FAKULTA MATEMATIKY, FYZIKY
A INFORMATIKY
UNIVERZITY KOMENSKÉHO
KATEDRA INFORMATIKY

Matematika

Materiál na štátnu skúšku zo spoločného základu odboru Informatika

ONDREJ JOMBÍK

release 0.1.8/0.3.2 build 2005-01-18

Zvolen 2005

Tento dokument vznikol v januári 2005 počas týždňa pred štátnou skúškou z Matematiky v rámci odboru Informatika. Je to vlastne extrakt a prepis viacerých dobrých materiálov. Slúžiť má na lepšie a hlavne rýchlejšie pochopenie celej matematickej časti spoločného základu.

Vzhľadom na rozsiahlosť celej problematiky a limitovaný čas, dokument pokrýva len istú časť učiva. Keďže som skúšku úspešne absolvoval, je vysoko nepravdepodobné, že budem v aktualizácii dokumentu pokračovať. Ak sa však nájde niekto, kto by mal v rámci svojho učenia záujem o doplnenie či dokončenie materiálu, budem rád keď ma kontaktuje. Papierové materiály mu rád poskytnem.

Dokument je písaný v publikačnom systéme LaTeX a spravovaný v rámci `CVS` archívu `Platon SDG`, slovenskej skupiny zaoberajúcej sa najmä vývojom a propagáciou otvoreného softvéru. Aktuálna verzia materiálu sa nachádza na `http://platon.sk/projects/statnica-matematika/`.

Kontaktovať nás môžete na e-mailovej adrese `platon@platon.sk` alebo aj prostredníctvom našej internetovej webstránky `http://platon.sk/`.

Osobitné poďakovanie patrí Ľubomírovi Hostovi za vytvorenie skvelého pracovného a zostavovacieho rámca pre prácu so systémami LaTeX a pdfTeX.

Obsah

Kapitola 1

Algebra

1.1 Úvod

Definícia 1 Usporiadaná dvojica: $(a, b) = \{\{a\}, \{a, b\}\}$

Definícia 2 Karteziánsky súčin A, B: $A \times B = \{(a, b) \mid a \in A, b \in B\}$

Definícia 3 Relácia φ: $\varphi \subseteq A \times B$

1. reflexívna: $(x, x) \in \varphi$
2. symetrická: $(x, y) \in \varphi \Rightarrow (y, x) \in \varphi$
3. tranzitívna: $(x, y) \in \varphi \wedge (y, z) \in \varphi \Rightarrow (x, z) \in \varphi$

Definícia 4 Zobrazenie: taká relácia φ, že $\forall x \in A : \exists! y \in B : (x, y) \in \varphi$

- injektívne: $\forall x, y \in A : x \neq y \Rightarrow \varphi(x) \neq \varphi(y)$
- surjektívne: $\forall y \in B : \exists x \in A : \varphi(x) = y$
- bijektívne: injektívne a surjektívne zároveň

Definícia 5 Binárna operácia:

- komutatívna: $a * b = b * a$

- asociatívna $a * (b * c) = (a * b) * c$
- neutrálny prvok e:
  $x * e = x$
  $e * x = x$
- inverzný prvok x':
  $x * x' = e$
  $x' * x = e$

1.2 Štruktúry

Definícia 6 Usporiadaná dvojica $(G, +)$ sa nazýva pologrupa, ak platí:

1. $G \neq \emptyset$
2. $+$ je asociatívna binárna operácia na G

Definícia 7 Usporiadaná dvojica $(G, +)$ sa nazýva grupa, ak platí:

1. $(G, +)$ je pologrupa
2. $+$ má neutrálny prvok e
3. $\forall x \in G : \exists x' \in G : x + x' = x' + x = e$

Definícia 8 Usporiadaná trojica $(A, +, \circ)$ sa nazýva okruh, ak platí:

1. $(A, +)$ je komutatívna grupa
2. $\circ$ je binárna asociatívna operácia na A
3. $\circ$ je distributívna vzhľadom na $+$

Ak $\circ$ má e, tak okruh nazývame okruh s jednotkou.
Ak $\circ$ je komutatívna, tak okruh nazývame komutatívny okruh.

Definícia 9 Usporiadaná trojica $(A, +, \circ)$ sa nazýva obor integrity, ak platí:

1. $(A, +, \circ)$ je okruh

2. $\forall a, b \in A : a \neq 0 \wedge b \neq 0 \Rightarrow a \circ b \neq 0$

Definícia 10 Usporiadaná trojica $(A, +, \circ)$ sa nazýva teleso, ak platí:

1. $(A, +, \circ)$ je obor integrity
2. $(A, +, \circ)$ má neutrálny prvok operácie $\circ$

Definícia 11 Usporiadaná trojica $(A, +, \circ)$ sa nazýva pole, ak platí:

1. $(A, +, \circ)$ je teleso
2. $\circ$ je komutatívna

1.3 Vektorové priestory

Definícia 12 Vektorový priestor nad poľom F je usporiadaná trojica $(V, +, \varphi)$, ktorá:

1. $(V, +)$ je komutatívna grupa
2. φ je zobrazenie $\varphi : F \times V \to V$ zapisované $\varphi(c, \alpha) = c\alpha$, v ktorom pre $a, b \in F$ a $\alpha, \beta \in V$ platí:
   (a) $(a + b)\alpha = a\alpha + b\alpha$
   (b) $a(\alpha + \beta) = a\alpha + a\beta$
   (c) $a(b\alpha) = (ab)\alpha$
   (d) $1\alpha = \alpha$

Definícia 13 Hovoríme, že sústava $\alpha_1, \alpha_2, ..., \alpha_n$ vektorov je lineárne závislá, ak aspoň jeden z nich je lineárnou kombináciou zostávajúcich.

Definícia 14 Vektorový priestor $(V', \oplus, \psi)$ nazývame podpriestor vektorového priestoru $(V, +, \varphi)$, ak platí:

1. $V' \subset V$
2. $\forall \alpha, \beta \in V' : \alpha \oplus \beta = \alpha + \beta$

3. $\forall c \in F, \forall \alpha \in V' : \psi(c, \alpha) = \varphi(c, \alpha)$

Definícia 15 Bázou vektorového priestoru F nazývame lineárne nezávislú sústavu vektorov $\alpha_1, \alpha_2, ..., \alpha_n$ z V nad F takú, že sústava generuje vektorový priestor V. Označujeme $[\alpha_1, \alpha_2, ..., \alpha_n] = V$

Číslo n je počet vektorov v báze a nazývame ho dimenzia vektorového priestoru.

Veta 1 (Steinitzova o výmene) Nech V je vektorový priestor, $\alpha_1, \alpha_2, ..., \alpha_n$ sú ľubovoľné vektory z V také, že $V = [\alpha_1, \alpha_2, ..., \alpha_n]$. Nech $\beta_1, \beta_2, ..., \beta_m$ sú lineárne nezávislé vektory.
Potom existuje $\alpha_{i_1}, \alpha_{i_2}, ..., \alpha_{i_k}$ také, že $[\beta_1, \beta_2, ..., \beta_m, \alpha_{i_1}, \alpha_{i_2}, ..., \alpha_{i_k}] = V$.

1.4 Súčty podpriestorov

Definícia 16 Nech S, T sú podpriestory vektorového priestoru V nad F. Potom ich lineárnym súčtom nazývame množinu
$S + T = \{\alpha + \beta \mid \alpha \in S, \beta \in T\}$.

Veta 2 Nech S a T sú podpriestory V. Potom aj $S + T$ je podpriestor V.

Veta 3 Nech S a T sú podpriestory V.
Potom $dim(S + T) = dim(S) + dim(T) - dim(S \cap T)$.

Definícia 17 Nech S a T sú podpriestory V, nech $S \cap T = \{\overline{0}\}$.
Potom $S + T$ nazývame direktný súčet S a T a označujeme ho $S \oplus T$.

1.5 Linárne zobrazenia

Definícia 18 Nech V a W sú vektorové priestory nad F.
Zobrazenie $\varphi : V \to W$ sa nazýva lineárne zobrazenie ak, $\forall \alpha, \beta \in V, \forall c \in F$:

1. $\varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta)$
2. $\varphi(c\alpha) = c\varphi(\alpha)$

Veta 4 (Základná veta o lineárnych zobrazeniach) Nech $\alpha_1, \alpha_2, ..., \alpha_n$ je báza vektorového priestoru V. Nech $\beta_1, \beta_2, ..., \beta_n$ sú ľubovoľné (TODO asi je to blud, tiez ma byt baza?!) vektory z W. Potom $\exists!$ lineárne zobrazenie $\varphi : V \to W$, pre ktoré platí:
$\varphi(\alpha_1) = \beta_1, \varphi(\alpha_2) = \beta_2, ..., \varphi(\alpha_n) = \beta_n$.

Toto zobrazenie je dané predpisom
$\varphi(c_1\alpha_1 + c_2\alpha_2 + ... + c_n\alpha_n) = c_1\beta_1 + c_2\beta_2 + ... + c_n\beta_n$.

Definícia 19 Matica lineárneho zobrazenia ... TODO nechapem

Veta 5 (Kompozícia lineárnych zobrazení) Nech $\varphi : U(F) \to V(F)$ a $\psi : V(F) \to W(F)$ sú lineárne zobrazenia. Potom aj $\psi \circ \varphi$ $(= \psi(\varphi))$ je lineárne zobrazenie.

Veta 6 Matica kompozície dvoch lineárnych zobrazení je súčin matíc týchto lineárnych zobrazení v tomto poradí.

Veta 7 (Inverzné lineárne zobrazenie) Inverzné zobrazenie k lineárnemu zobrazeniu, ak existuje, je opäť lineárne.

Definícia 20 Nech $\varphi : V(F) \to W(F)$ je lineárne zobrazenie.

- Jadro zobrazenia φ je množina takých $\alpha \in V(F)$, pre ktoré $\varphi(\alpha) = \overline{0}$.
- Jadro zobrazenia φ je tiež funkcia $Ker(\varphi) = \{x \in V \mid \varphi(x) = \overline{0}\}$.
- Obraz zobrazenia φ je možina takých $\beta \in W(f)$, pre ktoré $\exists \alpha \in V(f) : \varphi(\alpha) = \beta$.
- Obraz zobrazenia φ je tiež funkcia $Im(\varphi) = \{\varphi(x) \in W \mid x \in V\}$.

1.6 Matice

Definícia 21 Nech F je pole. Obdĺžniková tabuľka prvkov poľa F s m riadkami a n stĺpcami sa nazýva matica typu $m \times n$ nad poľom F.

Definícia 22 Transponovanou maticou k matici $A = \| a_{ij} \|$ typu $m \times n$ je matica $B = A^T = \| b_{ij} \|$ typu $n \times m$ s vlastnosťou $b_{ij} = a_{ji}$.

Definícia 23 Riadkovým priestorom matice $A = \| a_{ij} \|$ typu $m \times n$ je vektorový podpriestor F^n generovaný všetkými riadkovými vektormi matice.

Definícia 24 Riadkovou (stĺpcovou) hodnosťou matice $A = \| a_{ij} \|$ typu $m \times n$ rozumieme dimenziu jej riadkového (stĺpcového) priestoru.

Definícia 25 Elementárna riadková operácia na matici A nad F je:

1. vzájomná výmena dvoch riadkov
2. vynásobenie niektorého riadku nenulovým prvkom $c \in F$
3. pripočítanie i-tého riadku k j-tému riadku

Definícia 26 Matice A a B sú riadkovo ekvivalentné, ak existuje konečná postupnosť elementárnych riadkových operácií, ktorými upravíme A na B.

Relácia riadkovej ekvivalencie je reláciou ekvivalencie.

Definícia 27 Matica A typu $m \times n$ nad F je trojuholníková redukovaná, ak platia nasledujúce tvrdenia:

1. vedúci prvok každého nenulového riadku je 1
2. nech $t_1, t_2, ..., t_k$ je postupnosť indexov vedúcich prvkov, potom je táto postupnosť rastúca
3. všetky prvky matice A ležiace nad a pod vedúcim prvkom sú nuly
4. každý nulový riadok matice A sa nachádza za ľubovoľným nenulovým riadkom matice A

Veta 8 Riadkovo ekvivalentným maticiam prislúcha ten istý vektorový priestor.

Veta 9 (Redukcia ľubovoľnej matice) Každá matica je riadkovo ekvivalentná s nejakou trojuholníkovou redukovanou.

1.7 Systémy lineárnych rovníc

Definícia 28 Koreň (riešenie) sústavy $\forall i \in 1..m \sum_{j=1}^{n} a_{ij}x_j = b_i$ je každá usporiadaná n-tica z $z_1, z_2, ..., z_n$ o ktorej platí $\forall i \in 1..m \sum_{j=1}^{n} a_{ij}z_j = b_i$.

Definícia 29 Systém lineárnych rovníc nazývame homogénny, ak má tvar $\forall i \in 1..m \sum_{j=1}^{n} a_{ij}x_j = 0$

Definícia 30
Matica sústavy: TODO picture
Rozšírená matica sústavy: TODO picture

Veta 10 (Frobeniova) Sústava lineárnych rovníc má aspoň jeden koreň práve vtedy, hodnosť matice tejto sústavy sa rovná hodnosti rozšírenej matice sústavy. TODO think about this!

Veta 11 Množina všetkých koreňov homogénnej sústavy lineárnych rovníc tvorí vektorový podpriestor vektorového priestory F^n.

Definícia 31 Fundamentálny systém homogénnej sústavy lineárnych rovníc je každá báza vektorového priestoru všetkých koreňov tejto sústavy.

Veta 12 Nech sústava lineárnych rovníc má aspoň jeden koreň, nech je to $\beta = (y_1, y_2, ..., y_n)$. Potom každý koreň tejto sústavy sa dá napísať v tvare $\gamma = \beta + \alpha$, kde α je vhodný koreň homogénnej sústavy prislúchjúcej k danej sústave.

1.8 Determinanty

Definícia 32 Nech A je štvorcová matica stupňa n nad F. Determinantom matice A označujeme súčet

$$\sum_{\varphi \in P(\{1..n\})} (-1)^{\tau(\varphi)} a_{1,\varphi(1)} a_{2,\varphi(2)} ... a_{n,\varphi(n)} := |A|$$

kde P je množina permutácií prvkov $\{1..n\}$ a $\tau(\varphi)$ je parita permutácie φ.

Definícia 33 Minor prislúchajúci prvku a_{ij} je matica, ktorá vznikne vypustením i-teho riadka a j-teho stĺpca. Označujeme M_{ij}. Ak $i = j$, hovoríme o hlavnom minore.

Definícia 34 Algebraickým doplnkom prvku a_{ij} matice A nazývame číslo $A_{ij} = (-1)^{i+j}|M_{ij}|$. Definície sa rôznia: niekde je uvádzané, že A_{ij} je to isté ako M_{ij}, teda nie skalár, ale matica. My budeme používať prvú definíciu.

Veta 13 Nech A je typu $n \times n$ nad F. Potom:

1. ak k i-temu riadku pripočítame j-tý riadok, determinant sa nezmení
2. ak vymeníme medzi sebou dva riadky, determinant zmení znamenienko
3. ak vynásobíme i-ty riadok nenulovým skalárom $c \in F$, potom determinant upravenej matice bude c-násobkom pôvodnej matice

Veta 14 Ak A je typu $n \times n$ nad F, potom $|A| = |A^T|$.

Veta 15 (Laplaceov rozvoj)

$$\forall i \in 1..n : |A| = a_{i1}A_{i1} + a_{i2}A_{i2} + ... + a_{in}A_{in}$$

$$\forall j \in 1..n : |A| = a_{1j}A_{1j} + a_{2j}A_{2j} + ... + a_{nj}A_{nj}$$

Veta 16 Ak A typu $n \times n$ je regulárna, potom $A^{-1} = \frac{1}{|A|} adj A$, kde $adj A =$ $(...TODOpicture...)$

Veta 17 (Cramerovo pravidlo) Ak determinant matice A systému n lineárnych rovníc o n neznámych je nenulový, tak systém ma práve jedno riešenie tvaru:

$$x_1 = \frac{|D_1|}{|A|}, x_2 = \frac{|D_2|}{|A|}, ..., x_n = \frac{|D_n|}{|A|}$$

kde D_i je matica, ktorá vznikne z A nahradením i-teho stĺpca absolútnymi členmi (tj. pravou stranou sústavy).

1.9 Euklidovské priestory

Definícia 35 Euklidovský priestorom nazývame usporiadanú dvojicu (E, φ), kde E je vektorový priestor nad $\mathbb{R}$ a $\varphi : E \times E \to \mathbb{R}$ je zobrazenie nazývané sklárny súčin (zapisujeme $\varphi(\alpha, \beta) = \langle\alpha, \beta\rangle$) pričom $\forall \alpha, \alpha', \beta \in E, \forall c \in \mathbb{R}$ platí:

1. $\langle\alpha, \alpha\rangle \geq 0, \langle\alpha, \alpha\rangle = 0 \Leftrightarrow \alpha = \overline{0}$
2. $\langle\alpha + \alpha', \beta\rangle = \langle\alpha, \beta\rangle + \langle\alpha', \beta\rangle$
3. $\langle\alpha, \beta\rangle = \langle\beta, \alpha\rangle$
4. $\langle c\alpha, \beta\rangle = c\langle\alpha, \beta\rangle$

Definícia 36 Matica skalárneho súčinu φ je matica $\parallel \varphi_{ij} \parallel$, pre ktorú platí $\langle\alpha, \beta\rangle = \overline{\alpha} \cdot \parallel \varphi_{ij} \parallel \cdot \overline{\beta}^T$.

Definícia 37 Dĺžka (norma) vektora α je $\parallel \alpha \parallel = \sqrt{\langle\alpha, \alpha\rangle}$

Definícia 38 Uhol φ vektorov α a β je $cos\varphi = \frac{\langle\alpha,\beta\rangle}{\|\alpha\|\|\beta\|}$

Veta 18 V euklidovskom vektorovom priestore platí:

1. $\parallel c \cdot \alpha \parallel = |c| \cdot \parallel \alpha \parallel$
2. $\parallel \alpha \parallel > 0$ pre $\alpha \neq \overline{0}$
3. $|\langle\alpha, \beta\rangle| \leq \parallel \alpha \parallel \cdot \parallel \beta \parallel$ (Schwarzova nerovnosť)
4. $\parallel \alpha + \beta \parallel \leq \parallel \alpha \parallel + \parallel \beta \parallel$ (Trojuholníková nerovnosť)

Definícia 39 Nech $\alpha_1, \alpha_2, ..., \alpha_n \in E(V, \varphi)$. Nech $\forall i, j \in \{1..n\}$ také, že $i \neq j$ platí:

- $\langle\alpha_i, \alpha_j\rangle = 0$, potom vektory $\alpha_1, \alpha_2, ..., \alpha_n$ sú ortogonálne
- $\langle\alpha_i, \alpha_j\rangle = 0$ a $\parallel \alpha_i \parallel = 1$, potom vektory $\alpha_1, \alpha_2, ..., \alpha_n$ sú ortonormálne

Definícia 40 Nech M je podmnožina vektorového priestoru E.
Potom ortogonálnym doplnkom množiny M nazývame množinu

$$M^{\perp} = \{\alpha \mid \alpha \in E \wedge \forall \beta \in M : \langle \alpha, \beta \rangle = 0\}$$

Definícia 41 Nech $\alpha_1, \alpha_2, ..., \alpha_n \in (E, \varphi)$ a $dim(E, \varphi) = n$. Potom vektory $\alpha_1, \alpha_2, ..., \alpha_n$ tvoria ortonormálnu bázu vektorového priestoru E, ak sú ortonormálne, tj. sú ortogonálne s dĺžkou 1.

Veta 19 Ortogonálne vektory Euklidovského vektorového priestoru sú lineárne nezávislé.

Ak je počet ortogonálnych vektorov taký aká je dimenzia priestoru, potom tvoria ortogonálnu bázu priestoru. Ak sú navyše ortonormálne, tvoria ortonormálnu bázu.

Veta 20 (Gramm-Schmidtova ortogonalizačná metóda) Nech vektory $\alpha_1, \alpha_2, ..., \alpha_n$ sú lineárne nezávislé z euklidovského vektorového priestoru E. Potom existuje ortonormálna báza $\beta_1, \beta_2, ..., \beta_n$ taká, že

$$[\alpha_1, \alpha_2, ..., \alpha_n] = [\beta_1, \beta_2, ..., \beta_n]$$

Príklad 1 $\alpha_1 = (1, 0, 0, 1), \alpha_2 = (0, 1, 0, 2), \alpha_3 = (0, 0, 1, 2)$
$\beta_1 = \alpha_1 = (1, 0, 0, 1)$
$\beta_2 = \alpha_2 + c_{21}\beta_1$, takže $\langle \beta_1, \beta_2 \rangle = 0 \Rightarrow c_{21} \Rightarrow \beta_2$
$\beta_3 = \alpha_3 + c_{32}\beta_2 + c_{31}\beta_1$, takže $\langle \beta_1, \beta_3 \rangle = 0 \wedge \langle \beta_2, \beta_3 \rangle = 0 \Rightarrow c_{32}, c_{31} \Rightarrow \beta_3$

Nakoniec $\beta_1, \beta_2, \beta_3$ normalizujeme.

1.10 Kvadratické formy

Definícia 42 Nech $n \in \mathbb{N}$, ďalej $i, j \in \{1, ..., n\}$ a tiež $x_1, ..., x_n$ sú premenné. Potom kvadratickou formou n premenných $x_1, ..., x_n$ nazývame výraz

$$\sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} x_i x_j$$

kde $a_{ij} \in F$.

Definícia 43 Kvadratická forma $f(x, y) = xAy^T$ je kladne defnitná, keď pre $x \neq 0, y \neq 0$ je vždy $f > 0$.

Ak pre $x \neq 0, y \neq 0$ je $f \geq 0$, hovoríme o kladnej seminidefinitnosti.

Veta 21 (Maticka kvadratickej formy) Každú kvadratickú formu n premenných $x_1, x_2, ..., x_n$ je možné vyjadriť práve jedným spôsobom v tvare $X \cdot A \cdot X^T$, kde $X = (x_1, x_2, ..., x_n)$ a A je štvorcová symetrická matica stupňa n.

Veta 22 (Kanonický tvar kvadratickej formy) Každú kvadratickú formu n premenných $x_1, x_2, ..., x_n$ možno vhodnou lineárnou transformáciou premenných upraviť na tvar $y_1^2 + ... + y_k^2 - y_{k+1}^2 - ... - y_s^2$, kde $s \leq n$.

Veta 23 (Silvestrov zákon zotrvačnosti) Ak kvadratickú formu upravíme dvoma spôsobmi tak, že v nových formách vystupujú iba druhé mocniny premenných s koeficientami ± 1, tak počet kladných aj počet záporných druhých mocnín je v obidvoch formách rovnaký.

Veta 24 (Silvestrova podmienka) Kvadratická forma $X \cdot A \cdot X^T$ so symetrickou maticou $A = \| a_{ij} \|$ je kladne semidefinitná práve vtedy, keď pre každé $k \in \{1, \ldots, n\}$ je $D_k > 0$, kde D_k je determinant matice

TODO picture

TODO nieco o stvorcovych maticiach

1.11 Podobnosť matíc

Definícia 44 Regulárna matica je každá štvorcová matica stupňa n, ktorej hodnosť je n. V opačnom prípade hovoríme o singulárnej matici.

Definícia 45 Matice A a B typu $n \times n$ nazývame podobnými, ak existuje regulárna matica P typu $n \times n$ taká, že $B = PAP^{-1}$ (ide o reláciu ekvivalencie).

Definícia 46 Nech $\varphi : V(R) \to V(R)$ je lineárne zobrazenie, nech $\alpha_1, \alpha_2, ..., \alpha_n$ je ľubovoľná báza $V(R)$. Nech $\varphi(\alpha_i) = a_{i1}\alpha_1 + a_{i2}\alpha_2 + ... + a_{in}\alpha_n$ pre $i \in 1..n$. Potom maticou transformácie φ vzhľadom na bázu $\alpha_1, \alpha_2, ..., \alpha_n$ nazývame maticu

TODO PICTURE

Veta 25 Nech A je matica lineárneho zobrazenia $\varphi : V(\mathbb{R}) \to V(\mathbb{R})$ vzhľadom na bázu $\alpha_1, \alpha_2, ..., \alpha_n$. Nech X je n-tica súradníc vektora $\alpha \in V(\mathbb{R})$ vzhľadom na bázu α_i. Potom $Y = XA$ je n-tica súradníc vektora $\varphi(\alpha)$ vzhľadom na α_i

Veta 26 Nech A je matica lineárneho zobrazenia φ vzhľadom na bázu $\alpha_1, \alpha_2, ..., \alpha_n$. Nech B je matica vzhľadom na bázu $\beta_1, \beta_2, ..., \beta_n$. Nech P je matica prechodu od bázy $\alpha_1, \alpha_2, ..., \alpha_n$ k báze $\beta_1, \beta_2, ..., \beta_n$. Potom $B = P \cdot A \cdot P^{-1}$.

Veta 27 Nech $f, g : V(\mathbb{R}) \to V(\mathbb{R})$ sú lineárne zobrazenia vzhľadom na $\alpha_1, \alpha_2, ..., \alpha_n$. Ďalej nech M_f je matica f, M_g je matica g. Potom:

1. matica lineárneho zobrazenia $f + g$ vzhľadom na $\alpha_1, ..., \alpha_n$ je $M_f + M_g$
2. matica lineárneho zobrazenia $c \cdot f$ vzhľadom na $\alpha_1, ..., \alpha_n$ je $c \cdot M_f$
3. matica lineárneho zobrazenia $f \circ g$ vzhľadom na $\alpha_1, ..., \alpha_n$ je $M_f \cdot M_g$

1.12 Vlastné čísla

Definícia 47 Vektor $\alpha \in V, \alpha \neq 0$ je <u>charakteristickým (vlastným) vektorom</u> lineárneho zobrazenia $f : V \to V$, ak existuje skalár $c \in F$ s vlastnosťou $f(\alpha) = c\alpha$.

Skalár c s touto vlastnosťou nazývame <u>charakteristickou (vlastnou) hodnotou</u> zobrazenia.

Definícia 48 <u>Charakteristická hodnota matice A</u> lineárneho zobrazenia je

$$A \cdot \alpha = c \cdot \alpha$$

$A \cdot \alpha = c \cdot \alpha \to A \cdot \alpha = c \cdot I \cdot \alpha \to (A - c \cdot I) \cdot \alpha = 0 \Leftrightarrow |A - c \cdot I| = 0$

Determinant matice $A - c \cdot I$ je <u>charakteristický polynóm</u>.

TODO nieco o ortogonalnych maticiach

1.13 Grupy

Definícia 49 Usporiadaná dvojica $(G, *)$ sa nazýva grupa, ak platí:

1. $G \neq \emptyset$
2. $*$ je asociatívna binárna operácia na G
3. $*$ má neutrálny prvok e
4. $\forall x \in G : \exists x^{-1} \in G : x * x^{-1} = x^{-1} * x = e$

Definícia 50 Grupa $(H, *)$ je podgrupa grupy $(G, \circ)$, ak platí:

1. $H \subseteq G$
2. $\forall a, b \in H : a * b = a \circ b$

Definícia 51 Grupa $(G, *)$ sa nazýva cyklická, ak existuje prvok $a \in G$ taký, že platí $[a] = G$.

Definícia 52 V grupe $(G, *)$ definujeme pre každé $n \in \mathbb{Z}$ a pre $\forall a \in G$ grupovú mocninu a^n takto:

- $a^0 = e$
- $a^n = \underbrace{a * a * \ldots * a}_{n\text{-krát}}$ pre $n > 0$
- $a^{-k} = \underbrace{a^{-1} * a^{-1} * \ldots * a^{-1}}_{k\text{-krát}}$ pre $n = -k < 0$

Definícia 53 Nech $a \in G$. Najmenšie kladné celé číslo $k > 0$ s vlastnosťou $a^k = e$ nazývame rád prvku a. Ak také číslo neexsituje, rád prvku je ∞.

Definícia 54 Hovoríme, že grupa $(G, *)$ je izomorfná s grupou $(H, \circ)$, ak existuje bijekcia $\varphi : G \to H$, pre ktorú platí: $\varphi(a * b) = \varphi(a) \circ \varphi(b)$. Zobrazenie φ nazývame izomorfizmus.

Veta 28 (Cayley) Každá grupa je izomorfná s nejakou grupou transformácií.

Veta 29 Každá podgrupa cyklickej grupy je cyklická.

1.14 Rozklady na grupách

Definícia 55 Rozkladom množiny A rozumieme taký systém M jej neprázdnych podmnožín, že:

1. $\bigcup_{M_i \in M} M_i = A$
2. $M_i, M_j \in M \wedge M_i \neq M_j \Rightarrow M_i \cap M_j = \emptyset$

Definícia 56 Nech H je podgrupa grupy $(G, *)$. Potom ľavou triedou G podľa H určenou prvkom a nazývame množinu $a * H = \{a * h \mid h \in H\}$.

Veta 30 Nech H je podgrupa G. Potom ${}^{G}|_{H} = \{xH \mid x \in G\}$ je rozklad na G, pričom $xH = \{xh \mid h \in H\}$.

Veta 31 (Lagrangeova veta) Nech G je konečná grupa a H jej podgrupa. Potom $|H| \mid |G|$, tj. počet prvkov podgrupy delí počet prvkov grupy.

1.15 Homomorfizmus grúp

Definícia 57 Zobrazenie $f : G \to H$, kde $(G, \circ)$ a $(H, *)$ sú grupy, nazývame homomorfizmus, ak $\forall x, y \in G : f(x \circ y) = f(x) * f(y)$.

Definícia 58 Podgrupa H grupy G sa nazýva invariantnou (normálnou) podgrupou, ak $\forall x \in G : xH = Hx$, resp. $\forall x \in G : x^{-1}Hx \subseteq H$.

Definícia 59 Množinu $Z(G) = \{g \in G \mid \forall x \in G : g * x = x * g\}$ nazývame centrum grupy $(G, *)$.

1.16 Faktorové grupy

Definícia 60 Pre triedy grupy $(G, *)$ podľa jej podgrupy H je faktorizovaná grupová operácia určená vzťahom $(Ha) * (Hb) = H(a * b)$, kde $a, b \in G$.

Definícia 61 Množina ${}^{G}|_{H}$ všetkých tried grupy $(G, *)$ podľa jej normálnej podgrupy H, sa nazýva faktorová grupa.

Veta 32 Množina ${}^{G}|_{H}$ tvorí grupu vzhľadom na operáciu násobenia tried po prvkoch $(Ha)(Hb) = Hab$.

- ak G je komutatívna, tak aj ${}^{G}|_{H}$ je komutatívna
- ak G je cyklická, tak aj ${}^{G}|_{H}$ je cyklická
- neutrálny prvok $He = H$
- inverzný prvok $(Ha)^{-1} = Ha^{-1}$

Veta 33 (Základná veta o homomorfizme grúp) Nech $f : G \to H$ je surjektívny homomorfizmus. Potom ${}^{G}|_{Kerf}$ je izomorfný s H.

1.17 Grupy permutácií

Definícia 62 Permutáciou na množine A sa nazývame ľubovoľné bijektívne zobrazenie $f : A \to A$.

Definícia 63 Cyklickou permutáciou (alebo cyklom) prvkov $a_1, a_2, ..., a_k$ množiny X nazývame permutáciu φ, ktorá každý prvok $a_i, i \in \{1, ..., k-1\}$ zobrazí na a_{i+1} a a_k zobrazí na a_1 a ostatné prvky množiny ponechá na mieste.

Číslo k nazývame dĺžka cyklu.

Definícia 64 Hovoríme, že cykly $(a_1, a_2, ..., a_n)$ a $(b_1, b_2, ..., b_m)$ sú disjunktné, ak množiny $\{a_1, a_2, ..., a_n\}$ a $\{b_1, b_2, ..., b_m\}$ sú disjunktné.

Veta 34 Každá permutácia z S_n rôzna od identickej sa dá napísať v tvare súčinu cyklov dĺžky aspoň 2. Ak odhliadneme od poradia cyklov v súčine, tak toto vyjadrenie je jednoznačné.

Veta 35 Rád permutácie, ktorá je súčinom navzájom disjnuktných cyklov je najmenší spoločný násobok ich dĺžok.

Definícia 65 Cykly dĺžky 2 nazývame transpozície. Permutácia sa nazýva párna, ak je súčinom párneho počtu transpozícií. Inak sa permutácia nazýva nepárna.

Veta 36 Každá permutácia sa dá aspoň jedným spôsobom napísať v tvare súčinu transpozícií.

1.18 Okruhy

Definícia 66 Okruhom rozumieme usporiadanú trojicu $(A, +, \cdot)$, kde

1. $(A, +)$ je komutatívna grupa
2. $\cdot$ je asociatívna binárna operácia
3. $\cdot$ je distributívna operácia vzhľadom na $+$

Ak $\cdot$ je komutatívna, tak hovoríme o komutatívnom okruhu.
Ak $\cdot$ má neutrálny prvok, tak hovoríme o okruhu s jednotkou.

Definícia 67 Okruh $(B, \oplus, \odot)$ je podokruh okruhu $(A, +, \cdot)$, ak platí:

1. $B \subseteq A$
2. $\forall a, b \in B : a \oplus b = a + b$
3. $\forall a, b \in B : a \odot b = a \cdot b$

Definícia 68 Charakteristikou okruhu A nazývame najmenšie prirodzené číslo $k > 0$ také, že $k \times a = 0$ pre $\forall a \in A$, kde $k \times a = \underbrace{a + a + ... + a}_{k\text{-krát}}$

Definícia 69 Neprázdna podmnožina I okruhu A sa nazýva ľavým (pravým) ideálom okruhu A, ak platí:

1. $\forall a, b \in I : (a - b) \in I$
2. $\forall a \in I, r \in A : r \cdot a \in I$ resp. $a \cdot r \in I$

Definícia 70 Hovoríme, že okruh A je izomorfný s okruhom A', ak existuje bijekcia $\varphi : A \to A'$ taká, že zachováva sčitovanie a násobenie.

Definícia 71 Homomorfizmus okruhu $(A, +, \cdot)$ do okruhu $(B, \oplus, \odot)$ je každé zobrazenie $f : A \to B$, o ktorom platí:

1. $\forall a, b \in A : f(a + b) = f(a) \oplus f(b)$
2. $\forall a, b \in A : f(a \cdot b) = f(a) \odot f(b)$

Veta 37 Ak $f, g : A \to B$ sú homomorfizmy, tak aj $f + g$ je homomorfizmus.

Veta 38 Ak $f, g : A \to B$ sú homomorfizmy, tak aj $f \cdot g$ je homomorfizmus.

Veta 39 Ak I je ideál okruhu A, tak množina ${}^{A}|_{I}$ všetkých tried aktívnej grupy A podľa podgrupy I s operáciami $\forall a, b \in A$:

$$(a + I) + (b + I) = (a + b) + I$$

$$(a + I)(b + I) = ab + I$$

tvorí okruh, ktorý nazývame faktorový okruh.

Ak A je komutatívny, tak aj ${}^{A}|_{I}$ je komutatívny.
Ak A je s jednotkou, tak aj ${}^{A}|_{I}$ je s jednotkou.

Definícia 72 Hovoríme, že ideál I okruhu A je prvoideálom, ak pre $\forall a, b \in A : a \cdot b \in I \Rightarrow a \in I \vee b \in I$.

Definícia 73 Hovoríme, že ideál I okruhu A je maximálny, ak $I \neq A$ a zároveň $\forall$ ideály $J : I \subseteq J \subseteq A \Rightarrow I = J \vee A = J$.

Veta 40 Faktorový okruh ${}^{A}|_{I}$ komutatívneho okruhu s jednotkou je obor integrity $\Leftrightarrow$ keď I je prvoideál.

Veta 41 Faktorový okruh ${}^{A}|_{I}$ komutatívneho okruhu s jednotkou je pole $\Leftrightarrow$ keď I je maximálny ideál.

Definícia 74 Okruh A nazývame oborom integrity ak má aspoň 2 prvky a pre $\forall a, b \in A, a \neq 0, b \neq 0$ platí $a \cdot b \neq 0$.

Definícia 75 Hovoríme, že okruh A je teleso, ak má aspoň 2 prvky a $\forall a \in A, a \neq 0 : \exists a' \in A : a \cdot a' = a' \cdot a = 1$

Definícia 76 Komutatívne teleso nazývame pole.

Veta 42 Nech A je obor integrity. Potom v A platia tzv. obmedzené pravidlá o krátení, $\forall a, b, c \in A, a \neq 0$:

1. $ab = ac \Rightarrow b = c$

2. $ba = ca \Rightarrow b = c$

Definícia 77 Zlomkom nad oborom integrity D nazývame usporiadanú dvojicu (a, b), kde $a, b \in D, b \neq 0$.

Dva zlomky nazývame ekvivalentnými $((a, b) \equiv (a', b')) \Leftrightarrow ab' = a'b$.

Súčet zlomkov definujeme $(a, b) + (c, d) = (ad + bc, bd)$.
Súčin zlomkov definujeme $(a, b)(c, d) = (ac, bd)$.

Definícia 78 Podielové pole $Q(D)$ oboru integrity D je množina všetkých tried ekvivalencie $[(a, b)]$ zlomkov nad D. Súčet a súčin tried sú definované nasledovne:

$$[(a, b)] + [(c, d)] = [(a, b) + (c, d)]$$
$$[(a, b)][(c, d)] = [(a, b)(c, d)]$$

1.19 Okruhy hlavných ideálov

Definícia 79 Hovoríme, že $x \in A$ generuje ideál I komutatívneho okruhu A s jednotkou, ak $I = xA = \{xa \mid a \in A\}$.

Ideál I generovaný nejakým $x \in A$ nazývame hlavný.

Definícia 80 Komutatívny okruh A s jednotkou nazývame okruh hlavných ideálov, ak každý ideál v A je hlavný.

Definícia 81 Nech A je komutatívny okruh. Hovoríme, že a delí b, $a|b$, ak $\exists c : b = c\dot{a}, a, b, c \in A$.

Definícia 82 Nech A je komutatívny okruh s jednotkou. Hovoríme, že $d \in A$ je najväčším spoločným deliteľom prvkov $a, b \in A$, ak platí:

1. $d|a \wedge d|b$
2. $c|a \wedge c|b$, tak $c|d$

Veta 43 Každé dva prvky z okruhu hlavných ideálov majú najväčšieho spoločného deliteľa.

Definícia 83 Prvok p z okruhu hlavných ideálov A nazývame ireducibilným prvkom, ak p má iba nevlastných deliteľov, tj. delia ho iba delitele jednotky a prvky s ním asociované.

Asociované prvky sú $\forall a, b : a|b \wedge b|a$.

Veta 44 Každý prvok $a \in A$, A je okruh hlavných ideálov, a nie je deliteľ 1, sa dá napísať jediným spôsobom v tvare:

$$a = a_0 p_1 p_2 ... p_n$$

kde p_i sú ireducibilné prvky z A (až na poradie a asociovanosť) a a_0 je deliteľ 1.

Veta 45 (Vlastnosti deliteľnosti)

1. tranzitívnosť: $a|b \wedge b|c \Rightarrow a|c$
2. všetky prvky delia 0:
   (a) $0|0$ pretože $0 = 0 \cdot 0$
   (b) $a|0$ pretože $0 = a \cdot 0$

Definícia 84 Nech A je podokruh B. Prvok $n \in B$ je algebraický nad A, ak existujú $a_0, a_1, ..., a_n \in A$ tak, že

$$a_0 + a_1 n + a_2 n^2 + ... + a_n n^n = 0$$

pričom aspoň jedno $a_i \neq 0$.

V opačnom prípade n voláme transcendentný.

1.20 Okruhy polynómov

Definícia 85 Nech B je komutatívny okruh s jednotkou, nech A je podokruh B, pričom $1 \in A$. Nech ďalej $x \in B$. Hovoríme, že okruh $A[x]$ je okruh polynómov v neurčitej x nad okruhom A, ak pre ľubovoľné $f(x), g(x) \in A[x]$ platí $f(x) = g(x) \Leftrightarrow$ postupnosti ich koeficientov sa rovnajú.

Veta 46 Ku každému komutatívnemu okruhu A s jednotkou existuje okruh polynómov $A[x]$, ktorý je určený jednoznačne až na izomorfizmus.

Definícia 86 Nech $f(x), g(x) \in F[x]$, F je pole. Hovoríme, že $f(x)$ delí $g(x)$, ak existuje $h(x) \in F[x] : g(x) = f(x) \cdot h(x)$, kde $\{a_n\} \cdot \{b_n\} = c_n, c_n = \sum_{i+j=n} a_i b_j$.

Ak $f(x)|g(x)$ a $g(x)|f(x)$ hovoríme o asociovaných polynómoch.

Veta 47 (O delení so zvyškom) Nech $f(x), g(x) \in F[x], g(x) \neq 0$. Potom $\exists q(x), r(x) \in F[x] : f(x) = g(x) \cdot q(x) + r(x), st\ r(x) < st\ g(x)$ a $q(x), r(x)$ sú jednoznačne určené.

Definícia 87 Nech $f_1(x), ..., f_k(x) \in F[x]$. Potom $d(x) \in F[x]$ nazveme najväčším spoločným deliteľom $f_1(x), ..., f_k(x)$, ak

1. $d(x)|f_i(x) \forall i$
2. $h(x)|f_i(x) \forall i \Rightarrow h(x)|d(x)\ (h(x) \in F[x])$

Veta 48 V okruhu polynómov $F[x]$ majú každé dva polynómy najväčší spoločný deliteľ, ktorý je určený jednoznačne až na multiplikatívnu konštantu a dá sa vypočítať pomocou Euklidovho algoritmu.

Definícia 88 Polynómy $f_1(x), ..., f_k(x) \in F[x]$ nazveme nesúdeliteľnými ak $NSD(f_1(x), ..., f_k(x)) = 1$.

Veta 49 $f(x), g(x), h(x) \in F[x]$

- $f(x)|g(x) \cdot h(x) \wedge NSD(f(x), g(x)) = 1 \Rightarrow f(x)|h(x)$
- $f(x)|h(x) \wedge g(x)|h(x) \wedge NSD(f(x), g(x)) = 1 \Rightarrow f(x)g(x)|h(x)$

Definícia 89 Nech $f(x), g(x) \in F[x]$. Potom $g(x)$ je triviálny deliteľ $f(x)$, ak $st\ g(x) = 0$ alebo $f(x) \sim g(x)$.

Definícia 90 Nech $f(x) \in F[x], st\ f(x) \geq 1$. Potom $f(x)$ nažývame ireducibilným v $F[x]$, ak $f(x)$ má v $F[x]$ iba triviálne delitele.

V opačnom prípade hovoríme o reducibilnom polynóme.

Veta 50 (Rozklad na súčin ireducibilných polynómov) Nech polynóm $f(x) = a_0 + ... + a_n x^n, f(x) \in F[x], a_n \neq 0, n \geq 1$. Potom $\exists p_1(x), ..., p_m(x) \in F[x], p_i(x)$ je ireducibilný, také, že platí

$$f(x) = a_n p_1(x) ... p_m(x)$$

pričom rozklad je určený jednoznačne až na poradie.

Definícia 91 Nech F je podpole poľa F'. Nech $f(x) \in F[x]$. Potom prvok $c \in F'$ nazveme koreňom polynómu $f(x)$ v poli F', ak platí

$$f(c) = a_0 + a_1c + ... + a_nc^n = 0$$

Veta 51 Nech F je nadpole F', nech $f(x) \in F[x]$. Potom $c \in F'$ je koreň $f(x) \Leftrightarrow (x-c)|f(x)$ v $F'[x]$.

Definícia 92 Nech F je podpole F'. Potom $c \in F'$ voláme k-násobným koreňom $f(x) \in F[x]$, ak $(x-c)^k|f(x)$ a $(x-c)^{k+1}$ nedelí $f(x)$ v $F'[x]$.

Definícia 93 Pole F sa nazýva algebraicky uzavreté, ak každý polynóm $f(x) \in F[x], st\ f(x) \geq 1$ má v poli F aspoň jeden koreň.

Veta 52 (Steinitzova veta) Ku každému poľu F existuje algebraicky uzavreté nadpole F'.

Veta 53 (Gaussova veta / Základná veta algebry) Pole komplexných čísiel $\mathbb{C}$ je algebraicky uzavreté.

Veta 54 Nech $f(x) \in F[x], st\ f(x) \in \{2,3\}$. Potom $f(x)$ je ireducibilný nad $F \Leftrightarrow f(x)$ nemá korene v F.

Veta 55 Nech F je pole. Potom $F[x]$ je okruh hlavných ideálov.

Definícia 94 Nech F je pole, nech $f(x) = a_0 + ... + a_nx^n \in F[x]$. Polynóm $Df(x) = a_1 + 2a_2x + ... + na_nx^{n-1} \in F[x]$ nazývame formálnou deriváciou polynómu $f(x)$.

Veta 56 Nech $f(x), g(x) \in F[x]$. Potom

1. $D(f(x) + g(x)) = Df(x) + Dg(x)$
2. $D(f(x) \cdot g(x)) = (Df(x)) \cdot g(x) + f(x) \cdot (Dg(x))$

Veta 57 Nech $f(x) \in F[x], st\ f(x) \geq 1$. Potom $f(x)$ má v nejakom nadpoli F aspoň jeden viacnásobný koreň $\Leftrightarrow st\ NSD(f(x), Df(x)) \geq 1$.

Veta 58 Nech $f(x) = a_0 + ... + a_nx^n, n \geq 1, f(x) \in F[x]$. Ďalej nech $c \in F$. Potom existujú jednoznačne určené prvky $b_0, b_1, ..., b_n \in F$ také, že

$$f(x) = b_0 + b_1(x-c) + ... + b_n(x-c)^n$$

1.21 Rozšírenia polí

Definícia 95 Pole L nazývame jednoduchým algebraickým rozšírením poľa $F, F \subseteq L$, ak existuje prvok $u \in L$ algebraický nad F taký, že pole $L = F(u)$ je generované množinou $F \cup \{u\}$.

Ak u je transcendentný nad F, hovoríme o jednoduchom transcendentnom rozšírení.

Veta 59 Jednoduché transcendenté rozšírenie $F(u)$ poľa F je izomorfné s podielovým poľom $Q(F[x])$ okruhu $F[x]$ (polynómov 1 neurčitej nad F).

Definícia 96 Minimálnym polynómom prvku u algebraického nad F nazývame normovaný polynóm $p \in F[x]$, ktorý je generátorom ideálu $\{f \in F[x] \mid f(u) = c\}$ ($\forall f \in F[x]$ teda platí $f(u) = c \Leftrightarrow p|f$).

Veta 60 Ak p je minimálny polynóm prvku u algebraického nad poľom F, tak p je ireducibilný nad F.

Jednoduché algebraické rozšírenie $F(u)$ sa potom rovná okruhu $F[u] = \{f(u) \mid t \in F[x]\}$ (TODO: check this), ktorý je izomorfný s faktorovým okruhom.

Definícia 97 Stupňom algebraického prvku u nad poľom F nazývame stupeň n jeho minimálneho polynómu nad F. Stupeň n nad F označujeme $n = [u : F]$.

Definícia 98 Hovoríme, že pole F' je konečným (nekonečným) rozšírením poľa F, ak F' je konečnorozmerným (nekonečnorozmerným) vektorovým priestorom nad F.

Stupeň rozšírenia je $[F' : F] := dim\ F'\ nad\ F$.

Veta 61 Nech F' je konečné rozšírenie F, F'' je konečné rozšírenie F'. Potom F'' je konečné rozšírenie F a platí:

$$[F'' : F] = [F'' : F'] \cdot [F' : F]$$

Definícia 99 Pole F' nazývame k-násobným algebraickým rozšírením poľa F, ak existujú prvky $u_1, u_2, ..., u_k \in F'$ a postupnosť jednotlivých algebraických rozšírení

$$F_1 = F(u_1), F_2 = F_1(u_2), ..., F_k = F_{k-1}(u_k) = F'$$

Veta 62 Ak u je algebraický nad F, tak rozšírenie $F(u)$ je konečné nad F a platí $[F(u) : F] = [u : F]$.

Opačne, ak F' je konečné rozšírenie nad F, tak každý prvok $u \in F'$ je algebraický nad F a platí $[u : F] \leq [F' : F]$.

1.22 Konečné polia

Veta 63 Nech $[F' : F] = n$ a $|F| = q$. Potom $|F'| = q^n$.

Veta 64 Ak F je konečné pole charakteristiky p, tak existuje $m \in \mathbb{N}$ také, že $|F| = p^n$ (pritom platí, že charakteristika ľubovoľného poľa je prvočíslo alebo 0).

Veta 65 Každý prvok z poľa F, pričom $|F| = q$, je koreňom polynómu $x^p - x \in F[x]$.

Definícia 100 Pole $F' \supset F$ nazývame rozkladovým poľom polynómu $f(x) \in F[x]$, ak je najmenším poľom, nad ktorým sa dá polynóm $f(x)$ napísať v tvare súčinu lineárnych činiteľov.

Veta 66 Ak p je ireducibilný polynóm nad poľom F, tak existuje jednoduché algebraické rozšírenie $F(u)$ generované koreňom polynómu p (napr. $F[x]/p(x)$).

Veta 67 Pre každý polynóm f nad poľom $F, st\ f > 0$, existuje rozkladové pole f nad F.

Veta 68 Ak L, L' sú rozkladové polia polynómu f nad F, tak L je izomorfné s L'.

Veta 69 Pre každé číslo tvaru $q = p^n$, kde p je prvočíslo, $n \in \mathbb{N}, n > 0$, existuje (okrem izomorfizmu) práve jedno q-prvkové pole. Je to rozkladové pole polynómu $x^q - x$ nad $\mathbb{Z}_p$.

Veta 70 Každé dve končné polia s rovnakým počtom prvkov sú izomorfné.

Kapitola 2

Matematická analýza

Kapitola 3

Diskrétna matematika

3.1 Výroky a dôkazy

Definícia 101 Výrok je:

- tvrdenie, o ktorého pravdivosti alebo nepravdivosti má zmysel uvažovať
- *pravdivý* alebo *nepravdivý*
- oznamovacia veta

Definícia 102 Výroková forma alebo formula je výrok, ktorý obsahuje premenné. Ak obsahuje kvantifikátory $\forall, \exists$ tak je to kvantifikovaná formula.

Definícia 103 Matematický dôkaz tvrdenia T je konečná postupnosť $a_1, a_2, ..., a_n$, kde a_i je výrok alebo formula a implikácie $a_1 \rightarrow a_2$, $a_2 \rightarrow a_3, ..., a_{n-1} \rightarrow a_n = T$ sú tautológie.

Definícia 104 Základné typy dôkazov:

1. Priamy
2. Nepriamy
3. Obmenou ($a \rightarrow b \equiv \neg b \rightarrow \neg a$)
4. Matematickou indukciou

3.2 Relácie

Definícia 105 Relácia φ je relációu ekvivalencie na A, ak spĺňa nasledujúce vlastnosti:

1. reflexívnosť: $\forall a \in A : (a, a) \in \varphi$
2. symetrickosť: $\forall a, b \in A : (a, b) \in \varphi \Leftrightarrow (b, a) \in \varphi$
3. tranzitívnosť: $\forall a, b, c \in A : (a, b) \in \varphi \wedge (b, c) \in \varphi \Rightarrow (a, c) \in \varphi$

Príslušnosť $(a, b) \in \varphi$ značíme $a \sim b$.

Definícia 106 Majme nasledujúce vlastnosti relácie φ:

1. asymetrickosť: $(a, b) \in \varphi \Rightarrow (b, a) \notin \varphi$
2. trichotomickosť: $a \neq b \Rightarrow (a, b) \in \varphi \vee (b, a) \in \varphi$
3. zobrazenie: $\varphi \subseteq A \times B$ je zobrazenie ak $(\forall a \in A)(\exists! b \in B) : (a, b) \in \varphi$

Relácia sa nazýva čiastočné usporiadanie, ak je tranzitívna a asymetrická. Relácia sa nazýva (lineárne) usporiadanie, ak je tranzitívna, asymetrická a trichotomická.

3.3 Množiny a mohutnosti

Definícia 107 Systém $\mathcal{S} \subseteq P(A)$ sa nazýva rozklad množiny A, ak $\mathcal{S}$ je systém po dvoch disjunktných neprázdnych množín s vlastnosťou $\bigcup_{M \in \mathcal{S}} M = A$.

Definícia 108 Majme reláciu ekvivalencie a definujme množinu $A(x)$ tak, že $A(x) = \{y \in A \mid x \sim y\}$. Potom $\mathcal{S} = \{A(x) \in P(A) \mid x \in A\}$ je rozklad množiny A.

Definícia 109 Množiny A a B majú rovnakú mohutnosť ak existuje bijektívne zobrazenie $f : A \rightarrow B$. Značíme $|A| \equiv |B|$.

Ak existuje injektívne zobrazenie $f : A \rightarrow B$, potom $|A| \leq |B|$.
Ak $|A| \leq |B| \wedge |A| \neq |B|$, potom $|A| < |B|$.

Definícia 110 Množina A je spočítateľná $\Leftrightarrow |A| = \aleph_0$.
Množina A je konečná $\Leftrightarrow |A| < \aleph_0$.

Definícia 111 (Kardinálne číslo) Množiny rozdelíme do tried ekvivalencie podľa počtu prvkov. Z každej triedy vyberieme jednu zastupujúcu množinu, tzv. kardinálne číslo.

$$\begin{array}{rcccl} |X| & = & 0 & = & \emptyset \\ |X| & = & 1 & = & \{\emptyset\} \\ |X| & = & 2 & = & \{\emptyset, \{\emptyset\}\} \\ \vdots & & & & \end{array}$$

Potom definujeme:

- súčet: $|A| + |B| = |A \times \{\emptyset\} \cup B \times \{\{\emptyset\}\}|$
- súčin: $|A| \cdot |B| = |A \times B|$
- mocnina: $|A|^{|B|} = |\text{Množina } \forall \text{ zobrazení } f : B \to A|$

3.4 Cantor-Bernsteinova veta

Veta 71 (Cantor-Bernstein)

$$|A| \leq |B| \wedge |B| \leq |A| \Rightarrow |A| = |B|$$

Dôkaz 71.1 Dokazujeme, že ak existuje injekcia $f : A \to B$ a zároveň injekcia $g : B \to A$, potom $|A| = |B|$. Vyjadríme si množiny $A_1 = g(B), A_2 = g(f(A)), A_3 = g(f(A_1))$. Dostávame $A \supseteq A_1 \supseteq A_2 \supseteq ... \supseteq A_k \supseteq ....$ Označme $D = \bigcap_{i=0}^{\infty} A_i$. Potom $A = D \cup (A - A_1) \cup (A_1 - A_2) \cup ...$ a tiež $A_1 = D \cup (A_1 - A_2) \cup (A_2 - A_3) \cup ....$
...

3.5 Cantorova veta

Veta 72 (Cantorova) Pre každú množinu $X \neq \emptyset$ platí $|X| < |P(X)|$, kde $P(X) = \{Y \mid Y \subset X\}$.

Dôsledok 72.1

$$|X| < 2^{|X|} = P(X)$$

Dôsledok 72.2 Neexistuje množina všetkých množín.

3.6 Princíp zapojenia a vypojenia

Veta 73 (Zapojenie-vypojenie) Nech $A_1, A_2, ..., A_n$ sú konečné množiny. Pre $\forall k = 1, 2, ..., n$ položme

$$S_k = \sum_{1 \le i_1 < i_2 < ... < i_k \le n} |A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_k}|$$

kde sumačný symbol sa vzťahuje na všetky podmnožiny $\{i_1, i_2, ..., i_k\}$ množiny $\{1, 2, ..., n\}$. Potom

$$|A_1 \cup A_2 \cup ... \cup A_n| = \sum_{k=1}^{n} (-1)^{k+1} S_k$$

Dôkaz 73.1 Úvahou alebo matematickou indukciou vzhľadom na počet množín.

Veta 74 Nech S_B^A je množina všetkých surjektívnych zobrazení z A do B. Nech $|A| = m$, $|B| = n$ a $B = \{b_1, b_2, ..., b_n\}$. Potom

$$|S_B^A| = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m$$

Dôkaz 74.1 Všetkých zobrazení je n^m. Musíme odpočítať počet nesurjekcií $|S_B'^A|$. To sú také zobrazenia $f : A \to [B - \{1\ prvok\}]$. Takýchto zobrazení je $(n-1)^m$. Takýchto prvkov je $\binom{n}{1}$, čize celkom je to $\binom{n}{1}(n-1)^m$ zobrazení. Podobne pre dva prvky je to $\binom{n}{2}(n-2)^m$. Pomocou princípu zapojenia a vypojenia dostávame celkový počet nesurjekcií:

$$|S_B'^A| = \sum_{k=1}^{n} (-1)^{k+1} \binom{n}{k} (n-k)^m$$

Výsledný počet zobrazení je teda

$$|S_B^A| = n^m - |S_B'^A| = \sum_{k=1}^{n} (-1)^k \binom{n}{k} (n-k)^m$$

Veta 75 Nech $A_1, A_2, ..., A_n$ sú konečné množiny. Nech $A(r)$ označuje počet prvkov, ktoré sa nachádzajú v práve r množinách a $A'(r)$ označuje počet prvkov, ktoré sa nachádzajú v aspoň r množinách. Potom

$$A(r) = \sum_{k=r}^{n} (-1)^{k-r} \binom{k}{r} S_k \qquad r = 0, 1, ..., n$$

$$A'(r) = \sum_{k=r}^{n} (-1)^{k-r} \binom{k-1}{r-1} S_k \qquad r = 1, 2, ..., n$$

3.7 Dirichletov princíp

Veta 76 Nech X, Y sú konečné množiny a f je zobrazenie množiny X do Y. Ak $|X| > |Y|$, tak existuje také $y \in Y$, že aspoň pre dva rôzne prvky $x_1, x_2 \in X$ platí $f(x_1) = f(x_2) = y$.

Veta 77 Nech f je zobrazenie množiny X do Y. Nech $\lambda \in \mathbb{N}^+$. Ak $\lambda \cdot |Y| < |X|$, tak $\exists y \in Y$ také, že množina $\{x \in X \mid f(x) = y\}$ má mohutnosť väčšiu než λ.

3.8 Spernerova veta

Veta 78 (Spernerova) Nech A je konečná množina o n prvkoch a $A_1, A_2, ..., A_m$ sú jej neprázdne konečné podmnožiny také, že $A_i \not\subseteq A_j, i \neq j$, tj. nezapadajú do seba. Potom platí

$$m \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$$

kde $|A| = n$, tj. m je maximálny možný počet takých množín.

3.9 Ko:nigova veta

Veta 79 (Ko:nigova o strome) Nech každý vrchol stromu T má konečný stupeň vetvenia. Ak mám nekonečný počet vrcholov, potom existuje v strome aspoň jedna nekonečne dlhá vetva.

3.10 Ramseyho čísla

Definícia 112 Každý graf, ktorý má aspoň $R(m, n)$ vrcholov buď obsahuje K_m ako svoj podgraf, alebo doplnok grafu obsahuje K_n ako svoj podgraf.

Veta 80 (E:rdos, Sekeres) Pre $m, n \geq 2$ platí:

$$R(m, n) \leq R(m, n-1) + R(m-1, n)$$

Veta 81 Pre $m, n \geq 2$ platí:

$$R(m, n) \leq \binom{m+n-1}{n-1}$$

Veta 82 (Ramseyho) Pre ľubovoľné $m, n \geq 2, m, n \in \mathbb{N}$ existuje prirodzené číslo $R(m, n)$ také, že pre každé číslo $r \geq R(m, n)$ platí, že pri ľubovoľnom zafarbení hrán grafu K_r dvoma farbami v ňom existuje jednofarebný podgraf K_m ofarbený prvou farbou alebo jednofarebný podgraf K_n ofarbený druhou farbou.

3.11 Systémy reprezentantov

Veta 83 (Hallova) Pre systém $M = (S_1, S_2, ..., S_m)$ existuje m-tica navzájom rôznych reprezentantov práve vtedy, keď zjednotenie ľubovoľných k-množín obsahuje aspoň k prvkov.

Veta 84 (Ko:nigova) V ľubovoľnej binárnej matici je najväčší počet po dvoch nezávislých jendotlivých prvkov rovný najmenšiemu počtu buniek pokrývajúcich všetky jednotky.

Kapitola 4

Pravdepodobnosť a štatistika

Kapitola 5

Teória grafov

Kapitola 6

Kombinatorická analýza

Kapitola 7

Logika pre informatikov

Literatúra