{x} \in V : f(\vec{x}) = \vec{y}$. Máme, $\vec{x} = \alpha_1 \vec{a}_1 + \dots + \alpha_n \vec{a}_n$, teda $f(\alpha_1 \vec{a}_1 + \dots + \alpha_n \vec{a}_n) = \vec{y} \Rightarrow \alpha_1 f(\vec{a}_1) + \dots + \alpha_n f(\vec{a}_n)$. Takže $\vec{y} \in [f(\vec{a}_1), \dots, f(\vec{a}_n)]$ máme $W \subset [f(\vec{a}_1), \dots, f(\vec{a}_n)]$. Obrátená inklúzia je zrejmalá.
 $\Leftarrow$: Predpokladajme, že $W = [f(\vec{a}_1), \dots, f(\vec{a}_n)]$. Nech $\vec{b} \in W$ je ľubovoľný, potom $\vec{b} = \beta_1 f(\vec{a}_1) + \dots + \beta_n f(\vec{a}_n) = f(\underbrace{\beta_1 \vec{a}_1 + \dots + \beta_n \vec{a}_n}_{\in V})$. $\vec{b}$ má vzor f je surjektívne.

□

Dôsledok. Ak V a W sú konečne generované vektorové priestory nad R , tak lineárne zobrazenie $f : V \rightarrow W$ je lineárny izomorfizmus $\Leftrightarrow f$ zobrazuje bázu priestoru V na bázu priestoru W .

Poznámka. Ak $V \cong W$, tak $\dim(V) = \dim(W)$.

Dôsledok.

Každý n -rozmerný ($n \geq 1$) vektorový priestor nad $\mathbb{R}$ je lineárne izomorfný s $\mathbb{R}^n$.

Dôkaz. Nech $V \neq \{\vec{0}\}$ má nejakú bázu $(\vec{a}_1, \dots, \vec{a}_n)$. V $\mathbb{R}^n$ zoberme štandardnú bázu $(\vec{e}_1, \dots, \vec{e}_n)$. Zo základnej vety o lineárnych zobrazeniach vieme, že existuje práve jedno lineárne zobrazenie $f : V \rightarrow \mathbb{R}^n$ také, že $f(\vec{a}_i) = \vec{e}_i$, $i = 1, 2, \dots, n$. Podľa predchádzajúceho dôsledku f je lineárny izomorfizmus, teda $V \cong \mathbb{R}^n$.

□

Veta 8.10. Nech $f : R^k \rightarrow R^s$ je lineárne zobrazenie. Potom:

1. f je injektívne $\Leftrightarrow h(\mathbf{M}_f) = k$.
2. f je surjektívne $\Leftrightarrow h(\mathbf{M}_f) = s$.
3. f je lineárny izomorfizmus $\Leftrightarrow k = s$ a $h(\mathbf{M}_f) = k$.

Dôkaz. $\mathbf{M}_f \in \mathfrak{M}_{k,s}(R)$ má riadky $f(\vec{e}_1), \dots, f(\vec{e}_k)$. To znamená, že $f : R^k \rightarrow \text{Im}(f)$ je surjekcia, teda z vety 8.9 vyplýva, že priestor $\text{Im}(f)$ je generovaný $\text{Im}(f) = [f(\vec{e}_1), \dots, f(\vec{e}_k)]$. Teda $\dim(\text{Im}(f)) = \dim[f(\vec{e}_1), \dots, f(\vec{e}_k)] = h(\mathbf{M}_f)$. Z vety o faktorovom izomorfizme: $R^k / \text{Ker}(f) \cong \text{Im}(f)$. Teda $k - \dim(\text{Ker}(f)) = \dim(\text{Im}(f)) = h(\mathbf{M}_f)$.

1. f je injektívne $\Leftrightarrow \text{Ker}(f) = \{\vec{0}\} \Leftrightarrow \dim\{\text{Ker}(f)\} = 0 \Leftrightarrow h(\mathbf{M}_f) = k$.
2. f je surjektívne $\Leftrightarrow \text{Im}(f) = R^s \Leftrightarrow [f(\vec{e}_1), \dots, f(\vec{e}_n)] = R^s \Leftrightarrow \dim[f(\vec{e}_1), \dots, f(\vec{e}_k)] = s = h(\mathbf{M}_f)$.

□

Lema 8.1.

Nech S je vektorový podpriestor priestoru V . Potom $S = V \Leftrightarrow \dim(S) = \dim(V)$.

Dôkaz. $\Rightarrow$: Ak $S = V$, tak $\dim(S) = \dim(V)$

$\Leftarrow$: Predpokladajme, že $\dim(S) = \dim(V)$. Nech teraz $S \neq V$. Nech $(\vec{a}_1, \dots, \vec{a}_p)$ je báza v S . Existuje $\vec{x} \in V - S$. Potom vektory $\vec{a}_1, \dots, \vec{a}_p, \vec{x}$ sú lineárne nezávislé, a teda $\dim(V)$ je aspoň $p+1$, kým $\dim(S) = p$; spor s tým, že $\dim(S) = \dim(V)$.

□

Definícia 8.9. Lineárne zobrazenie $f : R^k \rightarrow R^k$ sa volá *transformácia* priestoru R^k . Lineárna transformácia $f : R^k \rightarrow R^k$ sa nazýva *regulárna*, ak f je lineárny izomorfizmus.

Veta 8.11. Lineárna transformácia $f : R^k \rightarrow R^k$ je regulárna $\Leftrightarrow h(\mathbf{M}_f) = k$.

Dôkaz. Vyplýva to z vety 8.10 □

Definícia 8.10. Matica $\mathbf{A} \in \mathfrak{M}_{k,k}(R)$ sa nazýva *regulárna*, ak $h(\mathbf{A}) = k$.

Potom Veta 8.11 znie takto: Lineárna transformácia $f : R^k \rightarrow R^k$ je regulárna $\Leftrightarrow$ jej matica $\mathbf{M}_f$ je regulárna.

Definícia 8.11. Inverzná matica k danej matici $\mathbf{A} \in \mathfrak{M}_{k,k}(R)$ je taká matica $\mathbf{B} \in \mathfrak{M}_{k,k}(R)$, že platí $\mathbf{AB} = \mathbf{BA} = \mathbf{I}_k$. Pretože binárna operácia $\bullet$ na $\mathfrak{M}_{k,k}(R)$ je asociatívna a $\mathbf{I}_k$ je neutrálny prvok vieme, že ak taká matica $\mathbf{B}$ existuje, tak je jediný. Označíme ju $\mathbf{A}^{-1}$.

Pre aké matice $\mathbf{A} \in \mathfrak{M}_{k,k}(R)$ existuje $\mathbf{A}^{-1}$?

Nutná podmienka: ak $\mathbf{A}^{-1}$ existuje, tak $\mathbf{AA}^{-1} = \mathbf{A}^{-1}\mathbf{A} = \mathbf{I}_k$. Z toho potom vieme, že $f_{\mathbf{AA}^{-1}} : R^k \rightarrow R^k$, $f_{\mathbf{AA}^{-1}}(x_1, \dots, x_k) = (x_1, \dots, x_k)\mathbf{AA}^{-1} = ((x_1, \dots, x_k)\mathbf{A})\mathbf{A}^{-1} = f_{\mathbf{A}^{-1}}((x_1, \dots, x_k)\mathbf{A}) = f_{\mathbf{A}^{-1}}f_{\mathbf{A}}(x_1, \dots, x_k) = f_{\mathbf{A}^{-1} \circ f_{\mathbf{A}}}(x_1, \dots, x_k) \Rightarrow f_{\mathbf{AA}^{-1}} = f_{\mathbf{A}^{-1} \circ f_{\mathbf{A}}} = f_{\mathbf{A}^{-1}\mathbf{A}} = f_{\mathbf{I}_k} = id_{R^k} = f_{\mathbf{A}^{-1}\mathbf{A}}$. Podobne $f_{\mathbf{A}^{-1}\mathbf{A}} = f_{\mathbf{A} \circ f_{\mathbf{A}^{-1}}}$, teda $f_{\mathbf{A} \circ f_{\mathbf{A}^{-1}}} = f_{\mathbf{A}^{-1}\mathbf{A}} = f_{\mathbf{I}_k} = id_{R^k} = f_{\mathbf{A}^{-1} \circ f_{\mathbf{A}}}$. To znamená, že $(f_{\mathbf{A}})^{-1} = f_{\mathbf{A}^{-1}}$.

Veta 8.12. K matici $\mathbf{A} \in \mathfrak{M}_{k,k}(R)$ existuje inverzná $\Leftrightarrow \mathbf{A}$ je regulárna.

Dôkaz.

$\Rightarrow$ už máme.

$\Leftarrow$ Predpokladajme, že $\mathbf{A}$ je regulárna. Teda $f_{\mathbf{A}} : R^k \rightarrow R^k$ je regulárna lineárna transformácia, t.j. $f_{\mathbf{A}}$ je lineárny izomorfizmus. Potom existuje k nemu inverzný lineárny izomorfizmus $g : R^k \rightarrow R^k$. Teda $g \circ f_{\mathbf{A}} = f_{\mathbf{A}} \circ g = id_{R^k}$. Pritom $g = f_{\mathbf{M}_g}$. To znamená, že $f_{\mathbf{M}_g} \circ f_{\mathbf{A}} = f_{\mathbf{A}} \circ f_{\mathbf{M}_g} = id_{R^k}$. To je to isté ako: $f_{\mathbf{AM}_g} = f_{\mathbf{M}_g\mathbf{A}} = f_{\mathbf{I}_k}$. Z korešpondencie: $\mathbf{AM}_g = \mathbf{M}_g\mathbf{A} = \mathbf{I}_k$, teda $\mathbf{M}_g = \mathbf{A}^{-1}$. Zároveň máme: $\mathbf{A}^{-1} = \mathbf{M}_{(f_{\mathbf{A}})^{-1}}$. □

Definícia 8.12. Ak matica nie je regulárna, tak je *singulárna*.

$\mathbf{A} \in \mathfrak{M}_{k,k}(R)$, $\mathbf{A}$ je singulárna $\Leftrightarrow h(\mathbf{A}) < k$.

Nech $\mathbf{A} \in \mathfrak{M}_{k,k}(\mathbb{R})$ je regulárna matica. Ako vypočítať $\mathbf{A}^{-1}$? $\mathbf{A} = \begin{pmatrix} a_{11} & \dots & a_{1k} \\ \vdots & \ddots & \vdots \\ a_{k1} & \dots & a_{kk} \end{pmatrix}$.
 $f_{\mathbf{A}}(1, 0, \dots, 0) = (a_{11}, \dots, a_{1k}), \dots, f_{\mathbf{A}}(0, 0, \dots, 1) = (a_{k1}, \dots, a_{kk})$. Treba nájsť inverzné zobrazenie $f_{\mathbf{A}}^{-1}$. Pretože $f_{\mathbf{A}} : \mathbb{R}^k \rightarrow \mathbb{R}^k$ je lineárny izomorfizmus $((a_{11}, \dots, a_{1k}), \dots, (a_{k1}, \dots, a_{kk}))$ je tiež báza v $\mathbb{R}^k$. Preto zobrazenie $(f_{\mathbf{A}}^{-1}) : \mathbb{R}^k \rightarrow \mathbb{R}^k$ je úplne určené tým, že $(f_{\mathbf{A}}^{-1})(a_{11}, \dots, a_{1k}) = (1, 0, \dots, 0)$ až $(f_{\mathbf{A}}^{-1})(a_{k1}, \dots, a_{kk}) = (0, \dots, 0, 1)$. Aby sme dostali maticu zobrazenia $f_{\mathbf{A}}^{-1}$, potrebujeme vyrátať, na čo $f_{\mathbf{A}}^{-1}$ zobrazí $\vec{e}_1, \dots, \vec{e}_k$.
 $\begin{pmatrix} a_{11} & \dots & a_{1k} & 1 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{k1} & \dots & a_{kk} & 0 & \dots & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & \dots & 0 & b_{11} & \dots & b_{1k} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & b_{k1} & \dots & b_{kk} \end{pmatrix}$. Stručne:
 $(\mathbf{A} | \mathbf{I}_k) \sim (\mathbf{I}_k | \mathbf{A}^{-1})$.

Príklad. $\mathbf{A}^{-1} = ?$ ak $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix} \in \mathfrak{M}_{2,2}(\mathbb{R})$

$$\begin{pmatrix} 1 & 2 & 1 & 0 \\ -1 & 1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 & 0 \\ 0 & 3 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & \frac{1}{3} & \frac{1}{3} \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & \frac{1}{3} & -\frac{2}{3} \\ 0 & 1 & \frac{1}{3} & \frac{1}{3} \end{pmatrix} \Rightarrow \mathbf{A}^{-1} = \begin{pmatrix} \frac{1}{3} & -\frac{2}{3} \\ \frac{1}{3} & \frac{1}{3} \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{3} & -\frac{2}{3} \\ \frac{1}{3} & \frac{1}{3} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{3} & -\frac{2}{3} \\ \frac{1}{3} & \frac{1}{3} \end{pmatrix} \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}.$$

IX. SYSTÉMY LINEÁRNYCH ROVNÍC 2

Majme systém S s rovníc s n neznámymi nad R : $(S) \begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = b_1 \\ \dots \\ a_{s1}x_1 + \dots + a_{sn}x_n = b_s \end{cases}$.

Matica $\mathbf{A} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{s1} & \dots & a_{sn} \end{pmatrix} \in \mathfrak{M}_{s,n}(\mathbb{R})$ sa nazýva matica systému (S) . Matica

$\mathbf{A}' = \begin{pmatrix} a_{11} & \dots & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{s1} & \dots & a_{sn} & b_s \end{pmatrix} \in \mathfrak{M}_{s,n+1}(\mathbb{R})$ sa nazýva rozšírená matica systému (S) . Oz-

načme ďalej $\mathbf{B} = \begin{pmatrix} b_1 \\ \dots \\ b_s \end{pmatrix}$, to je tzv. matica pravých strán. Potom systém (S) môžeme

napísať takto: $\mathbf{A} \cdot \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \dots \\ b_s \end{pmatrix}$. t.j. ak označíme $\mathbf{X} = \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix}$ máme: $\mathbf{AX} = \mathbf{B}$. Toto

je maticový zápis systému (S) . Riešením systému $\mathbf{AX} = \mathbf{B}$ je každé $\mathbf{K} = (k_1, \dots, k_n)$ také, že $\mathbf{AK}^T = \mathbf{B}$. Ak matica $\mathbf{A}''$ vznikla z rozšírenej matice $\mathbf{A}'$ systému (S) konečným počtom ERO, tak systém, ktorého rozšírená matica je $\mathbf{A}''$ je ekvivalentná so systémom (S) . $\mathbf{AX} = \mathbf{B} \Leftrightarrow (\mathbf{AX})^T = \mathbf{B}^T \Leftrightarrow \mathbf{X}^T \mathbf{A}^T = \mathbf{B}^T \Leftrightarrow f_{\mathbf{A}^T}(\mathbf{X}^T) = \mathbf{B}^T$, kde $f_{\mathbf{A}^T} : \mathbb{R}^n \rightarrow \mathbb{R}^s$ je lineárne zobrazenie s maticou $\mathbf{A}^T$. Teda systém $\mathbf{AX} = \mathbf{B}$ je riešiteľný $\Leftrightarrow$ keď $\mathbf{B}^T \in \text{Im}(f_{\mathbf{A}^T})$. Množina riešení systému $\mathbf{AX} = \mathbf{B}$ je vlastne $(f_{\mathbf{A}^T})^{-1}(\{\mathbf{B}^T\})$.

Napríklad: $\begin{cases} x_1 + x_2 = 1 \\ x_1 - x_2 = 0 \end{cases} \quad \mathbf{A} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \mathbf{A}' = \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 0 \end{pmatrix} \quad \mathbf{X} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \quad \mathbf{B} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Riešenia sú také $(x_1, x_2) \in \mathbb{R}^2$, pre ktoré $f_{\mathbf{A}} \cdot (x_1, x_2) = (1, 0)$.

Riešenie je napr. $(\frac{1}{2}, \frac{1}{2})$. Iné riešenie nemôže mať, lebo matica $\mathbf{A}$ je regulárna, teda lineárna transformácia $f_{\mathbf{A}} : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ je lineárny izomorfizmus.

Homogénne lineárne systémy.

Definícia 9.1. Systém $(H) \begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = 0 \\ \vdots \\ a_{s1}x_1 + \dots + a_{sn}x_n = 0 \end{cases}$ sa volá *homogénny*, jeho ma-

ticový zápis je $\mathbf{AX} = \mathbf{0}$, kde $\mathbf{A}$ je matica toho systému.

Veta 9.1. Množina všetkých riešení homogénneho lineárneho systému (H) je vektorový priestor v $\mathbb{R}^n$.

Dôkaz. Označme $S =$ množinu riešení (H) . Potom $S \neq \emptyset$, lebo $(0, \dots, 0) \in S$. Použijeme kritérium vektorového podpriestoru. Nech $\alpha, \beta \in \mathbb{R}$, $K, L \in S$ sú ľubovoľné. Chceme ukázať, že $\alpha K + \beta L \in S$. Vieme, že $\mathbf{AK}^T = \mathbf{0}$, $\mathbf{AL}^T = \mathbf{0}$. Potom $\mathbf{A}(\alpha \mathbf{K}^T + \beta \mathbf{L}^T) = \alpha \mathbf{AK}^T + \beta \mathbf{AL}^T = \alpha \mathbf{0} + \beta \mathbf{0} = \mathbf{0}$. Teda naozaj $\alpha \mathbf{K}^T + \beta \mathbf{L}^T \in S$.

Iný dôkaz: $\mathbf{AX} = \mathbf{0} \Leftrightarrow \mathbf{X}^T \mathbf{A}^T = \mathbf{0}^T = \mathbf{0} \Leftrightarrow f_{\mathbf{A}^T}(\mathbf{X}^T) = \mathbf{0} \Leftrightarrow \mathbf{X}^T \in \text{Ker}(f_{\mathbf{A}^T})$. Teda $S = \text{Ker}(f_{\mathbf{A}^T})$, $f_{\mathbf{A}^T} : \mathbb{R}^n \rightarrow \mathbb{R}^s$. Vieme, že $[\text{Ker}(f_{\mathbf{A}^T})]$ jadro lineárneho zobrazenia je vektorový podpriestor. □

Nech $h(\mathbf{A}) = r$. Vieme, že konečným počtom ERO sa tá matica $\mathbf{A}$ upraví na RTM, ktorá má r nenulových riadkov. Povedzme, že tá RTM má vedúce prvky v stĺpcoch $t_1 < t_2 < \dots < t_r$. Premenením neznámych $y_1 = x_{t_1}, \dots, y_r = x_{t_r}, y_i = x_i$ v ostatných

prípadoch, dostaneme lineárny systém $(H') \begin{cases} y_1 + c_{1,r+1}y_{r+1} + \dots + c_{1n}y_n = 0 \\ \vdots \\ y_r + c_{r,r+1}y_{r+1} + \dots + c_{rn}y_n = 0 \end{cases}$.

Spätným preznačením neznámych sa od (H') dostaneme k systému s neznámymi

$x_1, \dots, x_n$, ktorého vektorový priestor riešení je priestor riešení systému (H) . Vektorový priestor riešení systému (H') je lineárne izomorfný s vektorovým priestorom riešení systému (H) . (Lineárny izomorfizmus $g: S' \rightarrow S$, $g(y_1, \dots, y_n) = (x_{t_1}, \dots, x_{t_r}, x_{r+1}, \dots, x_n)$.) Teda $\dim(S') = \dim(S)$. Teda stačí určiť $\dim(S)$. V (H') máme viazané neznáme $y_1, \dots, y_r$, kým $y_{r+1}, \dots, y_n$ sú voľné (nadobúdajú ľubovoľné hodnoty z $\mathbb{R}$). Pre $y_{r+1}=1, y_{r+2}=\dots=y_n=0$ dostaneme riešenie systému (H') . $d_{r+1}=(-c_{1,r+1}, \dots, -c_{r,r+1}, 1, 0, \dots, 0)$ atď. Pre $y_{r+1}=\dots=y_{n-1}=0, y_n=1$ dostaneme riešenie $d_n=(-c_{1n}, \dots, -c_{rn}, 0, \dots, 0, 1)$. Takto sme dostali $n-r$ riešení systému (H') .

Tvrdenie 9.1. $(d_{r+1}, \dots, d_n)$ je báza priestoru (S') , ktorý je priestorom riešení systému (H') . Teda $\dim(S') = \dim(S) = n-r$.

Dôkaz. $d_{r+1}, \dots, d_n$ sú zrejme lineárne nezávislé. Zostáva ukázať, že $d_{r+1}, \dots, d_n$ generujú priestor (S') . Nech $\mathbf{s}=(s_1, \dots, s_n) \in S'$ je ľubovoľné riešenie systému (H') . Chceme ukázať, že $\mathbf{s}$ je lineárnou kombináciou $d_{r+1}, \dots, d_n$. Takto: $(s_1, \dots, s_n) = s_{r+1}d_{r+1} + \dots + s_nd_n$. $s_1 = (-c_{1,r+1}s_{r+1} - \dots - c_{1n}s_n)$. 1.zložka vpravo: $-s_{r+1}c_{1,r+1} - \dots - s_nc_{1n}$. 1.zložka vľavo: $-c_{1,r+1}s_{r+1} - \dots - c_{1n}s_n$. Podobne pre ostatné zložky.

Dimenzia priestoru riešení homogénneho lineárneho systému = počet neznámych – hodnota matice systému. □

Príklad. Nad $\mathbb{R}$ vyriešte:

$$\begin{cases} 4x_1 + 5x_2 + 6x_3 - 3x_4 + 3x_5 = 0 \\ x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 = 0 \\ 2x_1 + 3x_2 + 4x_3 + 5x_4 + x_5 = 0 \\ 3x_1 + 4x_2 + 5x_3 + x_4 + 2x_5 = 0 \\ x_1 + 3x_2 + 5x_3 + 12x_4 + 9x_5 = 0 \end{cases}$$

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 1 & 3 & 5 & 12 & 9 \\ 4 & 5 & 6 & -3 & 3 \end{pmatrix} \sim \dots \sim \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 3 & 9 \\ 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \text{ RTM ekvivalentná s } \mathbf{A}: \begin{pmatrix} 1 & 0 & -1 & 0 & -15 \\ 0 & 1 & 2 & 0 & 12 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Teda daný systém je ekvivalentný s týmto:

$$\begin{cases} x_1 - x_3 - 15x_5 = 0 \\ x_2 + 2x_3 + 12x_5 = 0 \\ x_4 - x_5 = 0 \end{cases}$$

x_3, x_5 sú voľné. $x_3=s \in \mathbb{R}, x_5=t \in \mathbb{R}$. Pomocou nich vyjadríme x_1, x_2, x_4 : $x_4=t, x_2=-2s-12t, x_1=s+15t$. Teda vektorový priestor všetkých riešení je $S = \{(s+15t, -2s-12t, s, t, t)\} \mid s, t \in \mathbb{R}$. Báza priestoru S pre $s=1, t=0$: $(1, -2, 1, 0, 0)$, pre $s=0, t=1$: $(15, -12, 0, 1, 1)$.

Báza priestoru S je $((1, -2, 1, 0, 0), (15, -12, 0, 1, 1))$.

Veta 9.2. Pre ľubovoľnú maticu $\mathbf{A} \in \mathfrak{M}_{k,t}(\mathbb{R})$: $h(\mathbf{A}^T) = h(\mathbf{A})$.

Dôkaz. Nech $h(\mathbf{A})=r$. Uvažujme o lineárnom systéme $\mathbf{A}\mathbf{X}=\mathbf{0}$. Vektorový priestor riešení je $\text{Ker}(f_{\mathbf{A}^T})$. $f_{\mathbf{A}^T}: \mathbb{R}^t \rightarrow \text{Im}(f_{\mathbf{A}^T}), \mathbb{R}^t / \text{Ker}(f_{\mathbf{A}^T}) \cong \text{Im}(f_{\mathbf{A}^T})$. $t - \dim(\text{Ker}(f_{\mathbf{A}^T})) = \dim(\text{Im}(f_{\mathbf{A}^T}))$. $t - (t - h(\mathbf{A})) = h(\mathbf{A}^T) \Leftrightarrow h(\mathbf{A}) = h(\mathbf{A}^T)$. □

Nehomogénny systém lineárnych rovníc.

$$(N) \begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = b_1 \\ \vdots \\ a_{s1}x_1 + \dots + a_{sn}x_n = b_s \end{cases}$$

Aspoň jedno $b_i \neq 0$, tak nehomogénny systém s lineárnych rovníc s n neznámymi.

Veta 9.3. (Frobeniova, Kroneckerova – Capelliho)

Nehomogénny systém lineárnych rovníc je riešiteľný $\Leftrightarrow$ hodnosť matice systému sa rovná hodnosti rozšírenej matice systému.

Dôkaz. Maticový zápis: $\mathbf{B} = \begin{pmatrix} b_1 \\ \vdots \\ b_s \end{pmatrix}$ $\mathbf{X} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ $\mathbf{A} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{s1} & \cdots & a_{sn} \end{pmatrix}$ $\mathbf{A}\mathbf{X}=\mathbf{B} \Leftrightarrow \mathbf{X}^T\mathbf{A}^T=\mathbf{B}^T \Leftrightarrow f_{\mathbf{A}^T}(\mathbf{X}^T)=\mathbf{B}^T$. Z toho je jasné, že systém (N) je riešiteľný $\Leftrightarrow$ keď $\mathbf{B}^T \in \text{Im}(f_{\mathbf{A}^T})$. Označme a_i i -tý stĺpec matice $\mathbf{A}$. Potom $\mathbf{A}^T$ má riadky $a_1^T, \dots, a_n^T$. Systém (N) je riešiteľný $\Leftrightarrow \mathbf{B}^T \in \text{Im}(f_{\mathbf{A}^T}) \Leftrightarrow \mathbf{B}^T \in [a_1^T, \dots, a_n^T] = [a_1^T, \dots, a_n^T, \mathbf{B}^T] \Leftrightarrow \dim[a_1^T, \dots, a_n^T] = \dim[a_1^T, \dots, a_n^T, \mathbf{B}^T] \Leftrightarrow$ dimenzia priestoru generovaného riadkami matice $\mathbf{A}^T =$ dimenzia priestoru generovaného riadkami matice $(\mathbf{A}|\mathbf{B})^T \Leftrightarrow h(\mathbf{A}^T)=h((\mathbf{A}|\mathbf{B})^T) \Leftrightarrow h(\mathbf{A})=h(\mathbf{A}|\mathbf{B})$. □

Príklad. $\begin{cases} x_1 + x_2 = 1 \\ x_1 + x_2 = 4 \end{cases}$ nad $\mathbb{R}$ nie je riešiteľný, lebo $h\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = 1$ ale $h\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 4 \end{pmatrix} = 2$

Veta 9.4. Uvažujme o nehomogénnej systéme (N) . Nech P je množina všetkých jeho riešení. Potom: ak $d \in P$ je nejaké riešenie systému (N) , tak každé riešenie systému (N) je tvaru $d+c$ pre vhodné c z vektorového priestoru riešení príslušného homogénneho systému $\mathbf{A}\mathbf{X}=\mathbf{0}$. Obrátene, $d+c$ kde c je riešením príslušného homogénneho systému – je riešením systému (N) . Teda ak S je vektorový priestor riešení príslušného homogénneho systému, tak $P=d+S$

Dôkaz. Ak $p \in P$ je ľubovoľné, tak $p=d+(p-d)$. $(p-d) \in S$. $[\mathbf{A}p^T=\mathbf{B}, \mathbf{A}d^T=\mathbf{B} \Rightarrow \mathbf{A}(p-d)^T=\mathbf{A}(p^T-d^T)=\mathbf{A}p^T-\mathbf{A}d^T=\mathbf{B}-\mathbf{B}=\mathbf{0}]$. Teda $P \subset d+S$. Ľubovoľné $d+S$, kde $s \in S$, tak $d+s \in P$, lebo $\mathbf{A}(d+s)^T=\mathbf{A}d^T+\mathbf{A}s^T=\mathbf{B}+\mathbf{0}=\mathbf{B}$. Teda tiež $d+S \subset P$. Vcelku: $P=d+S$. □

Príklad. Systém nad $\mathbb{R}$: $\begin{cases} x_1 + 5x_2 + 4x_3 + 3x_4 = 1 \\ 2x_1 - x_2 + 2x_3 - x_4 = 0 \\ 5x_1 + 3x_2 + 8x_3 + x_4 = 1 \end{cases}$

$$\begin{pmatrix} 1 & 5 & 4 & 3 & 1 \\ 2 & -1 & 2 & -1 & 0 \\ 5 & 3 & 8 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} \boxed{1} & 5 & 4 & 3 & 1 \\ 0 & \boxed{11} & 6 & 7 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Viazané: x_1, x_2 , voľné: $x_3=u, x_4=v$.

$$P = \left\{ \left(\frac{1}{11} - \frac{14}{11}u + \frac{2}{11}v, \frac{2}{11} - \frac{6}{11}u - \frac{7}{11}v, u, v \right) \in \mathbb{R}^4, u, v \in \mathbb{R} \right\} =$$

$$= \left(\frac{1}{11}, \frac{2}{11}, 0, 0 \right) + \left\{ \left(-\frac{14}{11}u + \frac{2}{11}v, -\frac{6}{11}u - \frac{7}{11}v, u, v \right) \in \mathbb{R}^4, u, v \in \mathbb{R} \right\}$$

kde $\left\{ \left(-\frac{14}{11}u + \frac{2}{11}v, -\frac{6}{11}u - \frac{7}{11}v, u, v \right) \in \mathbb{R}^4, u, v \in \mathbb{R} \right\}$ je vektorový priestor riešení príslušného homogénneho systému.

Poznámka. Po úprave rozšírenej matice nehomogénneho systému na trojuholníkový tvar považujeme za viazané tie neznáme, ktoré zodpovedá vedúcim prvkom nenulových riadkov rozšírenej matice (v trojuholníkovom tvare). Ostatné sú voľné.

Determinanty.

$\{1, 2, \dots, n\}$ permutácia tejto množiny je každá bijekcia $\varphi : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$. $\varphi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \varphi(1) & \varphi(2) & \cdots & \varphi(n) \end{pmatrix}$.

Napr.: $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ je permutácia množiny $\{1, 2, 3\}$.

Definícia 9.2. $S_{\{1,2,\dots,n\}}$ = množina všetkých permutácií množiny $\{1,2,\dots,n\}$. Ak $\varphi = \begin{pmatrix} 1 & 2 & \dots & n \\ \varphi(1) & \varphi(2) & \dots & \varphi(n) \end{pmatrix} \in S_{\{1,2,\dots,n\}}$, tak hovoríme, že dvojica $(\varphi(i), \varphi(j))$ tvorí *inverziu* vo φ , ak $i < j$, ale $\varphi(i) > \varphi(j)$.

Príklad. V permutácii $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ sú 2 a 1 v inverzii.

Definícia 9.3. Počet inverzií v permutácii $\varphi \in S_{\{1,\dots,n\}}$ označíme $s(\varphi)$. Permutácia φ je *párna*, ak $(-1)^{s(\varphi)} = 1$ a φ je *nepárna*, ak $(-1)^{s(\varphi)} = -1$.

Definícia 9.4. Nech $\mathbf{A} \in \mathfrak{M}_{nn}(R)$, kde R je hocikaké pole. *Determinant* matice $\mathbf{A}$ je prvok poľa R , definovaný takto: $\det(\mathbf{A}) = \sum_{\varphi \in \{1,2,\dots,n\}} (-1)^{s(\varphi)} a_{1\varphi(1)} \cdots a_{n\varphi(n)}$.

Príklady.

1. $\mathbf{A} = (a_{11}) \in \mathfrak{M}_{11}(R) : \det(\mathbf{A}) = a_{11}$.
2. $\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, $\det(\mathbf{A}) = (-1)^{s\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}} a_{11}a_{22} + (-1)^{s\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}} a_{12}a_{21} = a_{11}a_{22} + (-1)^1 a_{12}a_{21} = a_{11}a_{22} - a_{12}a_{21}$.
3. $\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$, potom $\det(\mathbf{A}) = \cdots = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}$.

Definícia 9.5. Vyňatím prvkov i -teho riadku ($i=1,2,\dots,n$) dostaneme

$$\det(\mathbf{A}) = a_{i1} \cdot \underbrace{(\text{súčty súčinov bez } a_{i1})}_{\mathbf{A}_{i1}} + \cdots + a_{in} \cdot \underbrace{(\text{súčty súčinov bez } a_{in})}_{\mathbf{A}_{in}}$$

$\mathbf{A}_{ij}$ sa nazýva *algebraický doplnok* k prvku a_{ij} .

Uvidíme, že $\mathbf{A}_{ij}$ sa dá vyjadriť pomocou determinantu vhodnej matice stupňa $n-1$ odvodennej z $\mathbf{A}$.

Lema 9.1. Ak $\varphi, \psi \in S_{\{1,\dots,n\}}$ tak platí, že $(-1)^{s(\varphi \circ \psi)} = (-1)^{s(\varphi) + s(\psi)}$. Z toho máme, že: $(-1)^{s(\varphi)} = (-1)^{s(\varphi^{-1})}$.

Dôkaz. Pevne zvolíme $x_1, \dots, x_n \in R$ navzájom rôzne. Označme $P = \prod_{i < j} (x_i - x_j)$.

Pre $\varphi \in S_{\{1,\dots,n\}}$ a ľubovoľné $k \in \mathbb{Z}$ definujme $((-1)^k P)_\varphi = (-1)^k \prod_{1 \leq i < j \leq n} (x_{\varphi(i)} - x_{\varphi(j)})$

Je jasné, že $(-1)^k (-1)^{s(\varphi)} P = ((-1)^k P)$. Pre $\varphi, \psi \in S_{\{1,\dots,n\}} : P_{\varphi \circ \psi} = (P_\varphi)_\psi = ((-1)^{s(\varphi)} P)_\psi = (-1)^{s(\varphi)} (-1)^{s(\psi)} P = (-1)^{s(\varphi) + s(\psi)} P \Rightarrow (-1)^{s(\varphi \circ \psi)} = (-1)^{s(\varphi) + s(\psi)}$. $\square$

Vlastnosť 1. Pre každú maticu $\mathbf{A} \in \mathfrak{M}_{nn}(R)$ máme $\det(\mathbf{A}) = \det(\mathbf{A}^T)$.

Dôkaz. Prvok i -teho riadku a j -teho stĺpca v $\mathbf{A}^T$ bude $a_{ij}^T = a_{ji}$. Podľa definície determinantu vieme, že $\det(\mathbf{A}) = \sum_{\varphi \in S} (-1)^{s(\varphi)} a_{1\varphi(1)} a_{2\varphi(2)} \cdots a_{n\varphi(n)} =$

$$\begin{aligned} &= \sum_{\varphi \in S} (-1)^{s(\varphi)} a_{\varphi^{-1}(1)\varphi^{-1}(\varphi^{-1}(1))} \cdots a_{\varphi^{-1}(n)\varphi^{-1}(\varphi^{-1}(n))} = \\ &= \sum_{\varphi \in S} (-1)^{s(\varphi)} a_{\varphi^{-1}(1)} \cdots a_{\varphi^{-1}(n)} = \sum_{\varphi^{-1} \in S} (-1)^{s(\varphi)} a_{1\varphi^{-1}(1)}^T \cdots a_{n\varphi^{-1}(n)}^T = \\ &= \sum_{\varphi^{-1} \in S} (-1)^{s(\varphi^{-1})} a_{1\varphi^{-1}(1)}^T \cdots a_{n\varphi^{-1}(n)}^T = \det(\mathbf{A}^T). \end{aligned}$$

$\square$

Vlastnosť 2. Ak matica $\mathbf{B} \in \mathfrak{M}_{nn}(R)$ vznikne z matice $\mathbf{A} \in \mathfrak{M}_{nn}(R)$ jednou vzájomnou výmenou ľubovoľných dvoch riadkov, tak $\det(\mathbf{B}) = -\det(\mathbf{A})$.

Dôkaz. Napr. nech $\mathbf{B}$ vznikne z $\mathbf{A}$ vzájomnou výmenou prvého a druhého riadku.

Teda, ak $\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$, tak $\mathbf{B} = \begin{pmatrix} a_{21} & a_{22} & \cdots & a_{2n} \\ a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$. Označme

$$\psi = \begin{pmatrix} 1 & 2 & \cdots & n \\ 2 & 1 & \cdots & n \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n \\ \varphi(1) & \varphi(2) & \cdots & \varphi(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ \varphi(2) & \varphi(1) & \cdots & \varphi(n) \end{pmatrix},$$

$$(-1)^{s(\psi)} = (-1)^{s(\varphi)} (-1)^{s(\psi)} = -(-1)^{s(\varphi)}. \text{ Z definície determinantu:}$$

$$\det(\mathbf{B}) = \sum_{\varphi \in S} (-1)^{s(\varphi)} b_{1\varphi(1)} b_{2\varphi(2)} \cdots b_{n\varphi(n)} = \sum_{\varphi \in S} (-1)^{s(\varphi)} a_{2\varphi(1)} a_{1\varphi(2)} \cdots a_{n\varphi(n)} =$$

$$= \sum_{\varphi \in S} (-1)^{s(\varphi)} a_{1\varphi(2)} a_{2\varphi(1)} \cdots a_{n\varphi(n)} = \sum_{\psi \in S} (-1)^{s(\varphi)} a_{1\psi(1)} a_{2\psi(2)} \cdots a_{n\psi(n)} =$$

$$= - \sum_{\psi \in S} (-1)^{s(\psi)} a_{1\psi(1)} a_{2\psi(2)} \cdots a_{n\psi(n)} = -\det(\mathbf{A}).$$

□

Vlastnosť 3. Nech $\mathbf{A} = a_{ij} \in \mathfrak{M}_{nn}(R)$. Potom pre ľubovoľné $r, s \in \{1, \dots, n\}$ algebroidný doplnok k prvku a_{rs} je $\mathbf{A}_{rs} = (-1)^{r+s} \det(\mathbf{M}_{rs})$. Kde matica $\mathbf{M}_{rs}$ je matica typu $(r-1) \times (n-1)$, ktorá vznikne vynechaním r -teho riadku a s -teho stĺpca z matice $\mathbf{A}$.

Príklad. $\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \quad \mathbf{A}_{23} = (-1)^5 \det \begin{pmatrix} a_{11} & a_{12} \\ a_{31} & a_{32} \end{pmatrix}$

Dôkaz. Z definície determinantu: $\det(\mathbf{A}) = \sum_{\varphi \in S} (-1)^{s(\varphi)} \prod_{i=1}^n a_{i\varphi(i)} =$

$$= \sum_{\varphi \in S} (-1)^{s(\varphi)} a_{11} a_{2\varphi(2)} \cdots a_{n\varphi(n)} + \sum_{\varphi \in S} (-1)^{s(\varphi)} a_{1\varphi(1)} a_{2\varphi(2)} \cdots a_{n\varphi(n)}.$$

Z toho: $\mathbf{A}_{11} = \sum_{\varphi \in S} (-1)^{s(\varphi)} a_{2\varphi(2)} \cdots a_{n\varphi(n)} = \sum_{\psi \in S'} (-1)^{s(\psi)} a_{2\psi(2)} \cdots a_{n\psi(n)} =$

$$= \det \begin{pmatrix} a_{22} & \cdots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{n2} & \cdots & a_{nn} \end{pmatrix} = \det(\mathbf{M}_{11}) = (-1)^{1+1} \det(\mathbf{M}_{11}).$$

Teraz rátame $\mathbf{A}_{rs}$ pre ľubovoľné $r, s \in \{1, \dots, n\}$:

$$\mathbf{A} = \begin{pmatrix} a_{11} & \cdots & a_{1s-1} & a_{1s} & a_{1s+1} & \cdots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{r-11} & \cdots & a_{r-1s-1} & a_{r-1s} & a_{r-1s+1} & \cdots & a_{r-1n} \\ a_{r1} & \cdots & a_{rs-1} & a_{rs} & a_{rs+1} & \cdots & a_{rn} \\ a_{r+11} & \cdots & a_{r+1s-1} & a_{r+1s} & a_{r+1s+1} & \cdots & a_{r+1n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \cdots & a_{ns-1} & a_{ns} & a_{ns+1} & \cdots & a_{nn} \end{pmatrix}$$

Vzájomná výmena $r-1$ riadkov:

$$\mathbf{B} = \begin{pmatrix} a_{r1} & \cdots & a_{rs-1} & a_{rs} & a_{rs+1} & \cdots & a_{rn} \\ a_{11} & \cdots & a_{1s-1} & a_{1s} & a_{1s+1} & \cdots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{r-11} & \cdots & a_{r-1s-1} & a_{r-1s} & a_{r-1s+1} & \cdots & a_{r-1n} \\ a_{r+11} & \cdots & a_{r+1s-1} & a_{r+1s} & a_{r+1s+1} & \cdots & a_{r+1n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \cdots & a_{ns-1} & a_{ns} & a_{ns+1} & \cdots & a_{nn} \end{pmatrix}$$

Vzájomná výmena $s-1$ stĺpcov:

$$\mathbf{C} = \begin{pmatrix} a_{rs} & a_{r1} & \cdots & a_{rs-1} & a_{rs+1} & \cdots & a_{rn} \\ a_{1s} & a_{11} & \cdots & a_{1s-1} & a_{1s+1} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{r-1s} & a_{r-11} & \cdots & a_{r-1s-1} & a_{r-1s+1} & \cdots & a_{r-1n} \\ a_{r+1s} & a_{r+11} & \cdots & a_{r+1s-1} & a_{r+1s+1} & \cdots & a_{r+1n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{ns} & a_{n1} & \cdots & a_{ns-1} & a_{ns+1} & \cdots & a_{nn} \end{pmatrix}$$

Z toho čo sme dokázali vieme, že $\det(\mathbf{C}) = a_{rs} \det(\mathbf{M}_{rs}) + \text{členy bez } a_{rs}$. Z 1. a 2. vlastnosti: $(-1)^{s-1} \det(\mathbf{B}) = \det(\mathbf{C}) = (-1)^{s-1} \cdot (-1)^{r-1} \det(\mathbf{A}) = (-1)^{r+s} \det(\mathbf{A})$.
 $\det(\mathbf{A}) = a_{rs} (-1)^{r+s} \det(\mathbf{M}_{rs}) + (-1)^{r+s} \cdot \text{členy bez } a_{rs} \Rightarrow \mathbf{A}_{rs} = (-1)^{r+s} \det(\mathbf{M}_{rs})$. $\square$

Veta 9.5. (Laplaceova o rozvoji determinantoch)

Pre $\mathbf{A} \in \mathfrak{M}_{nn}(R)$ máme: $\det(\mathbf{A}) = a_{i1}(-1)^{i+1} \det(\mathbf{M}_{i1}) + \cdots + a_{in}(-1)^{i+n} \det(\mathbf{M}_{in})$. Toto vyjadrenie sa nazýva Laplaceov rozvoj determinantu matice $\mathbf{A}$ podľa i -teho riadku. Tiež: $\det(\mathbf{A}) = a_{1j}(-1)^{j+1} \det(\mathbf{M}_{1j}) + \cdots + a_{nj}(-1)^{n+j} \det(\mathbf{M}_{nj})$ pre všetky $j \in \{1, \dots, n\}$ tzv. rozvoj podľa j -teho stĺpca.

Dôkaz. Dôsledok vlastnosti 3. Máme $\det(\mathbf{A}) = a_{i1} \mathbf{A}_{i1} + \cdots + a_{in} \mathbf{A}_{in}$. Z vlastnosti 3 dosadíme vyjadrenia $\mathbf{A}_{ik} = (-1)^{i+k} \det(\mathbf{M}_{ik})$. S využitím vlastnosti 1 stĺpcový rozvoj. (t.j. $\det(\mathbf{A}^T) = \det(\mathbf{A})$.) $\square$

Príklad. $\det \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & 1 \\ 0 & 1 & 3 \end{pmatrix} = 1 \cdot \det \begin{pmatrix} -1 & 1 \\ 1 & 3 \end{pmatrix} + 0 = -4$.

Vlastnosť 4. Ak sú v matici $\mathbf{A} \in \mathfrak{M}_{nn}(R)$ dva riadky rovnaké (príp. dva stĺpce), tak $\det(\mathbf{A}) = 0$.

Dôkaz. Indukcia vzhľadom na n . Pre $n=2$: $\det \begin{pmatrix} a & b \\ a & b \end{pmatrix} = ab - ab = 0$.

Indukčný predpoklad: Predpokladajme, že tvrdenie platí pre také matice typu $n-1 \times n-1$. Nech $\mathbf{A} \in \mathfrak{M}_{nn}(R)$. Nech r -tý a s -tý riadok ($r < s$) v $\mathbf{A}$ sú rovnaké. Rozviňme determinant matice $\mathbf{A}$ podľa i -teho riadku, kde $i \neq r, i \neq s$. Potom $\det(\mathbf{A}) = a_{i1}(-1)^{i+1} \det(\mathbf{M}_{i1}) + \cdots + a_{in}(-1)^{i+n} \det(\mathbf{M}_{in})$. $\mathbf{M}_{ij}$ sú matice stupňa $n-1$, ktoré majú dva rovnaké riadky. Potom z indukčného predpokladu: $\det(\mathbf{A}) = 0$. $\square$

Vlastnosť 5. Nech $\mathbf{B} \in \mathfrak{M}_{nn}(R)$ vznikne z $\mathbf{A} \in \mathfrak{M}_{nn}(R)$ prirátaním ľubovoľného násobku ľubovoľného riadku v $\mathbf{A}$ k inému riadku v $\mathbf{A}$. Potom $\det(\mathbf{A}) = \det(\mathbf{B})$.

Dôkaz. Nech napríklad $\mathbf{B}$ vznikne z $\mathbf{A}$ tak, že k 1.riadku prirátame α -násobok 2.riadku. Rozviňme determinant $\mathbf{B}$ podľa prvého riadku:

$$\begin{aligned} \det(\mathbf{B}) &= (a_{11} + \alpha a_{21})(-1)^{1+1} \det(\mathbf{M}_{11}) + \cdots + (a_{1n} + \alpha a_{2n})(-1)^{1+n} \det(\mathbf{M}_{1n}) = \\ &= a_{11}(-1)^{1+1} \det(\mathbf{M}_{11}) + \cdots + a_{1n}(-1)^{1+n} \det(\mathbf{M}_{1n}) + \alpha(a_{21}(-1)^{1+1} \det(\mathbf{M}_{11}) + \cdots + \\ &+ a_{2n}(-1)^{1+n} \det(\mathbf{M}_{1n})) = \det(\mathbf{A}) + \alpha \det(\text{matice, ktorá má rovnaký 1. a 2.riadok}) \\ &= \det(\mathbf{A}). \end{aligned}$$

$\square$

Vlastnosť 6. Nech $\mathbf{B}$ vznikne z $\mathbf{A} \in \mathfrak{M}_{nn}(R)$ tak, že i -tý riadok (iba tento) vynásobíme $\alpha \in R - \{0\}$. Potom $\det(\mathbf{B}) = \alpha \det(\mathbf{A})$.

Dôkaz. Rozviňme determinant matice $\mathbf{B}$ podľa i -teho riadku:

$$\begin{aligned} \det(\mathbf{B}) &= \alpha a_{i1}(-1)^{i+1} \det(\mathbf{M}_{i1}) + \cdots + \alpha a_{in}(-1)^{i+n} \det(\mathbf{M}_{in}) = \\ &= \alpha [a_{i1}(-1)^{i+1} \det(\mathbf{M}_{i1}) + \cdots + a_{in}(-1)^{i+n} \det(\mathbf{M}_{in})] = \alpha \det(\mathbf{A}). \end{aligned}$$

$\square$

Vlastnosť 7.

$$\det \begin{pmatrix} \vec{a}_1 \\ \dots \\ \vec{a}_{i-1} \\ \vec{a}_i + \vec{b}_i \\ \dots \\ \vec{a}_n \end{pmatrix} = \det \begin{pmatrix} \vec{a}_1 \\ \dots \\ \vec{a}_{i-1} \\ \vec{a}_i \\ \dots \\ \vec{a}_n \end{pmatrix} + \det \begin{pmatrix} \vec{a}_1 \\ \dots \\ \vec{a}_{i-1} \\ \vec{b}_i \\ \dots \\ \vec{a}_n \end{pmatrix}$$

Dôkaz. Rozvoj podľa i -teho riadku. □

Vlastnosť 8. Ak matica $\mathbf{A} \in \mathfrak{M}_{nn}(R)$ má nulový riadok, tak $\det(\mathbf{A})=0$.

Dôkaz. Priamo z definície. □

Ak maticu $\mathbf{A} \in \mathfrak{M}_{nn}(R)$ upravíme pomocou ERO na trojuholníkovú maticu:

$$\mathbf{T} = \begin{pmatrix} t_{11} & t_{12} & \dots & t_{1n} \\ 0 & t_{22} & \dots & t_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & t_{nn} \end{pmatrix}$$

tak buď niektorý z prvkov $t_{11}, \dots, t_{nn}$ je 0 (to je vtedy, keď $h(\mathbf{T}) < n$ t.j. ak $\mathbf{T}$ je singulárna), alebo všetky $t_{11}, \dots, t_{nn}$ sú nenulové (to je vtedy, keď $h(\mathbf{A})=n$). Z Laplaceovej vety o rozvoji determinantu (ale aj priamo z definície) je jasné, že $\det(\mathbf{T}) = t_{11} \cdot t_{22} \cdot \dots \cdot t_{nn}$.

Príklad. Jedna z metód výpočtu $\det(\mathbf{A})$: $\mathbf{A}$ postupne upravujeme na trojuholníkovú maticu, ak zohľadníme vplyv jednotlivých ERO na determinant a fakt, že determinant trojuholníkovej matice je súčin prvkov hlavnej diagonály, tak ľahko vyrátame $\det(\mathbf{A})$.

$$\det \begin{pmatrix} 1 & -1 & 1 \\ -1 & 1 & 1 \\ 1 & 1 & -1 \end{pmatrix} = \det \begin{pmatrix} 1 & -1 & 1 \\ 0 & 0 & 2 \\ 0 & 2 & -2 \end{pmatrix} = - \det \begin{pmatrix} 1 & -1 & 1 \\ 0 & 2 & -2 \\ 0 & 0 & 2 \end{pmatrix} = -4 \cdot \det \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} = -4.$$

Tvrdenie 9.2. Matica $\mathbf{A} \in \mathfrak{M}_{nn}(R)$ je regulárna $\Leftrightarrow \det(\mathbf{A}) \neq 0$.

Dôkaz. Vieme, že $\mathbf{A}$ je regulárna $\Leftrightarrow$ je riadkovo ekvivalentná s nejakou trojuholníkovou maticou $\mathbf{T}$, pričom $t_{ii} \neq 0$ čiže $\prod_{k=1}^n t_{kk} \neq 0$. Z toho aký vplyv majú jednotlivé ERO na determinant vieme, že musí existovať $\alpha \in R - \{0\}$ také, že $\det(\mathbf{A}) = \alpha \cdot \det(\mathbf{T})$. Vcelku máme, že $\mathbf{A}$ je regulárna $\Leftrightarrow \det(\mathbf{T}) \neq 0 \Leftrightarrow \det(\mathbf{A}) \neq 0$. □

Príklad. Reálna matica $\begin{pmatrix} 1 & -1 & 1 \\ -1 & 1 & 1 \\ 1 & 1 & -1 \end{pmatrix}$ je regulárna, lebo jej determinant je nenulový.

Príklad.

$$\det \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & \dots & 1 \\ 1 & 1 & 0 & \dots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \dots & 0 \end{pmatrix} = \det \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & -1 & 0 & \dots & 0 \\ 0 & 0 & -1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & -1 \end{pmatrix} = (-1)^{n-1}$$

Príklad. **Vandermondov determinant**

$$\det \begin{pmatrix} 1 & 1 & 1 & 1 \\ a & b & c & d \\ a^2 & b^2 & c^2 & d^2 \\ a^3 & b^3 & c^3 & d^3 \end{pmatrix} = \det \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & b-a & c-a & d-a \\ 0 & b^2-a^2 & c^2-a^2 & d^2-a^2 \\ 0 & b^3-a^3 & c^3-a^3 & d^3-a^3 \end{pmatrix} = \det \begin{pmatrix} b-a & c-a & d-a \\ b^2-a^2 & c^2-a^2 & d^2-a^2 \\ b^3-a^3 & c^3-a^3 & d^3-a^3 \end{pmatrix} =$$

$$\begin{aligned}
&= \det \begin{pmatrix} b-a & c-a & d-a \\ b^2-ab & c^2-ac & d^2-ad \\ b^3-a^2b & c^3-a^2c & d^3-a^2d \end{pmatrix} = (b-a)(c-a)(d-a) \cdot \det \begin{pmatrix} 1 & 1 & 1 \\ b & c & d \\ b^2+ab & c^2+ac & d^2+ad \end{pmatrix} = \\
&= (b-a)(c-a)(d-a) \cdot \det \begin{pmatrix} 1 & 1 & 1 \\ b & c & d \\ b^2 & c^2 & d^2 \end{pmatrix} = (b-a)(c-a)(d-a) \cdot \det \begin{pmatrix} 1 & 1 & 1 \\ 0 & c-b & d-b \\ 0 & c^2-b^2 & d^2-b^2 \end{pmatrix} = \\
&= (b-a)(c-a)(d-a) \cdot \det \begin{pmatrix} c-b & d-b \\ c^2-b^2 & d^2-b^2 \end{pmatrix} = (b-a)(c-a)(d-a)(c-b)(d-b)(d-c).
\end{aligned}$$

Veta 9.6. Pre ľubovoľné $\mathbf{A}, \mathbf{B} \in \mathfrak{M}_{nn}(R)$: $\det(\mathbf{AB}) = \det(\mathbf{A}) \det(\mathbf{B})$.

Dôkaz. Ak $\mathbf{A}$, alebo $\mathbf{B}$ je singulárna, tak veta zrejme platí. $f_{\mathbf{AB}} : \mathbb{R}^n \rightarrow \mathbb{R}^n$ je lineárny izomorfizmus s maticou $\mathbf{AB}$. Vieme, že $f_{\mathbf{AB}} = f_{\mathbf{B}} \circ f_{\mathbf{A}}$. Ak $\mathbf{A}$ je singulárna, tak $f_{\mathbf{A}}$ zobrazí nejaký vektor $\vec{a} \in \mathbb{R}^n$, $\vec{a} \neq \vec{0}$ na nulový. Teda $f_{\mathbf{A}}(\vec{a}) = \vec{0}$. Potom $f_{\mathbf{B}} \circ f_{\mathbf{A}}(\vec{a}) = \vec{0} = f_{\mathbf{AB}}(\vec{a})$ a teda $\mathbf{AB}$ je singulárna, teda $\det(\mathbf{AB}) = 0$. Podobne ak $\mathbf{B}$ je singulárna a $\mathbf{A}$ je regulárna. Ak $\mathbf{A}$ aj $\mathbf{B}$ sú singulárne, tak tiež platí.

Ďalej: Predpokladajme, že $\mathbf{A}$ aj $\mathbf{B}$ sú regulárne. Keďže $\mathbf{A}$ je regulárna, dá sa konečným počtom ERO upraviť na trojuholníkovú maticu $\mathbf{T} = \begin{pmatrix} t_{11} & \cdots & t_{1n} \\ \cdots & t_{ii} & \cdots \\ 0 & \cdots & t_{nn} \end{pmatrix}$, pričom

$t_{ii} \neq 0$. Každá ERO sa dá realizovať tak, že danú maticu zľava vynásobíme takzvanou elementárnou maticou, ktorá prislúcha k tej ERO. Teda: $\mathbf{E}_1 \cdot \mathbf{E}_2 \cdots \mathbf{E}_k \cdot \mathbf{A} = \mathbf{T}$, kde $\mathbf{E}_i$ sú elementárne matice prislúchajúce k použitým ERO. Pretože $\mathbf{A}$ je regulárna, na jej úpravu na $\mathbf{T}$ stačí použiť iba prirátavanie násobkov riadkov k iným riadkom. Teda $\det(\mathbf{A}) = \det(\mathbf{E}_k \mathbf{A}) = \det(\mathbf{E}_{k-1} \mathbf{E}_k \mathbf{A}) = \cdots = \det(\mathbf{E}_1 \cdots \mathbf{E}_k \mathbf{A}) = \det(\mathbf{T})$. Analogicky ako ERO sa definujú aj ESO, k nim prislúchajú elementárne matice (taká matica vznikne z jednotkovej tak, že na nej urobíme tú ESO). Matica $\mathbf{B}$ sa konečným počtom ESO (zas vystačíme iba s prirátavaním násobkov stĺpcov k iným stĺpcom,

keďže $\mathbf{B}$ je regulárna) upraví na trojuholníkovú maticu $\mathbf{T}' = \begin{pmatrix} t'_{11} & \cdots & t'_{1n} \\ \vdots & \ddots & \vdots \\ 0 & \cdots & t'_{nn} \end{pmatrix}$ pričom

$\prod t'_{ii} \neq 0$. Urobiť nejaké ESO je to isté, ako danú maticu sprava vynásobiť príslušnou elementárnou maticou. Teda: $\mathbf{B} \mathbf{F}_1 \cdots \mathbf{F}_p = \mathbf{T}'$, kde $\mathbf{F}_i$ sú príslušné elementárne matice. Pritom $\mathbf{F}_1, \cdots, \mathbf{F}_p$ zodpovedajú iba prirátavaním násobku stĺpca k inému stĺpcu. Potom: $\det(\mathbf{B}) = \det(\mathbf{B} \mathbf{F}_1) = \cdots = \det(\mathbf{B} \mathbf{F}_1 \cdots \mathbf{F}_p) = \det(\mathbf{T}')$. Teraz

$$\begin{aligned}
\det(\mathbf{T} \mathbf{T}') &= \det \left(\begin{pmatrix} t_{11} & t_{12} & \cdots & t_{1n} \\ 0 & t_{21} & \cdots & t_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & t_{nn} \end{pmatrix} \begin{pmatrix} t'_{11} & t'_{12} & \cdots & t'_{1n} \\ 0 & t'_{22} & \cdots & t'_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & t'_{nn} \end{pmatrix} \right) = \\
&= \det \begin{pmatrix} t_{11}t'_{11} & \cdots & \cdots & \cdots \\ 0 & t_{22}t'_{22} & \cdots & \cdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & t_{nn}t'_{nn} \end{pmatrix} = t_{11}t'_{11} \cdots t_{nn}t'_{nn} = t_{11} \cdots t_{nn} t'_{11} \cdots t'_{nn} =
\end{aligned}$$

$$\begin{aligned}
&= \det(\mathbf{T}) \cdot \det(\mathbf{T}'). \text{ Potom } \det(\mathbf{A} \cdot \mathbf{B}) = \det(\mathbf{E}_1 \cdots \mathbf{E}_k \mathbf{A} \cdot \mathbf{B}) = \\
&= \det(\mathbf{E}_1 \cdots \mathbf{E}_k \mathbf{A} \cdot \mathbf{B} \mathbf{F}_1 \cdots \mathbf{F}_p) = \det(\mathbf{T} \mathbf{T}') = \det(\mathbf{T}) \det(\mathbf{T}') = \det(\mathbf{A}) \det(\mathbf{B}).
\end{aligned}$$

□

Inverzná matica pomocou determinantu.

Nech $\mathbf{A} = (a_{ij}) \in \mathfrak{M}_{nn}(R)$ je regulárna. Vieme, že existuje inverzná matica $\mathbf{A}^{-1}$. Definujme tzv. *adjungovanú* maticu k $\mathbf{A}$ ako maticu:

$$\text{adj}(\mathbf{A}) = \begin{pmatrix} A_{11} & A_{21} & \cdots & A_{n1} \\ A_{12} & A_{22} & \cdots & A_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ A_{1n} & A_{2n} & \cdots & A_{nn} \end{pmatrix}$$

Nech A_{ij} je algebraický doplnok k prvku a_{ij} . Teda $A_{ij} = (-1)^{i+j} \det(\mathbf{M}_{ij})$.

Veta 9.7. Ak $\mathbf{A}=(a_{ij})\in\mathfrak{M}_{nn}(R)$ je regulárna, tak $\mathbf{A}^{-1}=\frac{adj(\mathbf{A})}{\det(\mathbf{A})}$.

Dôkaz. Rátajme $\mathbf{C}=\mathbf{A}\cdot\frac{adj(\mathbf{A})}{\det(\mathbf{A})}\stackrel{?}{=}\mathbf{I}_n$. Matica $\frac{1}{\det(\mathbf{A})}\cdot\mathbf{A}\cdot adj(\mathbf{A})$ má na hlavnej diagonále prvky: $c_{ii}=\frac{1}{\det(\mathbf{A})}\cdot\underbrace{(a_{i1}A_{i1}+\dots+a_{in}A_{in})}_{\det(\mathbf{A})}=1$ a mimo hlavnej diagonály prvky (tj. pre $i\neq j$) $c_{ij}=\frac{1}{\det(\mathbf{A})}(a_{i1}A_{j1}+\dots+a_{in}A_{jn})=0$. Teda $\mathbf{C}=\mathbf{I}_n$. □

Príklad. $\mathbf{A}=\begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}$ $adj(\mathbf{A})=\begin{pmatrix} 1 & -2 \\ 1 & 1 \end{pmatrix}$ $\mathbf{A}^{-1}=\frac{1}{3}\cdot\begin{pmatrix} 1 & -2 \\ 1 & 1 \end{pmatrix}$

Systémy n rovníc s n neznámymi.

Fredholmova alternatíva.

Nech $\mathbf{AX}=\mathbf{B}$ je systém n lineárnych rovníc s n neznámymi. Potom sú dve možnosti:

1. Systém $\mathbf{AX}=\mathbf{B}$ má jediné riešenie bez ohľadu na to, aká je pravá strana $\mathbf{B}$ (to nastane vtedy, keď $h(\mathbf{A})=n$, t.j. vtedy, keď $\det(\mathbf{A})\neq 0$) a zároveň príslušný homogénny systém $\mathbf{AX}=\mathbf{0}$ má iba triviálne riešenie.
2. Nehomogénny systém $\mathbf{AX}=\mathbf{B}$ je riešiteľný už nie pre všetky $\mathbf{B}$, ale iba pre také, pre ktoré $h(\mathbf{A} \mid \mathbf{B})=h(\mathbf{A})$, to sa stane vtedy, keď $h(\mathbf{A})<n$ t.j. $\det(\mathbf{A})=0$, a zároveň príslušný homogénny lineárny systém má aspoň jedno triviálne riešenie.

Cramerovo pravidlo. Majme nehomogénny lineárny systém n rovníc s n neznámymi nad R : $\mathbf{AX}=\mathbf{B}$, kde $\mathbf{A}=\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$ $\mathbf{X}=\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ $\mathbf{B}=\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$. Predpokladajme, že $\mathbf{A}$ je regulárna. Potom systém $\mathbf{AX}=\mathbf{B}$ má jediné riešenie: $\mathbf{X}=\mathbf{A}^{-1}\mathbf{B}$.

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \frac{1}{\det(\mathbf{A})} \begin{pmatrix} A_{11} & \dots & A_{n1} \\ \vdots & \ddots & \vdots \\ A_{1n} & \dots & A_{nn} \end{pmatrix} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}, \text{ teda } x_i = \frac{1}{\det(\mathbf{A})} (A_{1i}b_1 + \dots + A_{ni}b_n) =$$

$$= \frac{1}{\det(\mathbf{A})} \det(\text{matice, ktorá vznikne tak, že } i\text{-tý stĺpec nahradíme } \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}).$$

Označme $\mathbf{A}_i = \begin{pmatrix} a_{11} & \dots & a_{1i-1} & b_1 & a_{1i+1} & \dots & a_{1n} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{ni-1} & b_n & a_{ni+1} & \dots & a_{nn} \end{pmatrix}$, tak potom jediné riešenie systému $\mathbf{AX}=\mathbf{B}$ je $\left(\frac{\det(\mathbf{A}_1)}{\det(\mathbf{A})}; \dots; \frac{\det(\mathbf{A}_n)}{\det(\mathbf{A})}\right)$.

Príklad. Lineárny systém nad $\mathbb{Z}_5$:

$$\begin{cases} 3x_1 + 4x_2 = 1 \\ x_1 + x_2 + 2x_3 = 1 \\ 3x_1 + 4x_2 + x_3 = 0 \end{cases} \quad \begin{pmatrix} 3 & 4 & 0 \\ 1 & 1 & 2 \\ 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

$\det(\mathbf{A})=4$, $\det(\mathbf{A}_1)=4$, $\det(\mathbf{A}_2)=3$, $\det(\mathbf{A}_3)=1$. Jediné riešenie systému daného je: $(4\cdot 4^{-1}, 3\cdot 4^{-1}, 1\cdot 4^{-1}) = (1, 2, 4) \in \mathbb{Z}_5$.

Príklad. Využitím Cramerovho pravidla riešte:

$$\begin{cases} x_1 + 5x_2 + 4x_3 + 3x_4 = 1 \\ 2x_1 - x_2 + 2x_3 - x_4 = 0 \end{cases} \quad \det \begin{pmatrix} 1 & 5 \\ 2 & -1 \end{pmatrix} = -11 \neq 0$$

Rovnice sú lineárne nezávislé, x_1, x_2 budú viazané x_3, x_4 budú voľné neznáme.

$$\begin{cases} x_1 + 5x_2 = 1 - 4u - 3v \\ 2x_1 - x_2 = -2u + v \end{cases} \Rightarrow \det(\mathbf{A}) = \begin{pmatrix} 1-4u-3v & 5 \\ -2u+v & -1 \end{pmatrix} = -1+14u-2v$$

$$\det(\mathbf{A}_2) = \begin{pmatrix} 1 & 1-4u-3v \\ 2 & -2u+v \end{pmatrix} = -2+6u+7v$$

Potom všeobecné riešenie daného systému je:

$$\left(\frac{1}{11} - \frac{14}{11}u + \frac{2}{11}v; \frac{2}{11} - \frac{6}{11}u - \frac{7}{11}v; u; v \right)$$

X. EUKLIDOVSKÝ VEKTOROVÝ PRIESTOR

Definícia 10.1. Nech V je vektorový priestor nad R . Potom skalárny súčin na V je zobrazenie $g : V \times V \rightarrow R$ pre ktoré platia tieto podmienky:

1. $g(\vec{x} + \vec{y}, \vec{z}) = g(\vec{x}, \vec{z}) + g(\vec{y}, \vec{z})$ pre $\forall \vec{x}, \vec{y}, \vec{z} \in V$.
2. $g(\vec{y}, \vec{x}) = g(\vec{x}, \vec{y})$ pre $\forall \vec{x}, \vec{y} \in V$.
3. $g(\alpha \vec{x}, \vec{y}) = \alpha g(\vec{x}, \vec{y})$ pre $\forall \vec{x}, \vec{y} \in V, \alpha \in R$.
4. Ak $\vec{x} \neq \vec{0}$, tak $g(\vec{x}, \vec{x}) > 0$.

Ak g je nejaký skalárny súčin na V , tak V sa nazýva *euklidovský* vektorový priestor (presnejšie je to euklidovský vektorový priestor (V, g)).

Poznámka. Ak g je skalárny súčin na V , tak namiesto $g(\vec{x}, \vec{y})$ sa často píše $\langle \vec{x}, \vec{y} \rangle$. $\langle \cdot, \cdot \rangle : V \times V \rightarrow R$. Potom vlastnosti skalárneho súčinu sa prepíšu takto:

1. $\langle \vec{x} + \vec{y}, \vec{z} \rangle = \langle \vec{x}, \vec{z} \rangle + \langle \vec{y}, \vec{z} \rangle$.
2. $\langle \vec{y}, \vec{x} \rangle = \langle \vec{x}, \vec{y} \rangle$.
3. $\langle \alpha \vec{x}, \vec{y} \rangle = \alpha \langle \vec{x}, \vec{y} \rangle$.
4. Ak $\vec{x} \in V - \{\vec{0}\}$, tak $\langle \vec{x}, \vec{x} \rangle > 0$.

Príklad. Pre $\mathbb{R}^n$ zoberme zobrazenie $\langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$,

$$\langle (x_1, \dots, x_n), (y_1, \dots, y_n) \rangle = x_1 y_1 + \dots + x_n y_n.$$

1. $\langle (x_1, \dots, x_n) + (z_1, \dots, z_n), (y_1, \dots, y_n) \rangle = \langle (x_1 + z_1, \dots, x_n + z_n), (y_1, \dots, y_n) \rangle = (x_1 + z_1)y_1 + \dots + (x_n + z_n)y_n = \langle (x_1, \dots, x_n), (y_1, \dots, y_n) \rangle + \langle (z_1, \dots, z_n), (y_1, \dots, y_n) \rangle = \langle \vec{x}, \vec{y} \rangle + \langle \vec{z}, \vec{y} \rangle$. Zistili sme, že vyššie definované zobrazenie $\langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$, $\langle (x_1, \dots, x_n), (y_1, \dots, y_n) \rangle = x_1 y_1 + \dots + x_n y_n$ je tzv. štandardný skalárny súčin na $\mathbb{R}^n$. (Existujú aj iné skalárne súčiny.)

Príklad. Euklidovský priestor nemusí byť konečne generovaný. $V = C(\langle 0, 1 \rangle) =$ priestor spojitých funkcií na $\langle 0, 1 \rangle$. Definujme zobrazenie: $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{R}$ takto: $\langle f, g \rangle = \int_0^1 f(x)g(x)dx$. $(C\langle 0, 1 \rangle, \langle \cdot, \cdot \rangle)$ je euklidovský vektorový priestor nie konečne generovaný.

Poznámka. Nech V je vektorový priestor nad $\mathbb{C}$. Skalárny súčin na V je zobrazenie $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{C}$, ktoré spĺňa:

1. $\langle \vec{x} + \vec{y}, \vec{z} \rangle = \langle \vec{x}, \vec{z} \rangle + \langle \vec{y}, \vec{z} \rangle$.
2. $\langle \vec{y}, \vec{x} \rangle = \overline{\langle \vec{x}, \vec{y} \rangle}$. (komplexne združené)
3. $\langle \alpha \vec{x}, \vec{y} \rangle = \alpha \langle \vec{x}, \vec{y} \rangle$.
4. Ak $\vec{x} \in V - \{\vec{0}\}$, tak $\langle \vec{x}, \vec{x} \rangle > 0$.

Príklad. $V = \mathbb{C}^n$ ($n \leq 1$). Definujme: $\langle \cdot, \cdot \rangle : \mathbb{C}^n \times \mathbb{C}^n \rightarrow \mathbb{C}$

$\langle (x_1, \dots, x_n), (w_1, \dots, w_n) \rangle = z_1 \bar{w}_1 + \dots + z_n \bar{w}_n$. Ak V je vektorový priestor nad $\mathbb{C}$ a $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{C}$ je skalárny súčin, tak $(V, \langle \cdot, \cdot \rangle)$ sa volá *unitárny* (alebo hermitovský) priestor.

V ďalšom už iba reálne euklidovské priestory uvažujeme!

Definícia 10.2. Nech $(V, \langle \cdot, \cdot \rangle)$ je euklidovský vektorový priestor. Potom *dĺžka* ľubovoľného vektora $\vec{x} \in V$ sa definuje ako reálne číslo: $|\vec{x}| = \sqrt{\langle \vec{x}, \vec{x} \rangle}$.

Príklad. V $\mathbb{R}^3$ so štandardným skalárnym súčinom: $|(1, 1, 1)| = \sqrt{1^2 + 1^2 + 1^2} = \sqrt{3}$.

Veta 10.1. Nech $(V, \langle \cdot, \cdot \rangle)$ je euklidovský priestor. Potom:

1. $|\alpha \cdot \vec{x}| = |\alpha| \cdot |\vec{x}|$ pre $\forall \alpha \in \mathbb{R}, \forall \vec{x} \in V$.
2. $|\vec{x}| = 0 \Leftrightarrow \vec{x} = \vec{0}$.
3. $|\langle \vec{x}, \vec{y} \rangle| \leq |\vec{x}| |\vec{y}|$. (Cauchyho-Schwarzova-Bunjakovského nerovnosť).
4. $|\vec{x} + \vec{y}| \leq |\vec{x}| + |\vec{y}|$ pre ľubovoľné $\vec{x}, \vec{y} \in V$ (trojuholníková nerovnosť).

Dôkaz.

$$1. |\alpha \vec{x}| = \sqrt{\langle \alpha \vec{x}, \alpha \vec{x} \rangle} = \sqrt{\alpha^2 \langle \vec{x}, \vec{x} \rangle} = |\alpha| \sqrt{\langle \vec{x}, \vec{x} \rangle} = |\alpha| |\vec{x}|.$$

$$2. \text{ Ak } \vec{x} = \vec{0}, \text{ tak } |\vec{x}| = |0 \cdot \vec{x}| = 0 \cdot |\vec{x}| = 0; \text{ ak by } \vec{x} \neq \vec{0}, \text{ tak by sme mali } |\vec{x}| = \sqrt{\langle \vec{x}, \vec{x} \rangle} > 0$$

–spor s predpokladom.

3. $\vec{x}, \vec{y}$ ľubovoľné pevne zvolené. Pre ľubovoľné $\alpha \in \mathbb{R}$ utvorme vektor $\alpha\vec{x} - \vec{y}$. Potom $\langle \alpha\vec{x} - \vec{y}, \alpha\vec{x} - \vec{y} \rangle \geq 0 \Rightarrow \langle \alpha\vec{x}, \alpha\vec{x} \rangle - \langle \vec{y}, \alpha\vec{x} \rangle - \langle \alpha\vec{x}, \vec{y} \rangle + \langle \vec{y}, \vec{y} \rangle = \alpha^2 \langle \vec{x}, \vec{x} \rangle - \alpha \langle \vec{y}, \vec{x} \rangle - \alpha \langle \vec{x}, \vec{y} \rangle + \langle \vec{y}, \vec{y} \rangle = \alpha^2 \langle \vec{x}, \vec{x} \rangle - 2\alpha \langle \vec{x}, \vec{y} \rangle + \langle \vec{y}, \vec{y} \rangle \geq 0$.

Zistili sme, že pre všetky $\alpha \in \mathbb{R}$ je $\langle \vec{x}, \vec{x} \rangle \alpha^2 - 2\alpha \langle \vec{x}, \vec{y} \rangle + \langle \vec{y}, \vec{y} \rangle \geq 0$ kvadratický člen v premennej α . Graf tohto trojčlena leží v nezápornej polrovine ($x_2 \geq 0$) pričom nepretína os x_1 . Teda tento trojčlen nemá dva rôzne reálne korene. Preto diskriminant $D = 4\langle \vec{x}, \vec{y} \rangle^2 - 4\langle \vec{x}, \vec{x} \rangle \cdot \langle \vec{y}, \vec{y} \rangle \leq 0$. Z toho: $4 \cdot \langle \vec{x}, \vec{y} \rangle^2 \leq 4\langle \vec{x}, \vec{x} \rangle \cdot \langle \vec{y}, \vec{y} \rangle$ t.j. $|\langle \vec{x}, \vec{y} \rangle| \leq |\vec{x}| \cdot |\vec{y}|$.
4. $|\vec{x} + \vec{y}|^2 = \langle \vec{x} + \vec{y}, \vec{x} + \vec{y} \rangle = \langle \vec{x}, \vec{x} \rangle + \langle \vec{x}, \vec{y} \rangle + \langle \vec{y}, \vec{x} \rangle + \langle \vec{y}, \vec{y} \rangle = \langle \vec{x}, \vec{x} \rangle + 2\langle \vec{x}, \vec{y} \rangle + \langle \vec{y}, \vec{y} \rangle = |\vec{x}|^2 + 2\langle \vec{x}, \vec{y} \rangle + |\vec{y}|^2 \leq |\vec{x}|^2 + 2|\vec{x}| \cdot |\vec{y}| + |\vec{y}|^2 = (|\vec{x}| + |\vec{y}|)^2$. Z toho $|\vec{x} + \vec{y}| \leq |\vec{x}| + |\vec{y}|$. □

Z 3.vlastnosti z vety 10.1. máme: ak $\vec{x} \neq \vec{0} \neq \vec{y}$, tak $-1 \leq \frac{\langle \vec{x}, \vec{y} \rangle}{|\vec{x}| \cdot |\vec{y}|} \leq 1$.

Definícia 10.3. Ak $(V, \langle \cdot, \cdot \rangle)$ je euklidovský vektorový priestor a $\vec{x}, \vec{y} \in V - \{\vec{0}\}$, tak uhol vektorov $\vec{x}, \vec{y}$ definujeme ako také $\alpha \in \langle 0, \pi \rangle$ pre ktoré $\cos \alpha = \frac{\langle \vec{x}, \vec{y} \rangle}{|\vec{x}| \cdot |\vec{y}|}$. Ak $\vec{x} = \vec{0}$, alebo $\vec{y} = \vec{0}$, tak definujeme uhol vektorov $\vec{x}, \vec{y}$ ako $\frac{\pi}{2}$.

Definícia 10.4. Nech $(V, \langle \cdot, \cdot \rangle)$ je euklidovský vektorový priestor. Hovoríme, že $\vec{x}, \vec{y} \in V$ sú na seba *kolmé*, ak $\angle(\vec{x}, \vec{y}) = \frac{\pi}{2}$. (*ortogonálne*).

Tvrdenie 10.1. Ak $(V, \langle \cdot, \cdot \rangle)$ je euklidovský vektorový priestor, tak $\angle(\vec{x}, \vec{y}) = \frac{\pi}{2} \Leftrightarrow \langle \vec{x}, \vec{y} \rangle = 0$.

Dôkaz. $\angle(\vec{x}, \vec{y}) = \frac{\pi}{2} \Leftrightarrow \vec{x} = \vec{0}$ alebo $\vec{y} = \vec{0}$ alebo $\vec{x}, \vec{y} \in V - \vec{0}$ a $\langle \vec{x}, \vec{y} \rangle = 0$. □

Príklady.

1. Nech $\mathbb{R}^3$ je euklidovský vektorový priestor so štandardným skalárnym súčinom. Potom $\vec{e}_1 = (1, 0, 0)$, $\vec{e}_2 = (0, 1, 0)$, $\vec{e}_3 = (0, 0, 1)$ sú navzájom ortogonálne.

2. V $\mathbb{R}^2$ so štandardným skalárnym súčinom. Na $(a, b) \in \mathbb{R}^2$ je vektor $(-b, a)$ kolmý.

Veta 10.2. Nech $(V, \langle \cdot, \cdot \rangle)$ je euklidovský vektorový priestor a nech vektory $\vec{a}_1, \dots, \vec{a}_n$ sú nenulové a navzájom kolmé vektory. Potom sú aj lineárne nezávislé.

Dôkaz. Nech $\alpha_1 \vec{a}_1 + \dots + \alpha_n \vec{a}_n = \vec{0}$. Chceme ukázať, že $\alpha_1 = \dots = \alpha_n = 0$.
 $\langle \vec{a}_1, \alpha_1 \vec{a}_1 + \dots + \alpha_n \vec{a}_n \rangle = \alpha_1 \underbrace{\langle \vec{a}_1, \vec{a}_1 \rangle}_{>0} + \alpha_2 \underbrace{\langle \vec{a}_1, \vec{a}_2 \rangle}_{=0} + \dots + \alpha_n \underbrace{\langle \vec{a}_1, \vec{a}_n \rangle}_{=0} = 0 = \langle \vec{0}, \vec{a}_1 \rangle \Rightarrow$
 $\Rightarrow \alpha_1 = 0$. Podobne všeobecne $0 = \langle \alpha_1 \vec{a}_1 + \dots + \alpha_n \vec{a}_n, \vec{a}_i \rangle = \alpha_i |\vec{a}_i|^2 \Rightarrow \alpha_i = 0$. □

Dôsledok. Ak $(V, \langle \cdot, \cdot \rangle)$ je n -rozmerný euklidovský vektorový priestor a vektory $\vec{a}_1, \dots, \vec{a}_n \in V - \{\vec{0}\}$ sú navzájom kolmé, tak $(\vec{a}_1, \dots, \vec{a}_n)$ je báza priestoru V .

Definícia 10.5. Ak $(\vec{a}_1, \dots, \vec{a}_n)$ je báza euklidovského vektorového priestoru V taká, že $\vec{a}_i \perp \vec{a}_j$ pre $\forall i \neq j$, tak tá báza sa nazýva *ortogonálna báza*. Ak navyše $|\vec{a}_i| = 1$ pre $i = 1, \dots, n$, tak tá báza sa nazýva *ortonormálna*.

Príklad. $(\vec{e}_1, \vec{e}_2, \vec{e}_3)$ je ortogonálna a ortonormálna báza euklidovského vektorového priestoru $(\mathbb{R}^3, \langle \cdot, \cdot \rangle)$.

Veta 10.3. Nech $(V, \langle \cdot, \cdot \rangle)$ je ľubovoľný euklidovský vektorový priestor a nech S je ľubovoľný jeho vektorový podpriestor (nenulový). Ak V je konečne generovaný, tak v S existuje ortonormálna báza.

Dôkaz. Nech $\dim(V) = n$, nech $(\vec{x}_1, \dots, \vec{x}_k)$ ($k \leq n$) je dajaká báza v S . Veta bude dokázaná, ak dokážeme, že existujú nenulové vektory $\vec{y}_1, \dots, \vec{y}_k \in S$ také, že pre ne

platí: $\vec{y}_1 = \vec{x}_1$, $\vec{y}_2 = \vec{x}_2 + \beta_{21}\vec{x}_1$, $\vec{y}_3 = \vec{x}_3 + \beta_{31}\vec{x}_1 + \beta_{32}\vec{x}_2, \dots, \vec{y}_k = \vec{x}_k + \beta_{k1}\vec{x}_1 + \dots + \beta_{kk-1}\vec{x}_{k-1}$, pričom $\vec{y}_i \perp \vec{y}_j$ pre $i \neq j$. Je jasné, že potom $\vec{y}_1, \dots, \vec{y}_k$ sú v S sú lineárne nezávislé. Keďže $\dim(S)=k$, tak $(\vec{y}_1, \dots, \vec{y}_k)$ je báza, a je ortogonálna.

Potom ortonormálna báza v S bude takáto: $\left(\frac{\vec{y}_1}{|\vec{y}_1|}, \dots, \frac{\vec{y}_k}{|\vec{y}_k|}\right)$.

$\left\langle \frac{\vec{y}_i}{|\vec{y}_i|}, \frac{\vec{y}_j}{|\vec{y}_j|} \right\rangle = \frac{1}{|\vec{y}_i||\vec{y}_j|} \cdot \langle \vec{y}_i, \vec{y}_j \rangle = 0$. Existenciu vektorov $\vec{y}_i$ dokážeme indukciou:

Ak $k=1$: S má bázu $(\vec{x}_1)$, ortonormálna bude: $\left(\frac{\vec{x}_1}{|\vec{x}_1|}\right)$. Predpokladajme, že veta

platí pre $k=s-1$. A teraz nech S má bázu $(\vec{x}_1, \dots, \vec{x}_s)$. Teda máme systém $\vec{y}_1 = \vec{x}_1, \dots, \vec{y}_{s-1} = \vec{x}_{s-1} + \dots + \beta_{s-1,s-2}\vec{x}_{s-2}$. Podľa indukčného predpokladu máme vektory $\vec{y}_1, \dots, \vec{y}_{s-1}$ potrebného tvaru. Treba už len ukázať, ako vyrátať vektor $\vec{y}_s \neq \vec{0}$ potrebného tvaru a taký, že $\langle \vec{y}_s, \vec{y}_i \rangle = 0$ pre všetky $i \leq s-1$. Hľadáme $\vec{y}_s$ v tvare: $\vec{y}_s = \vec{x}_s + \delta_{s1}\vec{y}_1 + \dots + \delta_{ss-1}\vec{y}_{s-1}$. Má byť: $0 = \langle \vec{y}_s, \vec{y}_1 \rangle = \langle \vec{x}_s, \vec{x}_1 \rangle + \delta_{s1}\langle \vec{x}_1, \vec{x}_1 \rangle + \delta_{s2}\underbrace{\langle \vec{y}_2, \vec{x}_1 \rangle}_{=0} + \dots + \delta_{ss-1}\underbrace{\langle \vec{y}_{s-1}, \vec{x}_1 \rangle}_{=0} \Rightarrow \langle \vec{x}_s, \vec{x}_1 \rangle + \delta_{s1}\langle \vec{x}_1, \vec{x}_1 \rangle = 0 \Rightarrow \delta_{s1} = -\frac{\langle \vec{x}_s, \vec{x}_1 \rangle}{\langle \vec{x}_1, \vec{x}_1 \rangle}$.

Z toho, že $\langle \vec{y}_s, \vec{y}_2 \rangle = 0$ vyrátame δ_{s2} atď.

□

Poznámka. Metóda dôkazu je konštruktívna; ukazuje indukčný postup na hľadanie ortogonálnej, ortonormálnej bázy. Je to tzv. *Gramov – Schmidtov* ortogonalizačný proces.

Príklad. Nech S je podpriestor v $\mathbb{R}^4$ so štandardným skalárnym súčinom. Treba nájsť ortonormálnu bázu podpriestoru S .

$S = [\vec{x}_1, \vec{x}_2, \vec{x}_3] = [(1, -1, 0, -1), (0, 1, 0, 2), (0, 0, 1, -2)]$. Najskôr ortogonálnu bázu: $\vec{y}_1 = \vec{x}_1 = (1, -1, 0, -1)$, $\vec{y}_2 = \vec{x}_2 + \alpha\vec{y}_1$; $\langle \vec{y}_1, \vec{y}_2 \rangle = 0 \Rightarrow \alpha = 1$, $\vec{y}_2 = (1, 0, 0, 1)$; $\vec{y}_3 = (0, 0, 1, 2) + \delta_1(1, -1, 0, -1) + \delta_2(1, 0, 0, 1)$. Potom: $\langle \vec{y}_3, \vec{y}_1 \rangle = 0 \wedge \langle \vec{y}_2, \vec{y}_1 \rangle = 0 \Rightarrow 0 = \langle (\delta_1 + \delta_2, -\delta_1, 1, 2 - \delta_1 + \delta_2), (1, -1, 0, -1) \rangle = \delta_1 + \delta_2 + \delta_1 + 2 + \delta_1 - \delta_2 = 0 \dots \Rightarrow \Rightarrow \delta_1 = -\frac{2}{3}$, $\delta_2 = 1 \Rightarrow \vec{y}_3 = (0, 0, 1, 2) - \frac{2}{3}(1, -1, 0, -1) + (1, 0, 0, 1) = (\frac{1}{3}, \frac{2}{3}, 1, -\frac{1}{3})$.

Ortonormálna báza: $\left(\left(\frac{1}{\sqrt{3}}, -\frac{1}{\sqrt{3}}, 0, -\frac{1}{\sqrt{3}}\right), \left(\frac{1}{\sqrt{2}}, 0, 0, \frac{1}{\sqrt{2}}\right), \frac{\sqrt{3}}{\sqrt{5}}\left(\frac{1}{3}, \frac{2}{3}, 1, -\frac{1}{3}\right)\right)$.

Definícia 10.6. Nech $(V, \langle \cdot, \cdot \rangle)$ je euklidovský vektorový priestor a nech $M \subset V$, $M \neq \emptyset$. (M nemusí byť podpriestor). Potom *ortogonálny doplnok* (komplement) množiny M vo V je množina $M^\perp := \{\vec{x} \in V; \langle \vec{x}, \vec{m} \rangle = 0 \forall \vec{m} \in M\}$

Veta 10.4. Nech $(V, \langle \cdot, \cdot \rangle)$ je euklidovský vektorový priestor. Potom:

1. $M \neq \emptyset$, $M \subset V \Rightarrow M^\perp$ je vektorový podpriestor priestoru V .
2. Ak $M, N \neq \emptyset$, $M, N \subset V$ a $M \subset N$ tak $N^\perp \subset M^\perp$.
3. Ak S, T sú vektorové podpriestory vo V , tak $(S+T)^\perp = S^\perp \cap T^\perp$.

Dôkaz.

1. $M^\perp \neq \emptyset$, lebo $\vec{0} \in M^\perp$. Kritérium vektorového podpriestoru: pre $\forall \vec{x}, \vec{y} \in M^\perp$, $\forall \alpha, \beta \in \mathbb{R}$. Potom pre ľubovoľné $\vec{m} \in M$: $\langle \alpha\vec{x} + \beta\vec{y}, \vec{m} \rangle = \underbrace{\alpha\langle \vec{x}, \vec{m} \rangle}_{=0} + \underbrace{\beta\langle \vec{y}, \vec{m} \rangle}_{=0} = 0$. Teda

$\alpha\vec{x} + \beta\vec{y} \in M^\perp$. Z toho $M^\perp$ je vektorový podpriestor vo V .

2. $M \subset N$. Ak $\vec{x} \in N^\perp$, tak $\langle \vec{x}, \vec{n} \rangle = 0$ pre všetky $\vec{n} \in N$ a teda tiež $\langle \vec{x}, \vec{m} \rangle = 0$ pre všetky $\vec{m} \in M$. Teda $\vec{x} \in M^\perp$.

3. Nech $\vec{x} \in (S+T)^\perp$. Teda $\langle \vec{x}, \vec{s} + \vec{t} \rangle = 0$ pre všetky $\vec{s} \in S, \vec{t} \in T$. Špeciálne $\langle \vec{x}, \vec{s} + \vec{0} \rangle = \langle \vec{x}, \vec{0} \rangle = 0$ pre ľubovoľný $\vec{s} \in S$. Takisto $\langle \vec{x}, \vec{t} \rangle = 0$ pre $\forall \vec{t} \in T$. To znamená, že $\vec{x} \in S^\perp \cap T^\perp$. Teda máme: $(S+T)^\perp \subset S^\perp \cap T^\perp$.

Obrátene: nech $\vec{x} \in S^\perp \cap T^\perp$. Potom $\langle \vec{x}, \vec{s} \rangle = 0$ pre všetky $\vec{s} \in S$; $\langle \vec{x}, \vec{t} \rangle = 0$ pre všetky $\vec{t} \in T$; potom $\langle \vec{x}, \vec{s} + \vec{t} \rangle = 0$ pre všetky $\vec{s} \in S, \vec{t} \in T$. Teda $\vec{x} \in (S+T)^\perp$

t.j. $S^\perp \cap T^\perp \subset (S+T)^\perp$. Vcelku: $S^\perp \cap T^\perp = (S+T)^\perp$.

□

Veta 10.5. *Nech $(V, \langle \cdot, \cdot \rangle)$ je euklidovský vektorový priestor, nech $S \subset V$ je vektorový podpriestor. (V je konečne generovaný). Potom každý vektor $z \in V$ sa dá jedínym spôsobom vyjadriť ako súčet vektora $z \in S$ a vektora $z \in S^\perp$. To znamená, že $V = S \oplus S^\perp$.*

Dôkaz.

Existencia vyjadrenia: Pre $S = \{\vec{0}\}$ jasné. Predpokladajme, že $S \neq \{\vec{0}\}$. Nech $(\vec{a}_1, \dots, \vec{a}_k)$ je ortonormálna báza v S (taká existuje – proces Gramov-Schmidtov). Doplňme ju na bázu $(\vec{a}_1, \dots, \vec{a}_k, \vec{b}_{k+1}, \dots, \vec{b}_n)$ priestoru V . Gramovým-Schmidtovým procesom prejdeme k ortonormálnej báze $(\underbrace{\vec{a}_1, \dots, \vec{a}_k}_{\in S}, \underbrace{\vec{a}_{k+1}, \dots, \vec{a}_n}_{\in S^\perp})$ priestoru

V . Potom ľubovoľný vektor $\vec{x} \in V$ má jediné vyjadrenie v tvare:

$$\vec{x} = \underbrace{x_1 \vec{a}_1 + \dots + x_k \vec{a}_k}_{\in S} + \underbrace{x_{k+1} \vec{a}_{k+1} + \dots + x_n \vec{a}_n}_{\in S^\perp}. \text{ Označme } x_1 \vec{a}_1 + \dots + x_k \vec{a}_k = \vec{x}_S,$$

$$x_{k+1} \vec{a}_{k+1} + \dots + x_n \vec{a}_n = \vec{x}_{S^\perp}. \text{ Máme } \vec{x} = \vec{x}_S + \vec{x}_{S^\perp}.$$

Jednoznačnosť vyjadrenia: Nech by tiež $\vec{x} = \vec{a} + \vec{b}$, pričom $\vec{a} \in S, \vec{b} \in S^\perp$. Chceme ukázať, že $\vec{a} = \vec{x}_S$ a $\vec{b} = \vec{x}_{S^\perp}$. Máme $\vec{x}_S + \vec{x}_{S^\perp} = \vec{a} + \vec{b}$, z čoho $\underbrace{\vec{x}_S - \vec{a}}_{\in S} = \underbrace{\vec{b} - \vec{x}_{S^\perp}}_{\in S^\perp}$. Rátajme:

$$0 \leq \langle \vec{x}_S - \vec{a}, \vec{b} - \vec{x}_{S^\perp} \rangle = \underbrace{\langle \vec{x}_S, \vec{b} \rangle}_{=0} - \underbrace{\langle \vec{a}, \vec{b} \rangle}_{=0} - \underbrace{\langle \vec{x}_S, \vec{x}_{S^\perp} \rangle}_{=0} + \underbrace{\langle \vec{a}, \vec{x}_{S^\perp} \rangle}_{=0}. \text{ Teda } 0 = \langle \vec{x}_S - \vec{a},$$

$$\vec{b} - \vec{x}_{S^\perp} \rangle = \langle \vec{x}_S - \vec{a}, \vec{x}_S - \vec{a} \rangle = \langle \vec{b} - \vec{x}_{S^\perp}, \vec{b} - \vec{x}_{S^\perp} \rangle. \text{ Potom } \vec{x}_S - \vec{a} = \vec{0} \wedge \vec{b} - \vec{x}_{S^\perp} = \vec{0} \Rightarrow \vec{x}_S = \vec{a} \wedge \vec{b} = \vec{x}_{S^\perp}.$$

□

Veta 10.6. *Nech $(V, \langle \cdot, \cdot \rangle)$ je konečne generovaný euklidovský vektorový priestor. Potom:*

1. Ak $S \subset V$ je vektorový podpriestor, tak $(S^\perp)^\perp = S$.
2. Ak $S, T \subset V$ sú vektorové podpriestory, tak $(S \cap T)^\perp = S^\perp + T^\perp$.

Dôkaz.

1. Pre ľubovoľné $\vec{x} \in S$ máme $\langle \vec{x}, \vec{y} \rangle = 0$ pre ľubovoľný $\vec{y} \in S^\perp$. Teda $\vec{x} \in (S^\perp)^\perp$. Zistili sme, že $S \subset (S^\perp)^\perp$. Z vety 8.24. vieme, že $V = S \oplus S^\perp$ a $V = (S^\perp) \oplus (S^\perp)^\perp$. Z toho: $\dim(V) = \dim(S) + \dim(S^\perp) = \dim(S^\perp) + \dim((S^\perp)^\perp)$. Teda $\dim(S) = \dim((S^\perp)^\perp)$. Keďže aj $S \subset ((S^\perp)^\perp)$, máme $S = (S^\perp)^\perp$.
2. $((S^\perp + T^\perp)^\perp)^\perp = (S^\perp + T^\perp) = ((S^\perp)^\perp \cap (T^\perp)^\perp)^\perp = (S \cap T)^\perp$.

□

Definícia 10.7. Nech $(V, \langle \cdot, \cdot \rangle)$ je euklidovský vektorový priestor a $\{\vec{0}\} \neq S \subset V$ je vektorový podpriestor. Potom každý vektor $\vec{x} \in V$ má jediné vyjadrenie v tvare $\vec{x} = \vec{x}_S + \vec{x}_{S^\perp}$, kde $\vec{x}_S \in S$ a $\vec{x}_{S^\perp} \in S^\perp$. Teda predpis, ktorý každému $\vec{x} \in V$ priradí $\vec{x}_S$ definuje zobrazenie $p: V \rightarrow V, p(\vec{x}) = \vec{x}_S$. Potom p sa nazýva *zobrazenie ortogonálnej projekcie* na podpriestor S .

Tvrdenie 10.3. Ak $\vec{x} \in S$, tak $p(\vec{x}) = \vec{x}$.

Dôkaz. Jediné také vyjadrenie je: $\vec{x} = \underbrace{\vec{x}}_{\in S} + \underbrace{\vec{0}}_{\in S^\perp}$. Teda $p(\vec{x}) = \vec{x}$.

□

Tvrdenie 10.4. $p(V) = S$.

Tvrdenie 10.5. $p \circ p = p$.

Dôkaz. Pre ľubovoľný $\vec{x} \in S$: $p \circ p(\vec{x}) = p(\underbrace{p(\vec{x})}_{\in S}) = p(\vec{x})$.

□

Tvrdenie 10.6. $p : V \rightarrow V$ je lineárne zobrazenie.

Dôkaz. Ľubovoľné $\vec{x}, \vec{y} \in V$, $\alpha, \beta \in \mathbb{R}$. Potom vieme, že $\vec{x} = \vec{x}_S + \vec{x}_{S^\perp}$ a $\vec{y} = \vec{y}_S + \vec{y}_{S^\perp}$ sú jediné vyjadrenia svojho druhu. Potom $\alpha\vec{x} + \beta\vec{y} = \underbrace{\alpha(\vec{x}_S + \vec{y}_S)}_{\in S} + \underbrace{\beta(\vec{x}_{S^\perp} + \vec{y}_{S^\perp})}_{\in S^\perp}$ je jediné

vyjadrenie vektora $\alpha\vec{x} + \beta\vec{y}$ ako súčet vektora z S a vektora z $S^\perp$. Podľa definície 8.24.: $p(\alpha\vec{x} + \beta\vec{y}) = \alpha(\vec{x}_S + \vec{y}_S) = \alpha\vec{x}_S + \beta\vec{y}_S = \alpha p(\vec{x}) + \beta p(\vec{y})$. $\square$

Príklad. Treba nájsť zobrazenie ortogonálnej projekcie na podpriestor S .

$S = [(1, 1, -1), (1, -1, 0)] \subset \mathbb{R}^3$ so štandardným skalárnym súčinom. Doplníme ortogonálnu bázu $((1, 1, -1), (1, -1, 0))$ podpriestoru S na ortogonálnu bázu priestoru $\mathbb{R}^3$. Nájdeme vektor $(k_1, k_2, k_3) \in \mathbb{R}^3$ taký, že $\langle (k_1, k_2, k_3), (1, 1, -1) \rangle = 0$ a tiež:

$\langle (k_1, k_2, k_3), (1, -1, 0) \rangle = 0$. Z toho: $k_1 + k_2 - k_3 = 0$ a $k_1 - k_2 = 0$. Vyriešime, zoberieme napríklad $(-1, -1, -2)$. Teda $\underbrace{((1, 1, -1), (1, -1, 0))}_{\in S}, \underbrace{(-1, -1, -2)}_{\in S^\perp}$ je ortogonálna

báza v $\mathbb{R}^3$.

$$\mathbb{R}^3 \ni (x_1, x_2, x_3) = \underbrace{a(1, 1, -1) + b(1, -1, 0)}_{\in S} + \underbrace{c(-1, -1, -2)}_{\in S^\perp} \Rightarrow \begin{cases} a + b - c = x_1 \\ a - b - c = x_2 \\ -a - 2c = x_3 \end{cases}$$

Vyriešime: $c = -\frac{1}{6}(x_1 + x_2 + 2x_3)$, $b = -\frac{1}{2}(x_1 - x_2)$, $a = \frac{1}{3}(x_1 + x_2 - x_3)$. Teda pre ľubovoľný $(x_1, x_2, x_3) \in \mathbb{R}^3$ platí:

$$(x_1, x_2, x_3) = \underbrace{\frac{x_1 + x_2 - x_3}{3} \cdot (1, 1, -1) + \frac{x_1 - x_2}{2} \cdot (1, -1, 0)}_{\in S} - \underbrace{\frac{x_1 + x_2 + 2x_3}{6} \cdot (-1, -1, -2)}_{\in S^\perp}$$

Teda $p(x_1, x_2, x_3) = \frac{x_1 + x_2 - x_3}{3} \cdot (1, 1, -1) + \frac{x_1 - x_2}{2} \cdot (1, -1, 0)$;

$p(x_1, x_2, x_3) = (\frac{5x_1 - x_2 - 2x_3}{6}; \frac{-x_1 + 5x_2 - 2x_3}{6}; \frac{-x_1 - x_2 + x_3}{3})$. Matica zobrazenia p :

$$\mathbf{M}_p = \begin{pmatrix} \frac{5}{6} & -\frac{1}{6} & -\frac{1}{3} \\ -\frac{1}{6} & \frac{5}{6} & -\frac{1}{3} \\ -\frac{1}{3} & -\frac{1}{3} & \frac{1}{3} \end{pmatrix} \quad \mathbf{M}_p \text{ je symetrická. Súčet na diagonále: } \dim(S).$$

Definícia 10.8. Nech $(V, \langle \cdot, \cdot \rangle)$ a $(W, \langle \cdot, \cdot \rangle)$ sú euklidovské vektorové priestory. Euklidovský izomorfizmus z V na W je lineárny izomorfizmus $f : V \rightarrow W$ taký, že $\langle f(\vec{x}), f(\vec{y}) \rangle = \langle \vec{x}, \vec{y} \rangle$ pre všetky $\vec{x}, \vec{y} \in V$.

Veta 10.7. Nech $(V, \langle \cdot, \cdot \rangle)$ je n -rozmerný euklidovský vektorový priestor. Potom existuje euklidovský izomorfizmus z V na $\mathbb{R}^n$ so štandardným skalárnym súčinom.

Dôkaz. Nech $(\vec{v}_1, \dots, \vec{v}_n)$ je nejaká ortonormálna báza vo V . Nech $(\vec{e}_1, \dots, \vec{e}_n)$ je štandardná báza v $\mathbb{R}^n$ (tá je tiež ortonormálna). Zo základnej vety o lineárnych zobrazeniach vieme, že existuje jediné lineárne zobrazenie $f : V \rightarrow \mathbb{R}^n$ také, že $f(\vec{v}_i) = \vec{e}_i$, $i = 1, \dots, n$. Z inej vety vieme, že f je lineárny izomorfizmus. f je aj euklidovský izomorfizmus, lebo: $\langle f(x_1\vec{v}_1 + \dots + x_n\vec{v}_n), f(y_1\vec{v}_1 + \dots + y_n\vec{v}_n) \rangle = \langle x_1f(\vec{v}_1) + \dots + x_nf(\vec{v}_n), y_1f(\vec{v}_1) + \dots + y_nf(\vec{v}_n) \rangle = \langle x_1\vec{e}_1 + \dots + x_n\vec{e}_n, y_1\vec{e}_1 + \dots + y_n\vec{e}_n \rangle = x_1y_1 + \dots + x_ny_n$. Ale aj $\langle x_1\vec{v}_1 + \dots + x_n\vec{v}_n, y_1\vec{v}_1 + \dots + y_n\vec{v}_n \rangle = x_1y_1 + \dots + x_ny_n$. $\square$

Príklad. $\mathbb{R}^n$, euklidovský izomorfizmus: $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ je napr. $f_A : \mathbb{R}^n \rightarrow \mathbb{R}^n$, kde $\mathbf{A} \in \mathfrak{M}_{nn}(\mathbb{R})$ a $\mathbf{A}\mathbf{A}^T = \mathbf{I}_n$.