Algebra a jej vety II.

Prírodovedecká fakulta UPJŠ Košice

Predmety: KGA/ALG1b, KGA/ALG1c **Prednáša:** doc. RNDr. Judita Lihová, CSc.
Obsah: Definície, vety, lemy a poznámky k predmetom
ZTEXovali: Róbert Novotný & Petra Murtinová. **Vydané:** 24.1.2002.

1 Vektorové priestory

1.1 Vektorové priestory nad poľom

Definícia 1.1.1
Vektorový priestor nad poľom $\mathbb{F}$ je množina V, na ktorej je definované sčitovanie prvkov z množiny V a násobenie prvkov z množiny V prvkami z poľa $\mathbb{F}$ tak, že platia nasledovné zákony:

1. $\forall a, b \in \mathsf{V} : a + b \in \mathsf{V}$
2. $\forall \alpha \in \mathbb{F}, a \in \mathsf{V} : \alpha \,.\, a \in \mathsf{V}$
3. $\forall a, b \in \mathsf{V} : a + b = b + a$
4. $\forall a, b, c \in \mathsf{V} : a + (b + c) = (a + b) + c$
5. $\exists \mathbf{o} \in \mathsf{V} : \forall\, a \in \mathsf{V} : a + \mathbf{o} = a$
6. $\forall a \in \mathsf{V}\, \exists\, b \in \mathsf{V} : a + b = \mathbf{o}$
7. $\forall \alpha \in \mathbb{F} : a, b \in \mathsf{V} : \alpha \,.\, (a + b) = \alpha \,.\, a + \alpha \,.\, b$
8. $\forall \alpha, \beta \in \mathbb{F}, a \in \mathsf{V} : (\alpha + \beta) \,.\, a = \alpha \,.\, a + \beta \,.\, a$
9. $\forall \alpha, \beta \in \mathbb{F}, a \in \mathsf{V} : (\alpha \,.\, \beta) \,.\, a = \alpha \,.\, (\beta \,.\, a)$
10. $\forall a \in \mathsf{V} : 1 \,.\, a = a$

Poznámka 1.1.2
Prvky z V nazývame vektory, prvky z $\mathbb{F}$ skaláre.

Dôsledok 1.1.3

1. *vo vektorovom priestore možno sčitovať ľubovoľný konečný počet vektorov, pričom nezáleží na uzátvorkovaní a poradí*
2. *jednoznačnosť nulového vektora* $\boldsymbol{o}$
3. *zákon krátenia pre sčitovanie*
4. *jednoznačnosť opačného vektora* $-a$
5. $\forall \alpha \in \mathbb{F}, a \in \mathsf{V} : \alpha \,.\, a = 0 \Leftrightarrow \alpha = 0 \vee a = \boldsymbol{o}$
6. $\forall a \in \mathsf{V} : (-1) \,.\, a = -a$
7. $\forall \alpha \in \mathbb{F}, a \in \mathsf{V} : -(\alpha \,.\, a) = (-\alpha) \,.\, a = \alpha \,.\, (-a)$

1.2 Podpriestory

Definícia 1.2.1
Nech $\mathbf{V}$ je vektorový priestor nad poľom $\mathbb{F}$. Pod ***podpriestorom*** tohto vektorového priestoru rozumieme takú neprázdnu podmnožinu $\mathbf{S}$ množiny $\mathbf{V}$, ktorá spĺňa nasledovné podmienky:

1. $a, b \in \mathbf{S} \Rightarrow a + b \in \mathbf{S}$ ($\mathbf{S}$ je uzavretá vzhľadom na sčítanie)
2. $\alpha \in F, a \in \mathbf{S} \Rightarrow \alpha \,.\, a \in \mathbf{S}$ ($\mathbf{S}$ je uzavretá vzhľadom na násobenie skalármi)

Príklad 1.2.2

1. Ak $\mathbf{V}$ je ľubovoľný vektorový priestor nad poľom $\mathbb{F}$, tak $\{\mathbf{o}\}$ a samotný $\mathbf{V}$ je podpriestorom vektorového priestoru $\mathbf{V}$.
2. $\mathbf{V}_2(\mathbb{F}), \mathbf{S} = \{(\alpha, 0) : \alpha \in \mathbb{F}\}$. $\mathbf{V}_1(\mathbb{F})$ nie je podpriestorom $\mathbf{V}_2(\mathbb{F})$

Veta 1.2.3
Nech $\mathbf{W}$ je podpriestor vektorového priestoru $\mathbf{V}(\mathbb{F})$. Potom $\mathbf{W}$ je vektorový priestor nad $\mathbb{F}$ (vzhľadom na operácie $+, .$ s prvkami $\mathbb{F}$ vo $\mathbf{V}$).

Veta 1.2.4
Prienik ľubovoľného neprázdneho systému podpriestorov vektorového priestoru $\mathbf{V}$ nad $\mathbb{F}$ je podpriestorom vektorového priestoru $\mathbf{V}$.

Dôsledok 1.2.5
Nech $\mathbf{V}$ je ľubovoľný vektorový priestor nad $\mathbb{F}$ a nech $\mathbf{M}$ je ľubovoľná podmnožina $\mathbf{V}$. Potom v systéme podpriestorov vektorového priestoru $\mathbf{V}$ obsahujúcich množinu $\mathbf{M}$ existuje najmenší (je podmnožinou každého podpriestoru).

Značenie: $[\mathbf{M}]$

$[\mathbf{M}]$ *je najmenší podpriestor vektorového priestoru $\mathbf{V}$ obsahujúci množinu M, resp. podpriestor generovaný množinou $\mathbf{M}$.*

Definícia 1.2.6
Nech $\mathbf{V}$ je vektorový priestor nad $\mathbb{F}$. Nech $a_1, \ldots, a_n \in \mathbf{V}$ je konečný počet vektorov. ***Lineárna kombinácia*** týchto vektorov je každý vektor tvaru

$$\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_n a_n, \quad \alpha_1, \ldots, \alpha_n \in \mathbb{F}$$

Veta 1.2.7
Nech $\mathbf{V}$ je vektorový priestor nad $\mathbb{F}$ a nech $\mathbf{M} \subseteq \mathbf{V}$.

1. *ak $\mathbf{M} = \emptyset$, tak $[\mathbf{M}] = \{\boldsymbol{o}\}$*
2. *ak $\mathbf{M} = \{a_1, \ldots, a_n\}$ je konečná množina, tak $[\mathbf{M}] = \{\alpha_1 a_1 + \ldots + \alpha_n a_n : \alpha_1, \ldots, \alpha_n \in \mathbb{F}\}$*
3. *ak $\mathbf{M}$ je nekonečná, tak $[\mathbf{M}] = \bigcup\limits_{\mathbf{K} \text{ cez } \forall \text{ konečné podmnožiny } \mathbf{M}} [\mathbf{K}]$*

Poznámka 1.2.8
$[\mathbf{M}]$ sa nazýva ***lineárny obal*** množiny $\mathbf{M}$, resp. ***obálka*** množiny $\mathbf{M}$.

Veta 1.2.9
Nech $\mathbf{W}_1, \mathbf{W}_2$ sú podpriestory $\mathbf{V}$ nad $\mathbb{F}$. Potom najmenší podpriestor $\mathbf{W}$ obsahujúci podpriestory $\mathbf{W}_1, \mathbf{W}_2$ pozostáva zo súčtov $a + b, a \in \mathbf{W}_2, b \in \mathbf{W}_2$

$$[\mathbf{W}_1 \cup \mathbf{W}_2] = \{a + b : a \in \mathbf{W}_1, b \in \mathbf{W}_2\}$$

Definícia 1.2.10
Lineárnym súčtom podpriestorov $\mathbf{W}_1, \mathbf{W}_2$ vektorového priestoru $\mathbf{V}$ nazývame $[\mathbf{W}_1 \cup \mathbf{W}_2]$

Značenie: $\mathbf{W}_1 + \mathbf{W}_2$

1.3 Lineárna nezávislosť

Definícia 1.3.1
Lineárnu kombináciu $0a_1 + \ldots + 0a_n$ nazývame ***triviálnou*** lineárnou kombináciou. ***Netriviálna*** lineárna kombinácia je každá lineárna kombinácia vektorov $a_1, \ldots, \alpha_n$, ktorá nie je triviálna. T.j. $\alpha_1 a_1 + \ldots + \alpha_n a_n$ taká, že aspoň jeden z koeficientov $\alpha_1, \ldots, \alpha_n$ je rôzny od 0.

Definícia 1.3.2
Vektory $a_1, \ldots, a_n$ tvoria ***lineárne nezávislý systém***, ak existuje taká netriviálna lineárna kombinácia týchto vektorov, ktorá sa rovná $\mathbf{o}$.

Dôsledok 1.3.3
1.) Systém pozostávajúci z jedného vektora a je lineárne závislý práve vtedy, ak $a = \boldsymbol{o}$.
2.) Ak $n > 1$, tak systém pozostávajúci z n vektorov $a_1, \ldots, a_n$ je lineárne závislý práve vtedy, ak niektorý z týchto vektorov je lineárnou kombináciou ostatných.

Definícia 1.3.4
Nekonečný systém S vektorov vo vektorovom priestore V nazývame ***lineárne závislý***, ak obsahuje konečný lineárne závislý podsystém.

Veta 1.3.5
Nadsystém lineárne závislého systému je lineárne závislý.

Veta 1.3.6
Vo vektorovom priestore $\mathsf{V}_n(\mathbb{F})$ je každý systém pozostávajúci z viac ako n vektorov lineárne závislý.

Definícia 1.3.7
Systém $\emptyset \neq \mathsf{S} \subseteq \mathsf{V}$ nazývame ***lineárne nezávislým***, ak nie je lineárne závislý.

Poznámka 1.3.8
Podsystém ľubovoľného nezávislého systému je nezávislý.

Veta 1.3.9
Nech $a_1, \ldots, a_r$ tvoria lineárne nezávislý systém vo vektorovom priestore V a nech

$$\{a_1, \ldots\, a_r\} \subseteq [\{b_1, \ldots, b_s\}].$$

Potom $r \leq s$.

1.4 Báza vektorového priestoru

Definícia 1.4.1
Bázou vektorového priestoru V nazývame taký systém S vektorov vo V, pre ktoré sú splnené nasledovné podmienky:

1. S je lineárne nezávislý
2. S generuje celý priestor V (t.j. $\mathsf{V} = [\mathsf{S}]$)

Veta 1.4.2
Nech $a_1, \ldots, a_n \in \mathsf{V}$. Potom $a_1, \ldots, a_n$ tvoria bázu V práve vtedy, keď každý vektor z V možno vyjadriť ako lineárnu kombináciu vektorov $a_1, \ldots, a_n$ a to jednoznačne.

Definícia 1.4.3
Ak vektory $v_1, \ldots, v_n$ tvoria bázu V a pre $a \in \mathsf{V} : a = \alpha_1 v_1 + \ldots + \alpha_n v_n$. Koeficienty $\alpha_1, \ldots, \alpha_n$ sa nazývajú ***súradnice vektora*** v vzhľadom k danej báze.

Definícia 1.4.4
Vektorový priestor $\mathbf{V}$ nad $\mathbb{F}$ nazývame ***konečnorozmerný***, ak existuje taká konečná množina vektorov vo $\mathbf{V}$, ktorá generuje $\mathbf{V}$. Inak $\mathbf{V}$ nazývame ***nekonečnorozmerný***.

Lemma 1.4.5
Nech $a_1, \dots, a_n \in \mathbf{V}$. Ak k nim pridáme vektor, ktorý je ich lineárnou kombináciou, potom platí:

$$[\{a_1, \dots, a_n, \alpha_1 a_1 + \ldots + \alpha_n a_n\}] = [\{a_1, \dots, a_n\}]$$

Veta 1.4.6
Každý nenulový konečnorozmerný vektorový priestor má konečnú bázu.

Veta 1.4.7
Ak vo vektorovom priestore $\mathbf{V}$ nad $\mathbb{F}$ existuje n-prvková báza ($n \in \mathbb{N}$), tak každá báza tohto priestoru obsahuje n prvkov.

Definícia 1.4.8
Nech $\mathbf{V}$ je konečnorozmerný vektorový priestor. Ak $\mathbf{V} = \{\mathbf{o}\}$, tak $\mathbf{V}$ má dimenziu 0. Ak $\mathbf{V} \neq \{\mathbf{o}\}$, tak jeho ***dimenzia*** je definovaná ako počet vektorov ľubovoľnej bázy.

Označenie: $\dim \mathbf{V}$

Poznámka 1.4.9
Ak $\dim \mathbf{V} = n (\in \mathbb{N}_0)$, tak každý systém vo $\mathbf{V}$ obsahujúci viac ako n vektorov je lineárne závislý.

Dôsledok 1.4.10
Vektorový priestor $\mathbf{V}_\infty(\mathbb{F})$ obsahujúci všetky skoro nulové postupnosti je nekonečnorozmerný.

Veta 1.4.11
V konečnorozmernom vektorovom priestore možno každý lineárne nezávislý systém rozšíriť na bázu.

Veta 1.4.12
Nech $\mathbf{V}$ je konečnorozmerný vektorový priestor dimenzie $n > 0$ a nech $a_1, \dots, a_n \in \mathbf{V}$. Potom sú ekvivalentné nasledovné podmienky:

1. *$a_1, \dots, a_n$ tvoria bázu*
2. *$a_1, \dots, a_n$ tvoria lineárne nezávislý systém*
3. *$[\{a_1, \dots, a_n\}] = \mathbf{V}$ (vektory $a_1, \dots, a_n$ generujú celý $\mathbf{V}$)*

1.5 Dimenzia lineárneho súčtu podpriestorov

Veta 1.5.1
Nech $\mathbf{V}$ je konečnorozmerný vektorový priestor nad $\mathbb{F}$, a nech $\mathbf{W}_1$, $\mathbf{W}_2$ sú jeho podpriestory. Potom

$$\dim(\mathbf{W}_1 + \mathbf{W}_2) = \dim \mathbf{W}_1 + \dim \mathbf{W}_2 - \dim(\mathbf{W}_1 \cap \mathbf{W}_2)$$

1.6 Izomorfizmus

Definícia 1.6.1
Nech $\mathbf{V}_1, \mathbf{V}_2$ sú vektorové priestory nad $\mathbb{F}$. Zobrazenie

$$\varphi : \mathbf{V}_1 \to \mathbf{V}_2$$

nazývame ***homomorfizmom*** (lineárnym zobrazením), ak spĺňa nasledovné podmienky:

1. $\forall a_1, a_2 \in \mathbf{V}_1 : \varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2)$
2. $\forall a \in \mathbf{V}_1, \lambda \in \mathbb{F} : \varphi(\lambda a) = \lambda\varphi(a)$

Dôsledok 1.6.2
Majme vektorové priestory $\mathbf{V}_1, \mathbf{V}_2$ nad $\mathbb{F}$ a majme $\varphi : \mathbf{V}_1 \to \mathbf{V}_2$. Potom φ je homomorfizmus práve vtedy, keď:

$$\forall n \in \mathbb{N}, \forall a_1, \ldots, a_n \in \mathbb{F} : \varphi(\alpha_1 a_1 + \ldots + \alpha_n a_n) = \alpha_1\varphi(a_1) + \ldots + \alpha_n\varphi(a_n)$$

(t.j. keď φ zachováva lineárne kombinácie)

Lemma 1.6.3
Nech φ je homomorfizmus $\mathbf{V}_1 \to \mathbf{V}_2$. Potom:

1. $\varphi(\boldsymbol{o}) = \boldsymbol{o}$
2. $\varphi(-a) = -\varphi(a) \quad \forall a \in \mathbf{V}_1$

Veta 1.6.4
Nech $\mathbf{V}$ je vektorový priestor nad $\mathbb{F}$, nech $\dim \mathbf{V} = n \geq 1$. Nech $b_1, \ldots, b_n$ je ľubovoľná báza vektorového priestoru $\mathbf{V}$. Zobrazenie $\varphi : \mathbf{V} \to \mathbf{V}_n(\mathbb{F})$, ktoré každému vektoru $\alpha \in \mathbf{V}$ priradí n-ticu jeho súradníc vzhľadom k báze $b_1, \ldots, b_n$, je izomorfizmus.

Poznámka 1.6.5
Ak existuje izomorfizmus $\mathbf{V}_1 \to \mathbf{V}_2$, tak $\mathbf{V}_1$ je izomorfný s vektorovým priestorom $\mathbf{V}_2$.

Veta 1.6.6
Relácia „byť izomorfný s“ je reflexívna, symetrická a tranzitívna, t.j. je reláciou ekvivalencie.

Dôsledok 1.6.7 (1)
Ak $\mathbf{V}$ je vektorový priestor nad $\mathbb{F}$, $\dim \mathbf{V} = n \geq 1$, tak $\mathbf{V}$ je izomorfný s vektorovým priestorom $\mathbf{V}_n(\mathbb{F})$.

Dôsledok 1.6.8 (2)
Ak $\mathbf{V}_1, \mathbf{V}_2$ sú vektorové priestory nad $\mathbb{F}$, pričom $\dim \mathbf{V}_1 = \dim \mathbf{V}_2 = n$, tak $\mathbf{V}_1, \mathbf{V}_2$ sú izomorfné.

Veta 1.6.9
Nech φ je izomorfizmus $\mathbf{V}_1$ na $\mathbf{V}_2$ a nech $b_1, \ldots, b_n$ tvoria bázu $\mathbf{V}_1$. Potom $\varphi(b_1), \ldots, \varphi(b_n)$ tvoria bázu $\mathbf{V}_2$.

Dôsledok 1.6.10
Ak $\mathbf{V}_1, \mathbf{V}_2$ sú izomorfné vektorové priestory a nech niektorý z nich je konečnorozmerný. Potom aj druhý je konečnorozmerný a má rovnakú dimenziu.

1.7 Hodnosť systému vektorov

Definícia 1.7.1
Systémy vektorov $\mathbf{S}$, $\mathbf{T}$ vo vektorovom priestore $\mathbf{V}$ nazývame ***ekvivalentnými***, ak generujú ten istý podpriestor.

$$[\mathbf{S}] = [\mathbf{T}]$$

Lemma 1.7.2
Nech $\mathbf{S} = a_1, \ldots, a_i, a_j, \ldots, a_n$ je systém vektorov vektorového priestoru $\mathbf{V}$. Každý z nasledovných systémov je ekvivalentný so systémom $\mathbf{S}$:

- $a_1, \ldots, a_j, a_i, \ldots, a_n$

- $a_1, \ldots, a_i, a_j + \lambda a_i, \ldots, a_n$, *pričom* λ *je ľubovoľný skalár*
- $a_1, \ldots, \kappa a_i, \ldots, a_n$, *pričom* κ *je nenulový skalár*
- $a_1, \ldots, a_n, \alpha_1 a_1 + \ldots + \alpha_n a_n$, *kde* $\alpha_1, \ldots, \alpha_n$ *sú ľubovoľné skaláre*

Definícia 1.7.3
Pod ***hodnosťou*** (konečného) systému vektorov $\mathsf{S} = a_1, \ldots, a_n$ rozumieme dimenziu lineárneho obalu tohto systému vektorov.

$$\mathrm{hod}\,\mathsf{S} = \dim[\{a_1, \ldots, a_n\}]$$

Poznámka 1.7.4
Ak S,T sú ekvivalentné systémy vektorov a jeden z týchto systémov je konečný, potom

$$\mathrm{hod}\,\mathsf{S} = \mathrm{hod}\,\mathsf{T}$$

Lemma 1.7.5
Nech $a_1, \ldots, a_n \in \mathbf{V}_n(\mathbb{F})$ *a nech* $b_1, \ldots, b_n$ *vzniknú z* $a_1, \ldots, a_n$ *vzájomnou výmenou niektorých dvoch zložiek. Potom*

1. a_n *je lineárnou kombináciou* $a_1, \ldots, a_{n-1}$ *práve vtedy, keď* b_n *je lineárnou kombináciou* $b_1, \ldots, b_{n-1}$
2. $\mathrm{hod}\{a_1, \ldots, a_n\} = \mathrm{hod}\{b_1, \ldots, b_n\}$

Poznámka 1.7.6
Systémy $a_1, \ldots, a_n; b_1, \ldots, b_n$ z predchádzajúcej lemmy vo všeobecnosti nemusia byť ekvivalentné.

1.8 Hodnosť matice

$$\boldsymbol{A} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \in \mathbb{F}_{m \times n}$$

Označme:
riadok matice $a_i = (a_{i1}, a_{i2}, \ldots, a_{in})$,
stĺpec matice $\overline{a_i} = (a_{1i}, a_{2i}, \ldots, a_{mi})$,

Definícia 1.8.1
Riadkovou (stĺpcovou) hodnosťou matice $\boldsymbol{A}$ rozumieme

$$\mathrm{hod}\{a_1, a_2, \ldots, a_m\} \qquad \mathrm{hod}\{\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}\}$$

Definícia 1.8.2
Podmaticou matice A rozumieme maticu, ktorú získame vynechaním niektorých riadkov a stĺpcov matice $\boldsymbol{A}$ (nemusíme vynechať nič, nemožno však vynechať všetko).

Definícia 1.8.3
Subdeterminantom matice $\boldsymbol{A}$ rozumieme determinant ľubovoľnej štvorcovej podmatice matice $\boldsymbol{A}$.

Definícia 1.8.4
Označme:
Priestor riadkov matice: $h_r(\boldsymbol{A}) = \mathrm{hod}\{a_1, \ldots, a_n\} = \dim[\{a_1, \ldots, a_n\}]$
Priestor stĺpcov matice: $h_s(\boldsymbol{A}) = \mathrm{hod}\{\overline{a_1}, \ldots, \overline{a_n}\} = \dim[\{\overline{a_1}, \ldots, \overline{a_n}\}]$
Maximum zo stupňov nenulových subdeterminantov matice $\boldsymbol{A}$: $t(\boldsymbol{A})$

Lemma 1.8.5
Nech $\boldsymbol{B}$ vznikne z $\boldsymbol{A}$ tak, že vymeníme v $\boldsymbol{A}$ navzájom niektoré riadky alebo stĺpce. Potom

$$h_r(\boldsymbol{A}) = h_r(\boldsymbol{B}), \qquad h_s(\boldsymbol{A}) = h_s(\boldsymbol{B}), \qquad t(\boldsymbol{A}) = t(\boldsymbol{B})$$

Lemma 1.8.6
Pre ľubovoľnú maticu $\boldsymbol{A}$ platí, že $h_r(\boldsymbol{A}) = t(\boldsymbol{A})$.

Poznámka 1.8.7
Analogicky možno dokázať:
Pre ľubovoľnú maticu $\boldsymbol{A}$ platí, že $h_s(\boldsymbol{A}) = t(\boldsymbol{A})$.

Dôsledok 1.8.8
Pre ľubovoľnú maticu $\boldsymbol{A}$ platí:

$$h_s(\boldsymbol{A}) = h_r(\boldsymbol{A}) = t(\boldsymbol{A}).$$

Definícia 1.8.9
Hodnosťou matice $\boldsymbol{A}$ rozumieme spoločnú hodnotu riadkovej a stĺpcovej hodnosti tejto matice.

Veta 1.8.10 (Frobeniova)
Majme danú sústavu rovníc:

$$(L) = \begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n & = & b_1 \\ & \vdots & \\ a_{m1}x_1 + \ldots + a_{mn}x_n & = & b_n \end{cases}$$

Táto sústava má riešenie $\Leftrightarrow$ keď hodnosť matice tejto sústavy je rovná hodnosti rozšírenej matice tejto sústavy.

1.9 Homogénne matice – fundamentálny systém riešení

Majme homogénnu sústavu rovníc:

$$(H) = \begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n & = & 0 \\ & \vdots & \\ a_{m1}x_1 + \ldots + a_{mn}x_n & = & 0 \end{cases}$$

Lemma 1.9.1
Množina všetkých riešení sústavy (H) $\Omega(H)$ je podpriestorom vektorového priestoru $\mathbf{V}_n(\mathbb{F})$.

Veta 1.9.2
Nech hodnosť matice sústavy (H) je k. Potom dimenzia priestoru riešení sústavy (H) je $(n-k)$.

Definícia 1.9.3
Fundamentálnym systémom riešení sústavy (H) rozumieme ľubovoľnú bázu riešení tejto sústavy.

2 Okruh, obor integrity

2.1 Definícia a dôsledky

Definícia 2.1.1
Okruhom nazývame usporiadanú trojicu ($\mathbf{O}$,+,.), kde $\mathbf{O}$ je ľubovoľná množina, a +, . sú binárne operácie spĺňajúce podmienky:

1. $\forall a, b \in \mathbf{O} : a + b = b + a$
2. $\forall a, b, c \in \mathbf{O} : a + (b + c) = (a + b) + c$
3. $\exists 0 \in \mathbf{O} : \forall a \in \mathbf{O} : a + 0 = a$ (zákon nulového prvku)
4. $\forall a \in \mathbf{O}\ \exists b \in \mathbf{O} : a + b = 0$ (zákon opačného prvku)
5. $\forall a, b, c \in \mathbf{O} : a\,.\,(b\,.\,c) = (a\,.\,b)\,.\,c$ (asociatívnosť .)
6. $\forall a, b, c \in \mathbf{O} : a\,.\,(b + c) = a\,.\,b + a\,.\,c$ (ľavý distributívny zákon)
7. $\forall a, b, c \in \mathbf{O} : (a + b)\,.\,c = a\,.\,c + b\,.\,c$ (pravý distributívny zákon)

Príklad 2.1.2 (príklady okruhov)
- každé pole
- $\mathbb{Z}$ (celé čísla), $\mathbb{Z}_n$ pre každé $n \in \mathbb{N}$

Definícia 2.1.3
Komutatívnym okruhom nazývame taký okruh, v ktorom navyše platí:

8. $\forall a, b \in \mathbf{O} : a\,.\,b = b\,.\,c$ (komutatívny zákon pre .)

Definícia 2.1.4
Okruh s jednotkovým prvkom je okruh, v ktorom navyše platí:

9. $\exists 1 \neq 0 : \forall a \in \mathbf{O} : a\,.\,1 = 1\,.\,a = a$ (zákon jednotkového prvku)

Definícia 2.1.5
Komutatívny okruh s jednotkovým prvkom je okruh v ktorom platia vlastnosti komutatívneho okruhu a zároveň vlastnosti okruhu s jednotkovým prvkom.

Definícia 2.1.6
Oborom integrity nazývame taký komutatívny okruh s jednotkovým prvkov v ktorom navyše platí:

10. $a\,.\,b = 0 \Rightarrow a = 0 \vee b = 0$ (zákon nulového súčinu)

Dôsledok 2.1.7
1. *jednoznačnosť nulového prvku*
2. *jednoznačnosť opačného prvku* $(-a$ *je opačný prvok k* $a)$
3. *zákon krátenia pre +:* $a + u = b + u \Rightarrow a = b$
4. $\forall a : a\,.\,0 = 0\,.\,a = 0$
5. $(-a)\,.\,b = a\,.\,(-b) = -(a\,.\,b)$
6. $(-a)\,.\,(-b) = a\,.\,b$
7. $\forall a : -(-a) = a$

8. *v okruhu s jednotkovým prvkov: jednoznačnosť jednotkového prvku*

9. *v okruhu s jednotkovým prvkom:* $(-1) \,.\, a = -a$

Veta 2.1.8
Nech $\mathbf{O}$ *je ľubovoľný okruh. Nasledovné zákony sú ekvivalentné:*

1. *zákon nulového súčinu*

2. *zákon nenulového súčinu* $(a \neq 0 \wedge b \neq 0 \Rightarrow a \,.\, b \neq 0)$

3. *ľavý zákon krátenia* $(u \,.\, a = u \,.\, b \wedge u \neq 0 \Rightarrow a = b)$

4. *pravý zákon krátenia* $(a \,.\, u = b \,.\, u \wedge u \neq 0 \Rightarrow a = b)$

Príklad 2.1.9
Okruhy:

- $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ so štandardným sčitovaním
- $\mathbb{Z}$ je okruhom aj oborom integrity
- $\mathbb{Z}_m$ (m je zložené číslo) – komutatívny okruh s jednotkovým prvkom
- $2\mathbb{Z}$ (párne celé čísla so štandardnými operáciami) – komutatívny okruh (bez jednotkového prvku)

Obor integrity vo všeobecnosti nie je pole (je to slabšia podmienka), ale každé pole je oborom integrity (napr. $\mathbb{Z}$).

Veta 2.1.10
Každý konečný obor integrity je pole.

2.2 Homomorfizmus, izomorfizmus

Definícia 2.2.1
Nech $(\mathbf{O}_1, +, .)$ a $(\mathbf{O}_2, \oplus, \odot)$ sú okruhy. Zobrazenie $\varphi : \mathbf{O}_1 \to \mathbf{O}_2$ nazývame ***homomorfizmom***, ak:

1. $\forall a, b \in \mathbf{O}_1 : \varphi(a + b) = \varphi(a) \oplus \varphi(b)$

2. $\forall a, b \in \mathbf{O}_1 : \varphi(a \,.\, b) = \varphi(a) \odot \varphi(b)$

Definícia 2.2.2
Vnorenie je prostý homomorfizmus.

Definícia 2.2.3
Izomorfizmus je bijektívny homomorfizmus.

Lemma 2.2.4
Nech $\varphi : \mathbf{O}_1 \to \mathbf{O}_2$ *je homomorfizmus. Potom:*

1. $\varphi(0) = 0$

2. $\varphi(-a) = -\varphi(a), \forall a \in \mathbf{O}_1$

Lemma 2.2.5
Nech $\mathbf{O}_1, \mathbf{O}_2$ *sú okruhy s jednotkovým prvkom. Nech* φ *je nenulový homomorfizmus* $\mathbf{O}_1 \to \mathbf{O}_2$ *a nech v* $\mathbf{O}_2$ *platí zákon nulového súčinu. Potom* $\varphi(1) = 1$

Lemma 2.2.6
Nech φ je nenulový homomorfizmus $\mathbb{F}_1 \to \mathbb{F}_2$, kde $\mathbb{F}_1, \mathbb{F}_2$ sú polia. Potom:

1. $\varphi(1) = 1$
2. $\forall a \in \mathbb{F}_1 - \{0\} : \varphi(a) \neq 0 \wedge \varphi(a^{-1}) = (\varphi(a))^{-1}$
3. *φ je vnorenie*

2.3 Podokruh, podobor integrity, podpole

Definícia 2.3.1
Nech $(\mathbf{O}, +, .)$ je ľubovoľný okruh. ***Podokruhom*** tohto okruhu nazývame neprázdnu podmnožinu $\mathbf{O}_1$ množiny $\mathbf{O}$ spĺňajúcu nasledovné podmienky:

1. $a, b \in \mathbf{O}_1 \Rightarrow a + b \in \mathbf{O}_1$ (uzavretosť pre $+$)
2. $a, b \in \mathbf{O}_1 \Rightarrow a \,.\, b \in \mathbf{O}_1$ (uzavretosť pre .)
3. $a \in \mathbf{O}_1 \Rightarrow -a \in \mathbf{O}_1$

Veta 2.3.2
Ak $\mathbf{O}_1$ je podokruhom okruhu $\mathbf{O}$, tak $\mathbf{O}_1$ je okruhom vzhľadom na $+, .$ definované na $\mathbf{O}$.

Definícia 2.3.3
Nech $(\mathbf{O}, +, .)$ je obor integrity. Pod ***podoborom integrity*** tohto oboru integrity rozumieme takú podmnožinu $\mathbf{O}_1 \subseteq \mathbf{O}$, ktorá je podokruhom pričom jednotkový prvok okruhu $\mathbf{O}$ patrí do $\mathbf{O}_1$.

Veta 2.3.4
Ak $\mathbf{O}_1$ je podoborom integrity oboru integrity $(\mathbf{O}, +, .)$, tak $(\mathbf{O}, +, .)$ je tiež oborom integrity.

Definícia 2.3.5
Nech $(\mathbb{F}, +, .)$ je pole. Pod ***podpoľom*** tohto poľa rozumieme takú podmnožinu $\mathbb{F}_1 \subseteq \mathbb{F}$, ktorá je podoborom integrity a navyše spĺňa podmienku:

$$a \in \mathbb{F}_1 - \{0\} \Rightarrow a^{-1} \in \mathbb{F}_1$$

Veta 2.3.6
Ak $\mathbb{F}_1$ je podpoľom poľa $(\mathbb{F}, +, .)$, tak $(\mathbb{F}, +, .)$ je tiež poľom.

Veta 2.3.7
Prienik ľubovoľného neprázdneho systému podokruhov $\mathbf{O}$ [podoborov integrity $\mathbf{O}$, podpolí poľa $\mathbb{F}$] je podokruhom [podoborom integrity, podpoľom].

Dôsledok 2.3.8
V každom obore integrity [poli] existuje najmenší podobor integrity [najmenšie podpole].

2.4 Rád, charakteristika oboru integrity

Definícia 2.4.1 („krížikové“ násobenie)
Nech $(\mathbf{O}, +, .)$ je ľubovoľný okruh. Nech $a \in \mathbf{O}$. Definujme

$$m \times a = \begin{cases} \underbrace{a + a + \ldots + a}_{(m)\text{-krát}} & m \in \mathbb{N} \\ \text{nulový prvok okruhu } \mathbf{O} & m = 0 \\ \underbrace{(-a) + (-a) + \ldots + (-a)}_{(-m)\text{-krát}} & -m \in \mathbb{N} \end{cases}$$

Veta 2.4.2
Nech $(\mathbf{O}, +, .)$ *je ľubovoľný okruh. Potom* $\forall a, b \in \mathbf{O}, \forall m, n \in \mathbb{Z}$ *platí:*

1. $m \times (-a) = (-m) \times a = -(m \times a)$
2. $(m \times a) + (n \times a) = (m + n) \times a$
3. $m \times (a + b) = (m \times a) + (m \times b)$
4. $m \times (n \times a) = mn \times a$
5. $(m \times a) \,.\, b = m \times a \,.\, b = a \,.\, (m \times b)$
6. $(m \times a) \,.\, (m \times b) = mn \times a \,.\, b$

Definícia 2.4.3
Nech $(\mathbf{O}, +, .)$ je ľubovoľný okruh a nech $a \in \mathbf{O}$. Ak neexistuje $n \in \mathbb{N}$ také, že $n \times a = 0$, hovoríme, že ***rád prvku*** a ***je*** ∞. V opačnom prípade (ak existuje $n \in \mathbb{N}$), najmenšie číslo $n \in \mathbb{N}$ také, že $n \times a = 0$ nazývame ***rádom prvku*** a.

Veta 2.4.4
Všetky nenulové prvky oboru integrity $\mathbf{O}$ *majú rovnaký rád.*

Definícia 2.4.5
Nech $(\mathbf{O}, +, .)$ je ľubovoľný obor integrity. Ak nenulové prvky majú rád ∞, hovoríme, že charakteristika $\mathbf{O}$ je 0. Ak nenulové prvky majú rád $n \in \mathbb{N}$, tak charakteristika $\mathbf{O}$ je n.

Príklad 2.4.6
$\operatorname{char} \mathbb{C} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{Z} = 0$
$\operatorname{char} \mathbb{Z}_p = p$ (p je prvočíslo)

Veta 2.4.7
Charakteristika ľubovoľného oboru integrity je 0 alebo prvočíslo.

Veta 2.4.8
Nech charakteristika oboru integrity $\mathbf{O}$ *je 0 resp.* p *(*p *je prvočíslo). Potom najmenší podobor tohto oboru integrity je izomorfný so* $\mathbb{Z}$*, resp. so* $\mathbb{Z}_p$*.*

Veta 2.4.9
Nech charakteristika poľa $\mathbb{F}$ *je 0 resp.* p*. Potom najmenšie podpole tohto poľa je izomorfné s* $\mathbb{Q}$ *resp. s* $\mathbb{Z}_p$*.*

3 Polynómy

3.1 Obor integrity polynómov

Definícia 3.1.1
Polynómom neurčitej x nad okruhom $\mathbf{O}$ nazývame výraz

$$\sum_{i=0}^{\infty} a_i x^i$$

pričom $\forall i \in \mathbb{N}_0 : a_i \in \mathbf{O}$ a množina tých i, pre ktoré $i \neq 0$ je konečná.
Polynóm, v ktorom $\forall i \in \mathbb{N}_0 : a_i = 0$ sa nazýva ***nulový polynóm***. Iný zápis polynómu:

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$$

Ak $a_n \neq 0$, potom n je ***stupeň polynómu***.
Stupeň nulového polynómu nie je definovaný.

Definícia 3.1.2
Polynómy $f(x) = \sum\limits_{i=0}^{\infty} a_i x^i$ a $g(x) = \sum\limits_{i=0}^{\infty} b_i y^i$ považujeme za ***rovné***, ak

$$\forall i \in \mathbb{N}_0 : a_i = b_i.$$

Definícia 3.1.3
Súčtom polynómov $f(x), g(x)$ rozumieme polynóm

$$\sum_{i=0}^{\infty} (a_i + b_i) x^i$$

Definícia 3.1.4
Súčinom polynómov $f(x), g(x)$ rozumieme polynóm

$$\sum_{i=0}^{\infty} c_i x^i,$$

kde

$$c_i = a_0 b_i + a_1 b_{i-1} + a_2 b_{i-2} + \ldots + a_i b_0 = \sum_{\substack{k,l \in \mathbb{N} \\ k+l=i}} a_i x^i$$

Súčin polynómov je tiež polynóm; ak $\operatorname{st} f(x) = n, \operatorname{st} g(x) = m$, potom $c_{n+m} = a_n b_m$.

Lemma 3.1.5
Súčin 2 nenulových polynómov nad oborom integrity je nenulový polynóm a jeho stupeň sa rovná súčtu stupňov týchto polynómov.

Poznámka 3.1.6
Označenie: $\mathbf{O}$ ... okruh $\mathbf{O}[x]$ ... množina všetkých polynómov neurčitej x nad okruhom $\mathbf{O}$.

Veta 3.1.7
Nech $\mathbf{O}$ je oborom integrity. Potom $\mathbf{O}[x]$ je vzhľadom na vyššie definované sčitovania a násobenie oborom integrity.

Definícia 3.1.8
Nech $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbf{O}[x], u \in \mathbf{O}, n \in \mathbb{N}$. ***Hodnotou*** polynómu $f(x)$ v bode u nazývame prvok z $\mathbf{O}$

$$a_0 + a_1 u + a_2 u^2 + \ldots + a_n u^n = f(u)$$

Definícia 3.1.9
Polynomickou funkciou prislúchajúcou polynómu $f(x)$ rozumieme zobrazenie

$$\mathbf{O} \to \mathbf{O} : \forall u \in \mathbf{O} : u \mapsto f(u)$$

3.2 Deliteľnosť v množine polynómov

Poznámka 3.2.1
Označme: $\mathbb{F}$ ... pole $\mathbb{F}[x]$ ... množina všetkých polynómov neurčitej x nad poľom $\mathbb{F}$

Definícia 3.2.2
Nech $f(x), g(x) \in \mathbb{F}[x]$. Hovoríme, že $f(x)$ ***delí*** g, ak

$$\exists h(x) \in \mathbb{F}[x] : g(x) = f(x) \,.\, h(x).$$

$$\text{Označenie:} \quad f(x) \mid g(x)$$

Veta 3.2.3 (vlastnosti relácie deliteľnosti)

1. $f(x) \mid f(x) \quad \forall f(x) \in \mathbb{F}[x]$ *(reflexívnosť)*
2. $f(x) \mid g(x) \wedge g(x) \mid h(x) \Rightarrow f(x) \mid h(x)$ *(tranzitívnosť)*
3. $f(x) \mid g(x) \wedge f(x) \mid h(x) \Rightarrow f(x) \mid g(x) \pm h(x)$
4. $f(x) \mid g(x) \Rightarrow f(x) \mid g(x) \,.\, h(x) \quad \forall h(x)$
5. $f(x) \mid g(x) \wedge g(x) \neq 0 \Rightarrow f(x) \neq 0, \operatorname{st} f(x) \leq \operatorname{st} g(x)$

Definícia 3.2.4
Polynómy $f(x), g(x)$ nazývame ***asociovanými***, ak

$$f(x) \mid g(x) \wedge g(x) \mid f(x).$$

$$\text{Označenie:} \quad f(x) \sim g(x)$$

Lemma 3.2.5
Relácia asociovanosti je ekvivalencia.

Lemma 3.2.6
Pre $f(x), g(x) \in \mathbb{F}[x]$ platí: $f(x) \sim g(x) \Leftrightarrow$ ak ľubovoľný z nich je c-násobkom druhého pre $c \neq 0$.

Veta 3.2.7 (o delení so zvyškom)
Nech $f(x), g(x) \in \mathbb{F}[x], g(x) \neq 0$. Potom existuje jediná dvojica polynómov $q(x), r(x) \in \mathbb{F}[x]$, že

$$f(x) = g(x) \,.\, q(x) + r(x),$$

pričom

$$r(x) = 0 \qquad \vee \qquad \operatorname{st} r(x) < \operatorname{st} g(x)$$

3.3 Najväčší spoločný deliteľ, najmenší spoločný násobok polynómov

Definícia 3.3.1
Nech $f(x), g(x) \in \mathbb{F}[x]$. ***Najväčším spoločným deliteľom*** polynómov $f(x)$,$g(x)$ nazývame taký polynóm $d(x)$, ktorý spĺňa podmienky:

1. $d(x) \mid f(x) \wedge d(x) \mid g(x)$
2. $d'(x) \mid f(x) \wedge d'(x) \mid g(x) \Rightarrow d'(x) \mid d(x)$

Veta 3.3.2

1. *Nech $d(x)$ je NSD polynómov $f(x), g(x)$ a nech $d_1(x) \sim d(x)$. Potom aj $d_1(x)$ je NSD polynómov $f(x), g(x)$.*
2. *Nech $d_1(x), d_2(x)$ sú ľubovoľné NSD polynómov $f(x), g(x)$. Potom $d_1(x) \sim d_2(x)$.*

Poznámka 3.3.3 (Euklidov algoritmus)
Nech $f(x), g(x) \in \mathbb{F}[x], g(x) \neq 0$.

$$\begin{array}{rrcll}
 & f(x) & = & g(x)\,.\,q_1(x) + r_2(x) & r_2(x) = 0 \ \vee \ \operatorname{st} r_2(x) < \operatorname{st} g(x) \\
\text{ak } r_2(x) \neq 0\text{:} & g(x) & = & r_2(x)\,.\,q_2(x) + r_3(x) & r_3(x) = 0 \ \vee \ \operatorname{st} r_3(x) < \operatorname{st} r_2(x) \\
\text{ak } r_3(x) \neq 0\text{:} & r_2(x) & = & r_3(x)\,.\,q_3(x) + r_4(x) & r_4(x) = 0 \ \vee \ \operatorname{st} r_4(x) < \operatorname{st} r_3(x) \\
 & & \vdots & & \vdots \\
 & r_{n-2}(x) & = & r_{n-1}(x)\,.\,q_{n-1}(x) + r_n(x) & r_n(x) = 0 \ \vee \ \operatorname{st} r_n(x) < \operatorname{st} r_{n-1}(x) \\
\text{ak } r_n(x) \neq 0\text{:} & r_{n-1}(x) & = & r_n(x)\,.\,q_n(x) + 0 &
\end{array}$$

Poznámka 3.3.4
Nech $f(x), g(x) \in \mathbb{F}[x]$. Označme množinu spoločných deliteľov polynómov $f(x), g(x)$ ako:

$$\mathbb{D}(f(x), g(x))$$

Lemma 3.3.5
Nech $f(x) = g(x)\,.\,h(x) + t(x)$. Potom:

$$\mathbb{D}(f(x), g(x)) = \mathbb{D}(g(x), t(x)).$$

Veta 3.3.6

1. *Pre každú dvojicu polynómov $f(x), g(x) \in \mathbb{F}[x]$ existuje ich NSD.*
2. *Ak $d(x)$ je ľubovoľný NSD polynómov $f(x), g(x)$, tak existujú polynómy $u(x), v(x) \in \mathbb{F}[x]$ také, že*
$$d(x) = f(x)\,.\,u(x) + g(x)\,.\,v(x).$$

3.4 Nesúdeliteľnosť polynómov

Definícia 3.4.1
Polynómy $f(x), g(x)$ nazývame ***nesúdeliteľnými***, ak polynóm $z(x) = 1$ je ich najväčším spoločným deliteľom.

Poznámka 3.4.2
Polynómy $f(x), g(x)$ sú nesúdeliteľné, ak $(f(x), g(x)) = 1$, pričom $(f(x), g(x))$ je ich normovaný spoločný deliteľ.

Veta 3.4.3
Polynómy $f(x), g(x) \in \mathbb{F}[x]$ sú nesúdeliteľné $\Leftrightarrow$ keď

$$\exists u(x), v(x) \in \mathbb{F}[x]: \quad 1 = f(x)\,.\,u(x) + g(x)\,.\,v(x)$$

Veta 3.4.4
Ak $d(x)$ je NSD $f(x), g(x)$, pričom $d(x) \neq 0$, tak polynómy $\frac{f(x)}{d(x)}$ a $\frac{g(x)}{d(x)}$ sú nesúdeliteľné.

Veta 3.4.5
Ak $f(x)$ je nesúdeliteľný s $g(x), h(x)$, tak $f(x)$ je nesúdeliteľný s $g(x)\,.\,h(x)$.

Veta 3.4.6
Ak $f(x) \mid g(x)\,.\,h(x)$ a $f(x)$ je nesúdeliteľný s $g(x)$, tak $f(x) \mid h(x)$.

Veta 3.4.7
Ak $f(x) \mid h(x)$ a $g(x) \mid h(x)$ a $f(x), g(x)$ sú nesúdeliteľné, tak $f(x)\,.\,g(x) \mid h(x)$.

Definícia 3.4.8
Polynóm $h(x)$ nazývamé ***najmenším spoločným násobkom*** polynómov $f(x), g(x)$, ak

1. $f(x) \mid h(x) \wedge g(x) \mid h(x)$

2. $h(x)$ delí všetky ostatné spoločné násobky, t.j. ak $t(x)$ je spoločným násobkom $\Rightarrow h(x) \mid t(x)$

Veta 3.4.9
Ak $h(x)$ je najmenším spoločným násobkom, tak všetky s ním asociované polynómy sú spoločnými násobkami.

Veta 3.4.10
Nech $d(x)$ je najväčším spoločným deliteľom polynómov $f(x), g(x)$ a nech $d(x) \neq 0$. Potom

$$\frac{f(x) \,.\, g(x)}{d(x)}$$

je najmenším spoločným násobkom $f(x), g(x)$.

3.5 Rozklad polynómov na ireducibilné činitele

Definícia 3.5.1
Nech $f(x)$ je ľubovoľný polynóm nad $\mathbb{F}$.
Triviálnymi deliteľmi polynómu $f(x)$ nazývame polynómy asociované s $f(x)$ a polynómy asociované s $h(x) = 1$ (polynóm nultého stupňa).
Netriviálnymi deliteľmi nazývame také delitele, ktoré nie sú triviálne.

Definícia 3.5.2
Polynóm stupňa väčšieho ako 1 nazývame:

a) ***ireducibilným***, ak má iba triviálne delitele

b) ***reducibilným***, ak má aj netriviálne delitele

Veta 3.5.3
Nech $f(x)$ je polynóm nad $\mathbb{F}$, $\operatorname{st} f(x) \geq 1$. Potom

$$f(x) \text{ je reducibilný} \Leftrightarrow \exists g(x), h(x) \in \mathbb{F}[x] : f(x) = g(x) \,.\, h(x),$$

pričom

$$\operatorname{st} g(x) < \operatorname{st} f(x) \wedge \operatorname{st} h(x) < \operatorname{st} f(x).$$

Lemma 3.5.4
Nech $p(x)$ je ireducibilný polynóm z $\mathbb{F}[x]$ a nech $p(x) \mid f(x) \,.\, g(x)$. Potom $p(x) \mid f(x) \vee p(x) \mid g(x)$.

Veta 3.5.5
Nech $f(x)$ je ľubovoľný polynóm z $\mathbb{F}[x]$. Potom:

1. *$f(x)$ sa dá rozložiť na súčin konečného počtu ireducibilných polynómov*

2. *ak $f(x) = p_1(x) \dots p_n(x) = q_1(x) \dots q_m(x)$, pričom $p_1(x), \dots, p_n(x), q_1(x), \dots, q_m(x)$ sú ireducibilné,*

tak $m = n$ a existuje taká permutácia φ množiny $\overline{n} = \{1, 2, \dots, n\}$, že $p_1(x) \sim q_{\varphi_1}(x), \dots, p_n(x) \sim q_{\varphi_n}(x)$

3.6 Korene polynómu

Definícia 3.6.1
Hodnotou polynómu $f(x)$ v $u \in \mathbb{F}$ rozumieme

$$f(u) = a_0 + a_1 u + \ldots + a_n u^n.$$

Lemma 3.6.2
Nech $f(x) \in \mathbb{F}[x], u \in \mathbb{F}$. Potom zvyšok po delení polynómu $f(x)$ polynómom $(x-u)$ bude $f(u)$.

Definícia 3.6.3
Nech $f(x) \in \mathbb{F}[x], u \in \mathbb{F}$. Potom u nazývame ***koreňom*** polynómu $f(x)$, ak $f(u) = 0$.

Dôsledok 3.6.4
u je koreňom $f(x) \Leftrightarrow (x-u) \mid f(x)$.

Lemma 3.6.5

1. *Ak $f(x) \in \mathbb{F}[x], \operatorname{st} f(x) > 1$ a $f(x)$ má koreň, tak je reducibilný.*
2. *Ak $\operatorname{st} f(x) = 2 \vee \operatorname{st} f(x) = 3$ a $f(x)$ je reducibilný, tak má koreň.*

Veta 3.6.6
Polynóm stupňa $n, n \geq 0$ nad poľom $\mathbb{F}$ má najviac n koreňov.

Dôsledok 3.6.7
Ak dva polynómy stupňa nanajvýš n majú rovnaké hodnoty vo viac ako n prvkoch z $\mathbb{F}$, tak sa rovnajú.

Dôsledok 3.6.8
Rôznym polynómom nad nekonečným poľom $\mathbb{F}$ prislúchajú rôzne polynomické funkcie.

Veta 3.6.9
Nech sú dané dvojice $(u_0, v_0), (u_1, v_1), \ldots, (u_n, v_n) \in \mathbb{F} \times \mathbb{F}$, pričom $u_0 \neq u_1 \neq \ldots \neq u_n$. Potom existuje práve jeden polynóm $f(x)$ nad $\mathbb{F}$ stupňa nanajvýš n taký, že $f(u_0) = v_0, \ldots, f(u_n) = v_n$.

Definícia 3.6.10
Nech $u \in \mathbb{F}$ je koreňom polynómu $f(x)$ nad $\mathbb{F}$. ***Násobnosťou*** tohto koreňa nazývame $k \in \mathbb{N}$ také, že

$$(x-u)^k \mid f(x) \wedge (x-u)^{(k+1)} \nmid f(x).$$

Ak koreň u má násobnosť k, tak hovoríme, že u je ***k-násobný koreň***. 1-násobnému koreňu hovoríme *jednoduchý*.

Definícia 3.6.11
Nech $f(x)$ je polynóm z $\mathbb{F}[x]$.
Ak $f(x) = c, c \in \mathbb{F}$, tak $f'(x) = 0$.
Ak $f(x) = a_0 + a_1 x + \ldots + a_n x^n, a_n \neq 0; n \in \mathbb{N}$, tak

- $f'(x) = a_1 + 2a_2 x + \ldots + n a_n x^{(n-1)},$
- $f^{(k)}(x) = [f^{(k-1)}(x)]'$.

Veta 3.6.12
Dané sú polynómy $f(x), g(x) \in \mathbb{F}[x]$.

1. $(f(x) + g(x))' = f'(x) + g'(x)$
2. $(f(x) \,.\, g(x))' = f'(x) \,.\, g(x) + f(x) \,.\, g'(x)$

3. $n \in \mathbb{N} : [f^{(n)}(x)]' = n \,.\, f^{(n-1)}(x) \,.\, f'(x)$

Veta 3.6.13
Nech $\mathbb{F}$ je pole charakteristiky 0. Nech $f(x) \in \mathbb{F}[x]$ a nech u je k-násobný koreň polynómu $f(x)$. Ak $k = 1$, tak u nie je koreňom $f'(x)$. Ak $k > 1$, tak u je $(k-1)$-násobný koreň $f'(x)$.

Veta 3.6.14
Nech $\mathbb{F}$ je pole charakteristiky 0. Nech $f(x) \in \mathbb{F}[x]$, a nech u je koreň $f(x)$.
Potom u je k-násobný koreň $\Leftrightarrow f(u) = 0 \wedge f'(u) = 0 \wedge \ldots \wedge f^{(k-1)}(u) = 0 \wedge f^{(k)}(u) \neq 0$.

3.7 Ireducibilné polynómy nad $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

3.7.1 Ireducibilné polynómy nad $\mathbb{C}$

Veta 3.7.1 (Fundamentálna veta algebry)
Každý polynóm nad $\mathbb{C}$ stupňa aspoň 1 má v $\mathbb{C}$ koreň.

Dôsledok 3.7.2 (1)
Nad $\mathbb{C}$ sú ireducibilné práve polynómy 1. stupňa.

Dôsledok 3.7.3 (2)
Každý polynóm nad $\mathbb{C}$ stupňa aspoň 1 sa dá rozložiť na súčin konečného počtu polynómov stupňa 1.

Dôsledok 3.7.4 (3)
Polynóm stupňa $n \in \mathbb{N}$ nad $\mathbb{C}[x]$ má v $\mathbb{C}$ práve n koreňov, ak každý započítavame toľkokrát, koľkonásobný je.

3.7.2 Ireducibilné polynómy nad $\mathbb{R}$

Veta 3.7.5
Nech $u \in \mathbb{C}$ je koreňom polynómu $f(x) \in \mathbb{R}[x]$. Potom $\overline{u}$ je tiež koreň $f(x)$, pričom $u, \overline{u}$ majú rovnakú násobnosť.

Veta 3.7.6
Každý polynóm $f(x)$ nad $\mathbb{R}$, kde $\mathrm{st}\, f(x) \geq 3$, je nad $\mathbb{R}$ reducibiný.

Dôsledok 3.7.7 (1)
Nad $\mathbb{R}$ sú ireducibilné práve polynómy 1. stupňa a tie polynómy 2. stupňa, ktoré nemajú v $\mathbb{R}$ koreň.

Dôsledok 3.7.8 (2)
Každý polynóm nad $\mathbb{R}$ stupňa aspoň 1 sa dá rozložiť na súčin konečného počtu polynómov 1. a 2. stupňa, ktoré nemajú v $\mathbb{R}$ koreň.

3.7.3 Ireducibilné polynómy nad $\mathbb{Q}$

Veta 3.7.9 (užitočná)
Nech $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ je polynóm s celočíselnými koeficientmi a nech $\frac{p}{q}; p, q \in \mathbb{Z}; (p, q) = 1$ je koreňom polynómu $f(x)$. Potom $p \mid a_0, q \mid a_n$.

Dôsledok 3.7.10
Ak polynóm $f(x) \in \mathbb{Z}[x]$ je normovaný a má racionálny koreň, tak ním musí byť celé číslo, ktoré delí hodnotu polynómu v bode 0 (absolútny člen).

Veta 3.7.11
Nech $f(x)$ je polynóm s celočíselnými koeficientmi stupňa $n, n \geq 1$, a nech existujú polynómy $g(x), h(x) \in \mathbb{Q}[x]$ také, že $f(x) = g(x) \,.\, h(x)$, pričom $\operatorname{st} h(x) < n$. Potom existujú aj polynómy $g^*(x), h^*(x) \in \mathbb{Z}[x]$ také, že $f(x) = g^*(x) \,.\, h^*(x)$, pričom $\operatorname{st} g^*(x) = \operatorname{st} g(x), \operatorname{st} h^*(x) = \operatorname{st} h(x)$.

Veta 3.7.12 (Eisensteinovo kritérium)
Nech $f(x) = a_0 + a_1x + \ldots + a_nx^n$ je polynóm s celočíselnými koeficientmi a nech existuje také prvočíslo p, že

$$p \mid a_0, p \mid a_1, \ldots p \mid a_{n-1}, p \nmid a_n, p^2 \nmid a_0.$$

Potom $f(x)$ je ireducibilný nad $\mathbb{Q}$.

Dôsledok 3.7.13
Nad $\mathbb{Q}$ existujú ireducibilné polynómy ľubovoľných stupňov. Obrátená veta k Eisensteinovmu kritériu neplatí.

3.8 Binomické rovnice nad $\mathbb{C}$

Definícia 3.8.1
Binomickým polynómom nad $\mathbb{C}$ stupňa $n, n \geq 1$ budeme nazývať polynóm $x^n + a, a \in \mathbb{C} - \{0\}$. ***Binomickou rovnicou*** budeme nazývať výraz $x^n + a = 0$. Riešenia rovnice $x^n = a$ budeme nazývať n***-tými odmocninami z*** a ($\sqrt[n]{a}$).

Veta 3.8.2
Nech $a \in \mathbb{C} - \{0\}$ má goniometrický tvar

$$a = r(\cos\varphi + i\sin\varphi).$$

Potom rovnici $x^n = a$ vyhovujú práve čísla

$$h_k = u_k(n) = \sqrt[n]{r}\left(\cos\frac{\varphi + 2k\pi}{n} + i\sin\frac{\varphi + 2k\pi}{n}\right)$$

pre všetky možné hodnoty $k \in \mathbb{Z}$. Spomedzi týchto čísel je práve n navzájom rôznych, ktoré môžeme dostať dosadením napr. $0, \ldots (n-1)$ za k.

Dôsledok 3.8.3
Rovnici $x^n = 1$ vyhovujú práve čísla

$$\varepsilon_k(n) = \varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, k \in \mathbb{Z}.$$

Veta 3.8.4
Nech $u \in \mathbb{C}$ je riešením rovnice $x^n = a, a \neq 0$. Potom $\varepsilon_0(n) \,.\, u, \varepsilon_1(n) \,.\, u \ldots \varepsilon_n(n) \,.\, u$ sú všetky riešenia rovnice $x^n = a$.

Lemma 3.8.5
Pre ľubovoľné $l \in \mathbb{Z}$ je $\varepsilon_k^l(n)$ tiež n-tá odmocnina z 1.

Definícia 3.8.6
Primitívnou n-tou odmocninou z 1 rozumieme každú takú n-tú odmocninu z 1, ktorej umocňovaním na celé čísla dostaneme všetky n-té odmocniny z 1.

Lemma 3.8.7
$\varepsilon_k(n) = 1 \Leftrightarrow n \mid k$.

Veta 3.8.8
$\varepsilon_k(n)$ je primitívnou $\sqrt[n]{1} \Leftrightarrow (n,k) = 1$ (t.j. n, k sú nesúdeliteľné).

3.9 Kubické rovnice

Poznámka 3.9.1
Kubickou rovnicou nazývame rovnicu tvaru

$$ax^3 + bx^2 + cx + d = 0$$

Úpravou na normovaný tvar a zavedením substitúcie $x = (y - \frac{b}{3})$ dostávame rovnicu

$$y^3 + py + q,\ \ p, q \in \mathbb{C}, (p \neq 0 \ \ \veebar \ \ q \neq 0),$$

z ktorej formálnym preznačením dostaneme

$$x^3 + px + q = 0$$

Poznámka 3.9.2 (Cardanove vzorce)
Pre korene kubických rovníc platia nasledovné vzťahy:

$$\begin{aligned}
\text{diskriminant } D &= -27q^2 - 4p^3 \\
\alpha^3 &= -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} = -\frac{q}{2} + \sqrt{\frac{-D}{108}} \\
\beta &= -\frac{p}{3\alpha} \\
x_1 &= \alpha + \beta \\
x_2 &= \alpha\varepsilon + \beta\varepsilon^2 = \alpha(-\frac{1}{2} + i\frac{\sqrt{3}}{2}) + \beta(-\frac{1}{2} - i\frac{\sqrt{3}}{2}) \\
x_3 &= \alpha\varepsilon^2 + \beta\varepsilon = \alpha(-\frac{1}{2} - i\frac{\sqrt{3}}{2}) + \beta(-\frac{1}{2} + i\frac{\sqrt{3}}{2})
\end{aligned}$$

3.10 Polynómy viacerých neurčitých

Definícia 3.10.1
Polynómom viacerých neurčitých $x_1, \ldots, x_n;\ n \in \mathbb{N}$ nad poľom $\mathbb{F}$ rozumieme súčet

$$\sum_{i \in \mathbf{I}} c_i x_1^{\alpha_{1_i}} \ldots x_n^{\alpha_{n_i}}$$

kde $\mathbf{I} \neq \emptyset$; $c_i \in \mathbb{F}; \alpha_{1_i} \ldots \alpha_{n_i} \in \mathbb{N}_0$, pričom $c_i \neq 0$ iba pre konečný počet indexov a
$\forall i, j \in \mathbf{I}; i \neq j, c_i \neq 0, c_j \neq 0 : (\alpha_{1_i} \ldots \alpha_{n_i}) \neq (\alpha_{1_j} \ldots \alpha_{n_j})$.

Poznámka 3.10.2
Nenulový sčítanec nazývame ***členom***.

Definícia 3.10.3
Ak $cx_1^{\alpha_1} \ldots x_n^{\alpha_n}$ je členom polynómu $f(x_1, \ldots, x_n)$, tak usporiadanú n-ticu $(\alpha_1, \ldots, \alpha_n)$ budeme nazývať ***výškou*** tohto člena.

Definícia 3.10.4
Polynómy $f(x_1, \ldots, x_n)$ a $g(x_1, \ldots, x_n)$ budeme považovať za ***rovné***, ak sú oba nulové, alebo sú oba nenulové a existuje taká vzájomne jednoznačná príbuznosť medzi ich členmi, že odpovedajúce si členy majú rovnaké koeficienty a rovnaké výšky.

Definícia 3.10.5
Súčet nenulových polynómov dostaneme sčítaním koeficientov pri členoch rovnakej výšky, ostatné opíšeme.

Definícia 3.10.6
Ak je aspoň jeden z polynómov nulový, tak súčin týchto polynómov je nulový. ***Súčin*** nenulových polynómov je rovný súčtu súčinov ich členov (každý s každým).

Definícia 3.10.7
Na množine n-tíc nezáporných celých čísel $(\mathbb{N}_0^n) = \{(\alpha_1, \ldots, \alpha_n : \alpha_i \in \mathbb{N}_0 \forall i\}$ definujeme reláciu „<“ takto:
ak $(\alpha_1, \ldots, \alpha_n) \neq (\beta_1, \ldots, \beta_n)$, tak $(\alpha_1, \ldots, \alpha_n) < (\beta_1, \ldots, \beta_n) \Leftrightarrow \alpha_i < \beta_i$ pre najmenšie i také, že $\alpha_i \neq \beta_i$.

Lemma 3.10.8
Pre vyššie definovanú reláciu „<“ na množine $\mathbb{N}_0^n$ platí:

1. $\forall \alpha, \beta \in \mathbb{N}_0^n, \alpha \neq \beta : \alpha < \beta \veebar \alpha > \beta$
2. $\alpha < \beta \Rightarrow \beta \not< \alpha$
3. $\alpha < \beta \wedge \beta < \gamma \Rightarrow \alpha < \gamma$
4. $\alpha < \beta \Rightarrow \alpha + \gamma < \beta + \gamma$

Definícia 3.10.9
Lexikografickým usporiadaním členov polynómu n neurčitých nazývame také usporiadanie, že výšky rastú alebo klesajú.
Najvyšším členom nenulového polynómu rozumieme člen s najvyššou výškou.

Lemma 3.10.10
Nech $f(x_1, \ldots, x_n)$, $g(x_1, \ldots, x_n)$ sú nenulové polynómy nad poľom $\mathbb{F}$. Potom súčin najvyšších členov polynómov $f(x_1, \ldots, x_n)$ a $g(x_1, \ldots, x_n)$ je najvyšším členom ich súčinu (a teda súčin je nenulový).

Veta 3.10.11
$\mathbb{F}[x_1, \ldots, x_n]$ *vzhľadom na vyššie definované sčitovanie a násobenie je oborom integrity.*

3.11 Symetrické polynómy

Definícia 3.11.1
Polynóm $f(x_1, \ldots, x_n)$ nad poľom $\mathbb{F}$ nazývame ***symetrickým***, ak sa nemení pri žiadnej permutácii neurčitých.

Poznámka 3.11.2
Označme množinu všetkých symetrických polynómov nad poľom $\mathbb{F}$ neurčitých $x_1, \ldots, x_n$ ako $\mathbb{F}^\circ$.

Veta 3.11.3
$\mathbb{F}^\circ[x_1, \ldots, x_n]$ *je podoborom integrity oboru integrity* $\mathbb{F}[x_1, \ldots, x_n]$.

Poznámka 3.11.4 (Základné symetrické polynómy)

$$\begin{aligned} \sigma_1(x_1, \ldots, x_n) &= \sum_{i=1}^{n} \\ \sigma_2(x_1, \ldots, x_n) &= \sum_{\substack{i, j = 1 \\ i < j}}^{n} x_i x_j \end{aligned}$$

$$
\begin{aligned}
\sigma_3(x_1,\ldots,x_n) &= \sum_{\substack{i,j,k=1\\ i<j<k}}^{n} x_i x_j x_k\\
&\vdots\\
\sigma_{n-1}(x_1,\ldots,x_n) &= \sum_{\substack{i_1,\ldots,i_n=1\\ i_1<\ldots<i_n}}^{n} x_{i_1}\ldots x_{i_{n-1}}\\
\sigma_n(x_1,\ldots,x_n) &= \prod_{i=1}^{n} x_i
\end{aligned}
$$

Veta 3.11.5
Nech $f(x_1,\ldots,x_n)\in\mathbb{F}[x_1,\ldots,x_n]$.
Potom $f(\sigma_1(x_1,\ldots,x_n),\sigma_2(x_1,\ldots,x_n),\ldots,\sigma_n(x_1,\ldots,x_n))\in\mathbb{F}^\circ[x_1,\ldots,x_n]$.

Veta 3.11.6 (základná o symetrických polynómoch)
Ku každému polynómu $g(x_1,\ldots,x_n)\in\mathbb{F}^\circ[x_1,\ldots,x_n]$ *existuje jediný taký symetrický polynóm* $f(x_1,\ldots,x_n)\in\mathbb{F}^\circ[x_1,\ldots,x_n]$, *že*

$$f(\sigma_1(x_1,\ldots,x_n),\sigma_2(x_1,\ldots,x_n),\ldots,\sigma_n(x_1,\ldots,x_n))=g(x_1,\ldots,x_n).$$

Definícia 3.11.7
Nech $f(x_1,\ldots,x_n)\in\mathbb{F}[x_1,\ldots,x_n]-\{0\}$.
Ak $cx_1^{\alpha_1}\ldots x_n^{\alpha_n}$ členom tohto polynómu, tak jeho ***stupeň*** je $\alpha_1+\ldots+\alpha_n$. ***Stupeň polynómu*** f je maximum zo stupňov jeho členov. Nenulový polynóm budeme nazývať ***homogénnym***, ak všetky jeho členy majú rovnaký stupeň.

3.12 Metóda neurčitých koeficientov

Lemma 3.12.1
Nech $f(x)$ *je homogénny polynóm stupňa* k *a* $g(x)$ *homogénny polynóm stupňa* l. *Potom* $(f\,.\,g)(x)$ *je homogénny polynóm stupňa* $k+l$.

Poznámka 3.12.2 (Vietove vzťahy)
Nech $u_1,\ldots,u_n$ sú korene polynómu $f(x)=a_0+a_1x+\ldots+a_nx^n;\ a_n\neq 0$, teda

$$f(x)=a_n(x-u_1)(x-u_2)\ldots(x-u_n).$$

Potom

$$\sigma_i(u_1,\ldots,u_n) = (-1)^i\,.\,\frac{a_{n-i}}{a_n},\quad i\in\{1,2,\ldots,n\}$$

4 Lineárne zobrazenia

4.1 Jadro a obor hodnôt

Definícia 4.1.1
Nech $\mathbf{V}_1, \mathbf{V}_2$ sú vektorové priestory nad $\mathbb{F}$.
Zobrazenie $\varphi : \mathbf{V}_1 \to \mathbf{V}_2$ nazývame ***lineárnym zobrazením (homomorfizmom)***, ak spĺňa:

1. $\forall a, b \in \mathbf{V}_1 : \varphi(a + b) = \varphi(a) + \varphi(b)$
2. $\forall a \in \mathbf{V}_1, \alpha \in \mathbb{F} : \varphi(\alpha \,.\, a) = \alpha \,.\, \varphi(a)$

Lemma 4.1.2
$\varphi : \mathbf{V}_1 \to \mathbf{V}_2$ je lineárne $\Leftrightarrow$ ak spĺňa podmienku:

$$\forall a, b \in \mathbf{V}_1,\ \alpha, \beta \in \mathbb{F} : \varphi(\alpha a + \beta b) = \alpha\varphi(a) + \beta\varphi(b)$$

Veta 4.1.3
Nech φ je lineárne zobrazenie $\mathbf{V}_1 \to \mathbf{V}_2$. Potom

1. $\varphi(\boldsymbol{o}) = \boldsymbol{o}$
2. $\varphi(-a) = -\varphi(a)$

Definícia 4.1.4
Nech φ je lineárne zobrazenie $\mathbf{V}_1 \to \mathbf{V}_2$. ***Jadrom*** tohto lineárneho zobrazenia nazývame množinu

$$\operatorname{Ker}\varphi = \{a \in \mathbf{V}_1 :\ \varphi(a) = \mathbf{o}\}.$$

Oborom hodnôt φ nazývame množinu

$$\operatorname{Im}\varphi = \{\varphi(a) : a \in \mathbf{V}_1\}$$

Lemma 4.1.5
Nech φ je lineárne zobrazenie $\mathbf{V}_1 \to \mathbf{V}_2$. Potom

(a) *φ je prosté $\Leftrightarrow$ $\operatorname{Ker}\varphi = \{\boldsymbol{o}\}$*

(b) *φ je na $\Leftrightarrow$ $\operatorname{Im}\varphi = \mathbf{V}_2$*

Veta 4.1.6
Nech φ je lineárne zobrazenie $\mathbf{V}_1 \to \mathbf{V}_2$. Potom

1. *$\operatorname{Ker}\varphi$ je podpriestor $\mathbf{V}_1$*
2. *$\operatorname{Im}\varphi$ je podpriestor $\mathbf{V}_2$*
3. *Ak navyše $\mathbf{V}_1$ je konečnorozmerný, tak $\dim\operatorname{Ker}\varphi + \dim\operatorname{Im}\varphi = \dim\mathbf{V}_1$.*

Definícia 4.1.7
Nech φ je lineárne zobrazenie $\mathbf{V}_1 \to \mathbf{V}_2$, pričom $\mathbf{V}_1$ konečnorozmerný.
Defekt φ definujeme ako

$$\operatorname{def}\varphi := \dim\operatorname{Ker}\varphi.$$

Hodnosť φ definujeme ako

$$\operatorname{hod}\varphi := \dim\operatorname{Im}\varphi.$$

Veta 4.1.8
Nech $\mathbf{V}_1, \mathbf{V}_2$ sú vektorové priestory nad $\mathbb{F}$, pričom $\mathbf{V}_1$ konečnorozmerný.
Nech $\{a_1, \dots, a_n\} \in \mathbf{V}_1$, $\{b_1, \dots, b_n\} \in \mathbf{V}_2$.

1. *Ak $a_1 \dots, a_n$ generuje $\mathbf{V}_1$, tak existuje najviac jedno lineárne zobrazenie $\varphi : \mathbf{V}_1 \to \mathbf{V}_2$ také, že*
   $\varphi(a_1) = b_1, \dots, \varphi(a_n) = b_n$.

2. *Ak $a_1 \dots, a_n$ tvoria bázu $\mathbf{V}_1$, tak existuje práve jedno lineárne zobrazenie $\varphi : \mathbf{V}_1 \to \mathbf{V}_2$, že* $\varphi(a_1) = b_1, \dots, \varphi(a_n) = b_n$.

3. *Ak $a_1 \dots, a_n$ tvoria lineárne nezávislý systém, tak existuje aspoň jedno lineárne zobrazenie* $\varphi : \mathbf{V}_1 \to \mathbf{V}_2$, *že* $\varphi(a_1) = b_1, \dots, \varphi(a_n) = b_n$.

4.2 Vektorový priestor matíc, lineárnych zobrazení

Poznámka 4.2.1
Označme si vektorový priestor matíc $\mathbb{F}_{m\times n}$. Označme si $\mathcal{L}(\mathbf{V}_1, \mathbf{V}_2)$ množinu všetkých lineárnych zobrazení $\mathbf{V}_1 \to \mathbf{V}_2$.

Veta 4.2.2
Množina $\mathbb{F}_{m\times n}$ je vzhľadom na vyššie definované sčitovanie a násobenie prvkami z $\mathbb{F}$ vektorovým priestorom dimenzie $m \times n$.

Definícia 4.2.3
Nech φ, ψ sú lineárne zobrazenia $\mathbf{V}_1 \to \mathbf{V}_2$, $\alpha \in \mathbb{F}$.

1. $\forall a \in \mathbf{V}_1 : \ (\varphi + \psi)(a) = \varphi(a) + \psi(a)$

2. $\forall a \in \mathbf{V}_1 : \ (\alpha\varphi)(a) = \alpha\varphi(a)$

Lemma 4.2.4
Ak $\varphi, \psi \in \mathcal{L}(\mathbf{V}_1, \mathbf{V}_2), \ \alpha \in \mathbb{F}$, tak $\varphi + \psi$, $\alpha\varphi$ sú tiež lineárne zobrazenia.

Veta 4.2.5
$\mathcal{L}(\mathbf{V}_1, \mathbf{V}_2)$ je vzhľadom na vyššie definované sčitovanie a násobenie skalármi vektorovým priestorom.

Definícia 4.2.6
Nech $B = \{b_1, \dots, b_n\}$ je báza $\mathbf{V}_1$ a $C = \{c_1, \dots, c_m\}$ je báza $\mathbf{V}_2$. Nech $\varphi \in \mathcal{L}(\mathbf{V}_1, \mathbf{V}_2)$. ***Maticou lineárneho zobrazenia*** φ vzhľadom k bázam B, C nazývame maticu, ktorej j-tý stĺpec pozostáva zo súradníc vektora $\varphi(b_j)$ vzhľadom k báze C.

$$\text{Označenie:} \qquad (\varphi)_{BC}$$

Veta 4.2.7
Nech $\mathbf{V}_1, \mathbf{V}_2$ sú nenulové konečnorozmerné vektorové priestory na $\mathbb{F}$. Nech B je ľubovoľná báza $\mathbf{V}_1$, C ľubovoľná báza $\mathbf{V}_2$. Potom $\mathcal{L}(\mathbf{V}_1, \mathbf{V}_2) \to \mathbb{F}_{m\times n}$ také, že

$$\varphi(\in \mathcal{L}(\mathbf{V}_1, \mathbf{V}_2) \mapsto (\varphi)_{BC}$$

je izomorfizmus.

Dôsledok 4.2.8
Nech $\mathbf{V}_1, \mathbf{V}_2$ sú konečnorozmerné vektorové priestory nad $\mathbb{F}$. Potom $\mathcal{L}(\mathbf{V}_1, \mathbb{V}_2)$ je tiež konečnorozmerný a platí:

$$\dim \mathcal{L}(\mathbf{V}_1, \mathbf{V}_2) = \dim \mathbf{V}_1 + \dim \mathbf{V}_2$$

4.3 Násobenie matíc, skladanie lineárnych zobrazení

Definícia 4.3.1
Nech $\boldsymbol{A} \in \mathbb{F}_{m\times n}, \boldsymbol{B} \in \mathbb{F}_{n\times p}$.

$$\boldsymbol{A} = \begin{pmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \vdots & \ddots & \vdots \\ \alpha_{m1} & \dots & \alpha_{mn} \end{pmatrix} \qquad \boldsymbol{B} = \begin{pmatrix} \beta_{11} & \dots & \beta_{1p} \\ \vdots & \ddots & \vdots \\ \beta_{n1} & \dots & \beta_{np} \end{pmatrix}$$

Súčinom matíc $\boldsymbol{A} \,.\, \boldsymbol{B}$ nazývame maticu typu $m \times p$, ktorá má na priesečníku i-tého riadku a j-tého stĺpca prvok

$$\sum_{k=1}^{n} \alpha_{ik}\beta_{jk} = \alpha_{i1}\beta_{1j} + \alpha i2\beta 2j + \ldots + \alpha_{in}\beta_{nj}$$

Veta 4.3.2
Nech $n \in \mathbb{N}$. Potom $(\mathbb{F}_{m\times n}, +, .)$ je okruh s jednotkovým prvkom.

Definícia 4.3.3
Nech $\varphi \in \mathcal{L}(\mathbf{V}_1, \mathbf{V}_2), \psi \in \mathcal{L}(\mathbf{V}_2, \mathbf{V}_3)$. Potom súčinom (kompozíciou) zobrazení φ, ψ rozumieme

$$\varphi \circ \psi : \mathbf{V}_1 \to \mathbf{V}_2 : (\varphi \circ \psi)(u) = \psi(\varphi(u))$$

Lemma 4.3.4
Ak $\varphi \in \mathcal{L}(\mathbf{V}_1, \mathbf{V}_2), \psi \in \mathcal{L}(\mathbf{V}_2, \mathbf{V}_3)$, tak $(\varphi \circ \psi) \in \mathcal{L}(\mathbf{V}_2, \mathbf{V}_3)$.

Lemma 4.3.5
$\varphi \circ (\psi + \chi) = \varphi \circ \psi + \varphi \circ \chi$

Lemma 4.3.6
$\lambda(\varphi \circ \psi) = (\lambda\varphi) \circ \psi = \varphi \circ (\lambda\psi)$

Definícia 4.3.7
Lineárnou transformáciou vektorového priestoru rozumieme lineárne zobrazenie $\mathbf{V} \to \mathbf{V}$.
V ďalšom budeme označovať

$$\mathcal{L}(\mathbf{V}) := \mathcal{L}(\mathbf{V}, \mathbf{V})$$

Veta 4.3.8
Množina $\mathcal{L}(\mathbf{V})$ je vzhľadom na sčitovanie a kompozíciu okruhom.
Ak $\mathbf{V}$ je nenulový, tak $\mathcal{L}(\mathbf{V})$ je okruhom s jednotkovým prvkom.

Veta 4.3.9
Nech φ je lineárne zobrazenie z $\mathcal{L}(\mathbf{V}_1, \mathbf{V}_2)$. Nech $B = \{b_1, \ldots, b_n\}$ je báza $\mathbf{V}_1, C = \{c_1, \ldots, c_m\}$ je báza $\mathbf{V}_2$. Potom

$$(\varphi \circ \psi)_{CD} = (\psi)_{CD} \,.\, (\varphi)_{BC}$$

Veta 4.3.10
Nech $\varphi \in \mathcal{L}(\mathbf{V}_1, \mathbf{V}_2)$. Nech $B = \{b_1, \ldots, b_n\}$ je báza $\mathbf{V}_1, C = \{c_1, \ldots, c_m\}$ je báza $\mathbf{V}_2$ Potom pre ľubovoľný vektor $u \in \mathbf{V}_1$ platí:

$$(\varphi(u))_C = (\varphi)_{BC} \,.\, (u)_B$$

4.4 Regulárne matice a regulárne transformácie

Definícia 4.4.1
Nech $\boldsymbol{A} \in \mathbb{F}_{m\times n}$. Inverznou maticou k matici $\boldsymbol{A}$ rozumieme takú maticu $\boldsymbol{B} \in \mathbb{F}_{n\times m}$, že

$$\boldsymbol{B} \,.\, \boldsymbol{A} = \boldsymbol{I}_n \qquad [\boldsymbol{A} \,.\, \boldsymbol{B} = \boldsymbol{I}_m]$$

Ak matica $\boldsymbol{B}$ spĺňa len prvú [druhú] rovnosť, nazývame ju ľavou [pravou] inverznou maticou k matici $\boldsymbol{A}$.

Veta 4.4.2
Nech $\boldsymbol{A} \in \mathbb{F}_{m\times n}$, $\boldsymbol{B}_1$ je ľavá inverzná matica k $\boldsymbol{A}$, $\boldsymbol{B}_2$ je pravá inverzná matica k $\boldsymbol{A}$. Potom

$$\boldsymbol{B}_1 = \boldsymbol{B}_2$$

Dôsledok 4.4.3
Ak k matici $\mathbf{A}$ existuje viac ľavých inverzných matíc, tak neexistuje žiadna ľavá inverzná matica. Ak k $\mathbf{A}$ existuje inverzná matica, tak je len jediná (je určená jednoznačne).

Definícia 4.4.4
Štvorcovú maticu $\boldsymbol{A}$ nazývame ***regulárnou***, ak k nej existuje inverzná matica.

Veta 4.4.5
Nech $\boldsymbol{A}, \boldsymbol{B} \in \mathbb{F}_{n\times n}$ (štvorcové). Potom

$$\det \boldsymbol{A} \,.\, \boldsymbol{B} = \det \boldsymbol{A} \,.\, \det \boldsymbol{B}$$

Veta 4.4.6
Nech $\mathbf{A} \in \mathbb{F}_{n\times n}$. Potom sú nasledovné podmienky ekvivalentné:

1. *$\mathbf{A}$ je regulárna*
2. $\det \mathbf{A} \neq 0$
3. $\operatorname{hod} \mathbf{A} = n$
4. *k $\mathbf{A}$ existuje ľavá inverzná matica*
5. *k $\mathbf{A}$ existuje pravá inverzná matica*
6. *$\mathbf{A}$ možno previesť na jednotkovú pomocou konečného počtu riadkových elementárnych úprav*
7. *$\mathbf{A}$ možno previesť na jednotkovú pomocou konečného počtu stĺpcových elementárnych úprav*

Veta 4.4.7
Postupnosť elementárnych riadkových [stĺpcových] úprav, ktorá prevedie štvorcovú regulárnu maticu $\mathbf{A}$ na jednotkovú prevedie jednotkovú maticu na inverznú k $\mathbf{A}$.

Definícia 4.4.8
Lineárnu transformáciu φ vektorového priestoru V nazývame ***regulárnou***, ak existuje $\psi \in \mathcal{L}(\mathsf{V})$, že:

$$\varphi \circ \psi = \iota_{\mathsf{V}} \qquad \psi \circ \varphi = \iota_{\mathsf{V}}$$

Veta 4.4.9
Nech $\varphi \in \mathsf{V}$, $\dim \mathsf{V} = n \geq 1$. Potom sú nasledovné podmienky ekvivalentné:

1. *φ je regulárna transformácia*
2. *φ je prosté*

3. $\operatorname{Ker}\varphi = \{\boldsymbol{o}\}$

4. φ *je na*

5. $\operatorname{Im}\varphi = \mathbf{V}$

6. φ *je permutácia množiny* $\mathbf{V}$

7. φ *je automorfizmus (izomorfizmus* $\mathbf{V} \to \mathbf{V}$*)*

8. *ak* $b_1, \ldots, b_n$ *tvoria bázu* $\mathbf{V}$, *tak* $\varphi(b_1), \ldots, \varphi(b_n)$ *tvoria bázu*

Veta 4.4.10
Nech $\varphi \in \mathbf{V}_1, \mathbf{V}_2$, $B = \{b_1, \ldots, b_n\}$ *je báza* $\mathbf{V}_1$, $C = \{c_1, \ldots, c_n\}$ *báza* $\mathbf{V}_2$. *Potom*

$$\operatorname{hod}\varphi = \operatorname{hod}(\varphi)_{BC}$$

Dôsledok 4.4.11
Nech $\varphi \in \mathbf{V}$, $B = \{b_1, \ldots, b_n\}$, $C = \{c_1, \ldots, c_n\}$ *sú ľubovoľné bázy* $\mathbf{V}$. *Potom*

$$\varphi \text{ je regulárna transformácia} \Leftrightarrow (\varphi)_{BC} \text{ je regulárna matica}$$

5 Grupy

5.1 Definície a dôsledky

Definícia 5.1.1
Grupou nazývame dvojicu $(\mathbf{G}, \bullet)$, kde $\mathbf{G}$ je množina a $\bullet$ je binárna operácia na $\mathbf{G}$ spĺňajúca:

1. $\forall a, b, c \in \mathbf{G}: \ a \bullet (b \bullet c) = (a \bullet b) \bullet c$
2. $\exists e \in \mathbf{G} \ \forall a \in \mathbf{G}: \ a \bullet e = e \bullet a = a$
3. $\forall a \in \mathbf{G} \ \exists b \in \mathbf{G}: \ a \bullet b = b \bullet a = e$

Ak navyše platí:

4. $\forall a, b \in \mathbf{G}: \ a \bullet b = b \bullet a,$

tak grupu nazvame ***komutatívnou*** alebo ***Abelovskou***.

Dôsledok 5.1.2

1. *jednoznačnosť neutrálneho prvku*
2. *zákony krátenia (ľavý a pravý)*
3. *jednoznačnosť inverzného prvku*
4. *každá z rovníc $ax = b, xa = b, \ a, b \in \mathbf{G}$, má práve jedno riešenie*

5.2 Homomorfizmus

Definícia 5.2.1
Nech $(\mathbf{G}_1, \bullet), (\mathbf{G}_2, \circ)$ sú grupy. Zobrazenie $\varphi : \mathbf{G}_1 \to \mathbf{G}_2$ nazývame ***homomorfizmom***, ak

$$\forall a, b \in \mathbf{G}_1 : \varphi(a \bullet b) = \varphi(a) \circ \varphi(b)$$

Definícia 5.2.2
Zobrazenie $\varphi : \mathbf{G}_1 \to \mathbf{G}_2$ nazývame izomorfizmom, ak φ je bijektívny homomorfizmus.

Lemma 5.2.3
Nech φ je homomorfizmus $(\mathbf{G}_1, \bullet) \to (\mathbf{G}_2, \circ)$. Potom

1. *obraz neutrálneho prvku je neutrálny prvok*
2. *obraz inverzného prvku k prvku $a \in \mathbf{G}_1$ je inverzný k $\varphi(a)$.*

Definícia 5.2.4
Symetriou geometrického útvaru (v $\mathbb{E}_3$) rozumieme bijektívne zobrazenie množiny bodov tohto útvaru na seba také, že zachováva vzdialenosti.

Veta 5.2.5
Existujú práve dve neizomorfné 4-prvkové grupy. (Grupa $(\mathbb{Z}_4, +)$; grupa symetrií obdĺžnika vzhľadom na skladanie.)

5.3 Podgrupa

Definícia 5.3.1
Nech $(\mathsf{G}, \bullet)$ je grupa. ***Podgrupou*** tejto grupy nazývame takú podmnožinu H množiny G, že:

1. H je uzavretá vzhľadom na operáciu $\bullet$ definovanú na G
2. H je grupa.

Veta 5.3.2
Nech $(\mathsf{G}, \bullet)$ je ľubovoľná grupa, $\mathsf{H} \subseteq \mathsf{G}$. Potom H je podgrupa práve vtedy, keď:

1. $a, b \in \mathsf{H} \Rightarrow a \bullet b \in \mathsf{H}$
2. $a \in \mathsf{H} \Rightarrow a^{-1} \in \mathsf{H}$
3. $e \in \mathsf{H}$*, pričom* e *je neutrálny prvok* G

Definícia 5.3.3
Grupou transformácií rozumieme každú podgrupu grupy všetkých permutácií nejakej neprázdnej množiny.

Veta 5.3.4 (Cayleyho o reprezentácii grúp)
Každá grupa je izomorfná s nejakou grupou transformácií.

5.4 Cyklické grupy

Veta 5.4.1
Prienik ľubovoľného neprázdneho systému podgrúp grupy $(\mathsf{G}, \bullet)$ je podgrupou grupy $(\mathsf{G}, \bullet)$.

Dôsledok 5.4.2
Ak $(\mathsf{G}, \bullet)$ je ľubovoľná grupa a $\mathsf{M} \subseteq \mathsf{G}$, tak existuje najmenšia podgrupa grupy $(\mathsf{G}, \bullet)$ obsahujúca množinu M.

Poznámka 5.4.3
Takúto podgrupu nazývame „podgrupou generovanou množinou M“ a označujeme $[\mathsf{M}]$. Zrejme platí:

$$[\emptyset] = \{e\} \qquad [\{a\}] = \{a\}$$

Definícia 5.4.4
Cyklickou grupou nazývame každú grupu $(\mathsf{G}, \bullet)$ takú, že

$$\mathsf{G} = [a], \text{pre } a \in \mathsf{G}$$

Definícia 5.4.5
Nech $(\mathsf{G}, \bullet)$ je grupa, nech $a \in \mathsf{G}$ a nech $n \in \mathbb{Z}$.
Definujeme:

$$a^n = \begin{cases} a \bullet \ldots \bullet a & \text{ak } n > 0 \\ e & \text{ak } n = 0 \\ a^{-1} \bullet \ldots \bullet a^{-1} & \text{ak } n < 0 \end{cases}$$

Lemma 5.4.6
$\forall a, b \in \mathsf{G}, \forall m, n \in \mathbb{Z}$ platí:

1. $a^{m+n} = a^m \bullet a^n$
2. $(a^n)^m = a^{m.n}$

Veta 5.4.7
Nech $(\mathsf{G}, \bullet)$ *je ľubovoľná grupa,* $a \in \mathsf{G}$. *Potom*

$$[a] = \{a^n : n \in \mathbb{Z}\}$$

Definícia 5.4.8
Nech $(\mathsf{G}, \bullet)$ je grupa, $a \in \mathsf{G}$.
Ak $a^n \neq e$ pre žiadne $n \in \mathbb{N}$, hovoríme, že rád a je ∞.
V opačnom prípade rádom prvku a nazývame najmenšie prirodzené číslo n také, že $a^n = e$.

Veta 5.4.9
Nech $(\mathsf{G}, \bullet)$ *je ľubovoľná grupa,* $a \in \mathsf{G}$.
Ak rád $a = \infty$, *tak všetky celočíselné mocniny prvku* a *sú navzájom rôzne.*
Ak rád $a = n$, *tak* $a^0, a^1, \ldots, a^{n-1}$ *sú navzájom rôzne a* $\forall m \in \mathbb{Z}\, \exists n \in \{0, \ldots, n-1\} : a^m = a^n$.

Dôsledok 5.4.10
Ak rád $a = \infty$, *tak* $[a] \cong (\mathbb{Z}, +)$.
Ak rád $a = n$, *tak* $[a] \cong (\mathbb{Z}_n, +)$.

Veta 5.4.11
Každá podgrupa cyklickej grupy je cyklická.