Poznamky z MATu

Marek Milkovic

1 Vyrokova logika

Vyrokova logika skuma sposob tvorby zlozenych vyrokov z danych jednoduchych vyrokov a zavislosti pravdivosti zlozeneho vyroku na pravdivosti vyrokov z ktorych je zlozeny.
P - neprazdna mnozina symbolov - *prvotnych vyrokov*
Prvotne vyroky predstavuju jednoduche vyroky. Zlozene vyroky sa skladaju z jednoduchych pomocou logickych spojek - $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$.
L_P - jazyk vyrokovej logiky - prvky P, logicke spojky a zatvorky ().
Ulohu zlozenych vyrokov hraju *vyrokove formule* jazyka L_P, ktore vznikaju ako:

1. Kazda prvotna formula $p \in P$ je vyrokova formula
2. Ak su A, B vyrokove formule, tak aj $\neg A$, $A \wedge B$, $A \vee B$, $A \rightarrow B$, $A \leftrightarrow B$.
3. Kazda vyrokova formula vznikne konecnym poctom pouzitia pravidiel 1 a 2

Pravdivostne ohodnotenie prvotnych formuli - $v : P \rightarrow \{0, 1\}$
Rozsirenie na vsetky formule - $\bar{v}$

1. $\bar{v}(p) = v(p) \forall p \in P$
2. Ak su A, B vyrokove formule, tak $\bar{v}(\neg A), \bar{v}(A \wedge B), \bar{v}(A \vee B), \bar{v}(A \rightarrow B), \bar{v}(A \leftrightarrow B)$ sa definuje pomocou pravdivostnej tabulky v zavislosti na hodnote $\bar{v}(A), \bar{v}(B)$ (a tie pozname velmi dobre)

Vyrokova formula A je pravdiva pri ohodnoteni v - $\bar{v}(A) = 1$
Vyrokova formula A je tautologia ak $\bar{v}(A) = 1$ pre lubovolne ohodnotenie v - $\models A$
Vyrokove formule su *ekvivalentne* prave vtedy ak $\bar{v}(A) = \bar{v}(A)$ pre lubovolne ohodnotenie v - $A \leftrightarrow B$ musi byt tautologia
Kazda vyrokova formula je logicky ekvivalentna niektorej vyrokovej formuli, v ktorej su len spojky $\neg, \rightarrow$ (ale aj $\neg, \wedge$ a $\neg, \vee$)

1. Nicodova spojka - $\downarrow$ - NOR
2. Shefferova spojka - $|$ - NAND

1.1 Dokazatelnost vo vyrokovej logike

Vyrokova logika bude budovana ako formalna axiomaticka teoria
Abeceda

1. mnozina P
2. logicke spojky $\neg, \rightarrow$
3. pomocne symboly ()

Formule

1. vsetky prvotne formule su formule
2. ak su A, B formule tak aj $\neg A$ a $A \rightarrow B$ su formule
3. opakovanim 1 a 2 vznikaju formule

Jazyk - abeceda a formule tvoria jazyk
Axiomy - nekonecne mnoho axiomu zadanych pomocou 3 schemat

- (A1) $A \rightarrow (B \rightarrow A)$
- (A2) $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$
- (A3) $(\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B)$

Odvodzovacie pravidlo - *Modus ponens* - pravidlo odlucenia - z formuli $A, (A \rightarrow B)$ sa odvodi B. $A, (A \rightarrow B)$ su predpoklady, B je zaver
Dokaz - lubovolna konecna postupnost $A_1, ..., A_n$ vyrokovych formuli takych, ze $\forall i \leq n$ je A_i bud axiom, alebo zaver pravidla modus ponens
- Formula A je *dokazatelna*, ak existuje dokaz, ktoreho poslednou formulou je A - $\vdash A$
- Kazda dokazatelna formula vo vyrokovej logike je tautologia
Nech T je mnozina formuli vyrokovej logiky. Hovorime, ze konecna postupnost $A_1, ..., A_n$ je

dokazom formule A z predpokladu T, ak A_n je formula A a pre lubovolne $i \leq n$ plati ze A_i je bud axiom, alebo formula z T alebo A_i je zaverom modus ponens - formula A je *dokazatelna z predpoklatu* T - $T \vdash A$
Veta o dedukcii - Nech T je mnozina formuli, nech A, B su formule, potom $T \vdash A \rightarrow B$ prave vtedy ked $T \cup \{A\} \vdash B$.
Veta o uplnosti - pre lubovolnu formulu A vo vyrokovej logike plati $\vdash A$, prave ked $\models A$.

2 Predikatova logika 1.radu

Premenne - prvky z nejakej mnoziny
Funkcne symboly - $f, g, h...$ - operacie, n-arny symbol
Predikat - vztah medzi urcitym poctom objektov
Predikatovy symbol - $p, q, r...$ - vyjadrujeme nimi predikaty - n-arny symbol

Atomicka formula - zlozena premennych, konstant, funkcnych symbolov a predikatovych symbolov
Logicke spojky - rovnake ako vo vyrokovej logike
Kvantifikatory premennych - univerzalny $\forall$ a existencny $\exists$
Abeceda jazyka predikatovej logiky - premenne, konstanty, funkcne a predikatove symboly, logicke spojky, kvantifikatory a pomocne symboly ()
Premenna predikatovej logiky 1. radu predstavuje konkretny objekt, nedokaze predstavovat inu mnozinu

Term

1. Kazda premenna je term
2. Ak je f n-arny funkcny symbol, a $t_1, ..., t_n$ su termy, tak aj $f(t_1, ..., t_n)$ je term
3. Konecny uzitim pravidiel 1 a 2 vznikne term

Atomicka formula
Ak je p n-arny predikatovy symbol a $t_1, ..., t_n$ su termy, tak $p(t_1, ..., t_n)$ je *atomicka formula*

Formule

1. Kazda atomicka formula je formula
2. Ak su φ, ψ formule, tak aj $\neg\varphi, \varphi \wedge \psi, \varphi \vee \psi, \varphi \to \psi, \varphi \leftrightarrow \psi$ su formule
3. Ak je x premenna a φ formula, tak $\forall x\varphi$ a $\exists x\varphi$ su formule
4. Kazda formula vznikne konecnym uzitim formuli 1-3

Vyskyt premennej x vo formuli φ sa nazyva viazany, ak sa nachadza v nejakej podformuli v tvare $\forall x\psi$ alebo $\exists x\psi$. V opacnom pripade sa jedna o vyskyt volny. Formula co neobsahuje ziadnu volnu premennu sa nazyva *uzavrena formula* alebo aj *vyrok*.

2.1 Semantika predikatovej logiky

Chceme dat intepretaciu symbolom jazyka predikatovej logiky 1. radu. Vymedzime teda obor, ktory bude urcovat mozne hodnoty premennych M. Funkcnym symbolom budu odpovedat operacie na M. Predikatovym symbolom budu odpovedat vztahy medzi objektami M, ktore je mozne popisat ako relacie na M.

Realizacia jazyka - Nech je L jazyk 1. radu. Realizaciou jazyka rozumieme algebraicku strukturu $\mathcal{M}$, ktora sa sklada z

1. neprazdnej mnoziny M, ktoru nazveme *univerzum*
2. pre kazdy funkcny symbol f pocetnosti n je dane zobrazenie $f_{\mathcal{M}} : M^n \to M$

3. pre kazdy predikatovy symbol p pocetnosti n, okrem rovnosti, je dana relacia $p_{\mathcal{M}} \subseteq M^n$

Ohodnotenie premennych - Lubovolne zobrazenie e mnoziny vsetkych premennych do univerza M dane realizaciou $\mathcal{M}$ jazyka L
- Ak je x premenna, e ohodnotenie premennych, $m \in M$, potom znacime $e(x/m)$
- **Hodnotu termu** t v realizacii $\mathcal{M}$ pri danom ohodnoteni e znacime $t[e]$ a definovana je nasledovne

1. Ak je t premenna x potom $t[e]$ je $e(x)$
2. Ak je t v tvare $f(t_1, ..., t_n)$, kde f je n-arny funkcny symbol a t_i su termy, potom $t[e]$ je $f_{\mathcal{M}}(t_1[e], ..., t_n[e])$

Nech $\mathcal{M}$ je realizacia jazyka L, nech e je ohodnotenie premennych a φ je formula jazyka L. Definujeme, co znamena *formula φ je pravidva v $\mathcal{M}$ pri ohodnoteni e* - $\mathcal{M} \models \varphi[e]$

1. Ak je φ atomicka formula v tvare $p(t_1, ..., t_n)$, tak $\mathcal{M} \models \varphi[e]$ prave ked $(t_1[e], ..., t_n[e]) \in p_{\mathcal{M}}$
2. Ak je φ atomicka formula v tvare $t_1 = t_2$, tak $\mathcal{M} \models \varphi[e]$ prave ked $t_1[e]$ je ten isty prvok ako $t_2[e]$
3. Ak je φ v tvare $\neg\psi$, tak $\mathcal{M} \models \varphi[e]$ prave ked $\mathcal{M} \not\models \psi[e]$
4. Ak je φ v tvare $\eta \wedge \psi$, $\eta \vee \psi$, $\eta \rightarrow \psi$, $\eta \leftrightarrow \psi$ tak $\mathcal{M} \models (\eta \wedge \psi)[e]$ prave vtedy ak $\mathcal{M} \models \eta[e]$ a zaroven $\mathcal{M} \models \psi[e]$ a analogicky pre zvysok
5. Ak je φ v tvare $\forall x\psi$, tak $\mathcal{M} \models \varphi[e]$ prave vtedy ak $\forall m \in M : \mathcal{M} \models \psi[e(x/m)]$
6. Ak je φ v tvare $\exists x\psi$, tak $\mathcal{M} \models \varphi[e]$ prave vtedy ak $\exists m \in M : \mathcal{M} \models \psi[e(x/m)]$

Formula φ je *splnena* v realizacii $\mathcal{M}$, ak je φ pravdiva v $\mathcal{M}$ pri kazdom ohodnoteni e. Potom piseme $\mathcal{M} \models \varphi$.
Ak je φ uzavrena formula, tak vravime ze φ je *pravdiva* v $\mathcal{M}$.
Formula sa nazyva *splnitelna*, ak je splnena v nejakej realizacii.
Formula je *logicky platna*, ak je splnena v kazdej realizacii jazyka L - $\models \varphi$
Formula φ, ψ su *logicky ekvivalentne* ak v lubovolnej realizacii $\mathcal{M}$ a pri lubovolnom ohodnoteni e je $\mathcal{M} \models \varphi[e]$ prave vtedy ak $\mathcal{M} \models \psi[e]$.

2.2 Substitucia termov za premenne

Ak je φ formula, x je premenna a t je term, potom vyraz ktory vznikne z formule φ nahradenim kazdeho volneho vyskytu premennej x termom t je opat formula.
Term t je *substituovatelny* za x do formule φ, ak ziadny volny vyskyt premennej x sa nenachadza v obore kvatifikacie nejakeho kvantifikatoru premennej y, kde y je premenna obsiahnuta v terme t.
Budeme znacit $\varphi_x[t]$ formulu, ktora vznikne z φ nahradenim kazdeho volneho vyskytu x termom t.
Ak mame φ, x, t a t je substituovatelny za x do φ, potom $(\forall x\varphi) \rightarrow \varphi_x[t]; \varphi_x[t] \rightarrow (\exists x\varphi)$ su logicky platne formule.

2.3 Formalny system predikatovej logiky

Zavedieme predikatovu logiku ako formalny axiomaticky system. Obmedzime sa len na logicke spojky $\neg, \rightarrow$ a kvantifikatoru $\forall$.
Schema vyrokovych axiomov

- $\varphi \rightarrow (\psi \rightarrow \varphi)$
- $(\varphi \rightarrow (\psi \rightarrow \eta)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \eta))$
- $(\neg\psi \rightarrow \neg\varphi) \rightarrow (\varphi \rightarrow \psi)$

Schema axiomu kvantifikatoru

- $(\forall x(\varphi \rightarrow \psi)) \rightarrow (\varphi \rightarrow (\forall x\psi))$ (x nema volny vyskyt v φ)

Schema axiomu substitucie t je substituovatelny za x do φ

- $(\forall x\varphi) \rightarrow \varphi_x[t]$

Schema axiomov rovnosti

- $x = x$
- $(x_1 = y_1 \rightarrow (x_2 = y_2 \rightarrow (...(x_n = y_n \rightarrow f(x_1, x_2, ..., x_n) = f(y_1, y_2, ..., y_n))...)))$
- $(x_1 = y_1 \rightarrow (x_2 = y_2 \rightarrow (...(x_n = y_n \rightarrow p(x_1, x_2, ..., x_n) \rightarrow p(y_1, y_2, ..., y_n))...)))$

2.4 Odvodzovacie pravidla predikatovej logiky

- **Pravidlo odlucenia - modus ponens** - Z formuli φ,$\varphi \rightarrow \psi$ sa odvodi formula ψ
- **Pravidlo zobecnenia - generalizacia** - Pre lubovolnu premennu x sa z formule φ odvodi formula $(\forall x\varphi)$

Dokaz - lubovolna postupnost $\varphi_1, ..., \varphi_n$ formuli jazyka L v ktorej pre kazdy index i je formula φ_i bud axiom predikatovej logiky alebo je ju mozne odvodit z niektorych predchadzajucich formuli pouzitim pravidla odlucenia alebo zobecnenia.
Formula φ je *dokazatelna*, pokial existuje dokaz, ktoreho poslednou formulou je φ. Piseme $\vdash \varphi$.
Bud T mnozina formuli jazyka L. Formula φ je *dokazatelna z predpokladov T*, ak existuje dokaz z predpokladu T, teda postupnost formuli, ze jej poslednou formulou je φ a kazda predosla formula je bud axiom, alebo je to formula z T alebo vznikla uzitim pravidla odlucenia alebo zobecnenia. Piseme $T \vdash \varphi$.
Lubovolna formula jazyka L dokazatelna v predikatovej logike 1. radu je logicky platnou tj. splnena v kazdej realizacii jazyka L.
Lemma - Ak $\vdash \varphi \rightarrow \psi$ a x nema volny vyskyt v φ, tak $\vdash \varphi \rightarrow (\forall x\psi)$
Lemma - Ak $\vdash \varphi \rightarrow \psi$ a x nema volny vyskyt v φ, tak $\vdash (\exists x\varphi) \rightarrow \psi$
Lemma - Ak φ je formula, x je premenna a t term substituovatelny za x do φ, tak $\vdash \varphi_x[t] \rightarrow (\exists x\varphi)$

Lemma - Nech φ' je instanciou formule (φ' je teda v tvare $\varphi_{x_1,...,x_n}[t_1,...,t_n]$). Ak $\vdash \varphi$, tak aj $\vdash \varphi'$.
Ak su $x_1,...,x_n$ vsetky volne premenne vo formuli φ, potom formulu $\forall x_1,...,x_n\varphi$ nazyvame *uzaverom formule* φ.
Veta o uzavere - Ak je T mnozina formuli a φ' uzaver formule φ, potom $T \vdash \varphi$ prave vtedy ked $T \vdash \varphi'$
Veta o dedukcii - Nech T je mnozina formuli jazyka L, nech φ je uzavrena formula, ψ je lubovolna formula jazyka L. Potom $T \vdash \varphi \to \psi$ prave vtedy ked $T \cup \varphi \vdash \psi$.
Veta o konstantach - Nech T je mnozina formuli jazyka L, nech φ je formula. Nech $x_1,...,x_n$ su premenne a nech $c_1,...,c_n$ su nove konstanty, ktorych priradenim k L vznikne jazyk L'. Potom $T \vdash \varphi_{x_1,...,x_n}[c_1,...,c_n]$, prave ked $T \vdash \varphi$.
Lemma - Nech je jazyk L s rovnostou

$$\vdash x = y \to y = x$$
$$\vdash x = y \to (y = z \to x = z)$$

Lemma - Ak je f funkcny symbol s pocetnostou n, ak je p predikatovy symbol s cetnostou m jazyka L a ak su $u, v, w, s_1,...,s_n, t_1,...,t_n$ termy jazyka L.

1. $\vdash u = u$
2. $\vdash u = v \to v = u$
3. $\vdash u = v \to (v = w \to u = w)$
4. $\vdash s_1 = t_1 \to (s_2 = t_2 \to ...(s_n = t_n \to f(s_1,...,s_n) = f(t_1,...,t_n))...))$
5. $\vdash s_1 = t_1 \to (s_2 = t_2 \to ...(s_n = t_n \to p(s_1,...,s_n) \to p(t_1,...,t_n))...))$

2.5 Prenexny tvar formuli

Formula A je v prenexnom tvare, pokial ma tvar $Q_1x_1...Q_nx_nB$, kde

1. $n \geq 0$ pre kazde $i = 1,...,n$ je Q_i bud $\forall$ alebo $\exists$
2. $x_1,...,x_n$ su navzajom rozne premenne
3. B je otvorena formula (neobsahuje kvantifikatory)

Prevod formuli do prenexneho tvaru

1. **Vylucenie zbytocnych kvantifikatorov** - vynechame kvantifikatory $\forall x$ a $\exists x$ v podformulach tvaru $\forall xB$ alebo $\exists xB$, pokial sa premenna x nevyskytuje volne v B
2. **Premenovanie premennych** - Postupujeme z lava do prava premenovavanim premennych v podformuliach
3. **Eliminacia spojky** $\leftrightarrow$ - Prevedieme pomocou

$$A \leftrightarrow B ... (A \to B) \wedge (B \to A)$$

4. **Presun negacie dovnutra** - vykonavame postupne nahrady podformuli podla schemat

$$\begin{aligned}
\neg(\forall x A) & ...(\exists x \neg A) \\
\neg(\exists x A) & ...(\forall x \neg A) \\
\neg(A \to B) & ...(A \wedge \neg B) \\
\neg(A \vee B) & ...(\neg A \wedge \neg B) \\
\neg(A \wedge B) & ...(\neg A \vee \neg B) \\
\neg(\neg A) & ...A
\end{aligned}$$

5. **Presun kvantifikatov dolava** - pre podformulu B, v ktorej sa nevyskytuje premenna x vykonavame nahrady podla schemat

$$\begin{aligned}
(QxA) \vee B & ...Qx(A \vee B) \\
(QxA) \wedge B & ...Qx(A \wedge B) \\
(QxA) \to B & ...\bar{Q}x(A \to B) \\
A \to (QxB) & ...Qx(A \to B)
\end{aligned}$$

2.6 Veta o uplnosti

Ak je jazyk L 1.radu a T mnozina formuli jazyka L, hovorime, ze T je *teoria 1. radu* s jazykom L.
Hovorime ze teoria T je *sporna*, pokial pre kazdu formulu φ jazyka L plati $T \vdash \varphi$. V opacnom pripade je *bezesporna*.
Nech T je mnozina formuli a φ' je uzaver formule φ. Potom $T \vdash \varphi$ prave vtedy, ked $T \cup \{\neg\varphi'\}$ je sporna teoria.
Bud T teoria s jazykom L a nech $\mathcal{M}$ je nejaka realizacia jazyka L. Hovorime ze $\mathcal{M}$ je *model teorie* T, pokial $\mathcal{M} \models \varphi$ pre kazdu formulu $\varphi \in T$. Potom piseme $\mathcal{M} \models T$.
Formula φ je *dosledkom toerie* T, pokial pre kazdy model $\mathcal{M}$ teorie T je $\mathcal{M} \models \varphi$. Piseme $T \models \varphi$.
Veta o korektnosti - Ak je T teoria s jazykom L a φ formula, taka, ze $T \vdash \varphi$, potom $T \models \varphi$.

3 Algebraicke struktury

Bud A mnozina $n \in \mathbb{N}_0$. Zobrazenie $\omega : A^n \to A$ sa nazyva *n-arna operacia* na A.

$$\omega : \begin{cases} A^n \to A \\ (x_1, ..., x_n) \mapsto \omega x_1, ..., x_n \end{cases}$$

Pre $n = 0$:

$$\omega : \begin{cases} A^0 = \{\varnothing\} \to A \\ \varnothing \mapsto \omega\varnothing = \omega \end{cases}$$

Binarne operacie ($n = 2$) znacime zvycajne nejakym symbolom $\circ$.

$$\circ : \begin{cases} A^2 \to A \\ (x, y) \mapsto x \circ y \end{cases}$$

Unarne operacie ($n = 1$)

$$\omega : \begin{cases} A \to A \\ x \mapsto \omega x \end{cases}$$

Bud A mnozina $n \in \mathbb{N}_0, D \subseteq A^n$. Potom zobrazenie $\omega : D \to A$ sa nazyva *n-arna parcialna operacia* na A. ($-, /$ na $\mathbb{N}$)
Bud A mnozina, I mnozina indexov. Pre $i \in I$ bud ω_i n_i-arnou operaciou na A, $n_i \in \mathbb{N}_0$. Potom $\mathcal{A} := (A, (\omega_i)_{i\in\{1,..,n\}})$ oznacuje *algebru s nosnou mnozinou A a suborom operacii* $(\omega_i)_{i\in I} =: \Omega$. Casto byva I konecna, potom piseme

$$(A, \Omega) = (A, (\omega_i)_{i\in I}) =: (A, \omega_1, ..., \omega_n)$$

Neutralny prvok - bud A mnozina, $\circ$ binarna operacia na A. Prvok $e \in A$ sa nazyva neutralny prvok vzhladom k $\circ :\Leftrightarrow \forall x \in A : e \circ x = x \circ e = x$ (moze byt aj lavy neutralny $e \circ x = x$, alebo aj pravy neutralny $x \circ e = x$)
Zakon - Rovnice, ktore maju tvar $t_1(x, y, z, ...) = t_2(x, y, z, ...)$ s vhodnymi termami t_1, t_2 a musia byt splnene pre vsetky prvky uvazovanej algebry
Inverzny prvok - bud A mnozina, $\circ$ binarna operacia na A, e neutralny prvok, $x \in A$. Potom nazyvame prvok $y \in A$ inverzny k prvku $x :\Leftrightarrow x \circ y = y \circ x = e$. (Moze byt aj lavy inverzny $y \circ x = e$, alebo aj pravy inverzny $x \circ y = e$.)
Asociativny zakon - bud A mnozina, $\circ$ binarna operacia na A, $\circ$ sa nazyva asociativna: $\Leftrightarrow \forall x, y, z \in A : (x \circ y) \circ z = x \circ (y \circ z)$. Pokial je operacia asociativna, existuje ku kazdemu prvku nanajvys 1 inverzny prvok.
Operacia s delenim - binarna operacia $\circ$ sa nazyva operacia s delenim: $\Leftrightarrow \forall (a, b) \in A^2 \exists (x, y) \in A^2 : a \circ x = b$(lavy zakon o deleni) $\wedge\, y \circ a = b$(pravy zakon o deleni).
Operacia s kratenim - binarna operacia $\circ$ sa nazyva operacia s kratenim na A: $\Leftrightarrow \forall a, x_1, x_2, y_1, y_2 \in A : (a \circ x_1 = a \circ x_2 \Rightarrow x_1 = x_2)$(lavy zakon o krateni) $\wedge\, (y_1 \circ a = y_2 \circ a \Rightarrow y_1 = y_2)$(pravy zakon o krateni)
Komutativny zakon - binarna operacia $\circ$ sa nazyva komutativna: $\Leftrightarrow \forall x, y \in A : x \circ y = y \circ x$
Distributivny zakon - pokial su $+, \cdot$ binarne operacie na A, potom sa $\cdot$ nazyva distributivna nad $+ :\Leftrightarrow \forall x, y, z \in A : x \cdot (y + z) = x \cdot y + x \cdot z \wedge (y + z) \cdot x = y \cdot x + z \cdot x$

3.1 Typy algebier

- **Grupoid** - algebra $(A, \cdot)$ typu (2)
- **Pologrupa** - grupoid $(H, \cdot)$ a $\cdot$ je asociativna operacia
- **Monoid** - pologrupa $(H, \cdot)$ a existuje neutralny prvok
- **Grupa** - monoid $(G, \cdot)$ pokial pre kazdy prvok z G existuje prvok inverzny

- **Komutativna/abelovska grupa** - grupa $(G, \cdot)$ (resp. $(G, \cdot, e, ^{-1})$) kde pre $\cdot$ plati komutativny zakon
- **Okruh** - algebra $(R, +, \cdot)$ (resp. $(R, +, 0, -, \cdot)$) typu (2,2) (resp. (2,0,1,2)) pokial
  - $(R, +)$ (resp. $(R, +, 0, -)$) je abelovska grupa
  - $(R, \cdot)$ je pologrupa
  - $\cdot$ je distributivny nad $+$
- **Okruh s jednotkovym prvkom** - algebra $(R, +, 0, -, \cdot, 1)$ typu (2,0,1,2,0) pokial
  - $(R, +, 0, -, \cdot)$ je okruh
  - 1 je neutralny prvok vzhladom k $\cdot$
- **Komutativny okruh** - pre $\cdot$ plati komutativita
- **Komutativny okruh s jednotkovym prvkom** - vyssie 2 dokopy
- **Obor integrity** - komutativny okruh s jednotkovym prvkom $(R, +, 0, -, \cdot, 1)$ pokial
  - $R \setminus \{0\} \neq \varnothing$ (teda $0 \neq 1$)
  - $\forall x, y \in R : x \neq 0 \wedge y \neq 0 \Rightarrow xy \neq 0$ (neexistuju delitele nuly)
- **Teleso** - okruh s jednotkovym prvkom $(R, +, 0, -, \cdot, 1)$ pokial
  - $0 \neq 1$
  - $(R \setminus \{0\}, \cdot)$ je grupa
- **Pole** - komutativne teleso ($(R \setminus \{0\}, \cdot)$ musi byt abelovska grupa)
- **Svaz** - algebra $(V, \cap, \cup)$ typu (2,2), ak $\forall a, b, c \in V$ plati
  - $a \cap b = b \cap a, a \cup b = b \cup a$
  - $a \cap (b \cap c) = (a \cap b) \cap c, a \cup (b \cup c) = (a \cup b) \cup c$
  - $a \cap (a \cup b) = a, a \cup (a \cap b) = a$
- **Distributivny svaz** - musi platit

$$a \cap (b \cup c) = (a \cap b) \cup (a \cap c), a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$$

- **Ohraniceny svaz**
  - **Nulovy prvok svazu** - $\forall a \in A : a \cup 0 = a$
  - **Jednotkovy prvok svazu** - $\forall a \in A : a \cap 1 = a$
- **Komplementarny ohraniceny svaz** - $\forall a \in A : a \cap a' = 0 \wedge a \cup a' = 1$, a' sa nazyva komplement prvku a. Nazyva sa aj **Booleovsky svaz**.

- **Booleova algebra** - ak je $(B, \cap, \cup, 0, 1)$ booleovsky svaz, tak $(B, \cap, \cup, 0, 1, ')$ je booleova algebra

- **Vektorovy priestor** - bud $(K, +, 0, -, \cdot, 1)$ pole, $I = \{a, b, c\} \cup K$, kde $a, b, c \notin K$, , a, b, c po dvoch rozne. Algebra $(V, (\omega_i)_{i \in I})$ typu (2,0,1,$(1)_{\lambda \in K}$) sa nazyva vektorovy priestor nad K, iff

  - $(V, \omega_a, \omega_b, \omega_c) =: (V, +, 0, -)$ je abelovska grupa
  -

$$\begin{aligned}
&\forall x, y \in V, \lambda, \mu \in K: \\
&\omega_\lambda(x + y) = \omega_\lambda(x) + \omega_\lambda(y) \\
&\omega_{\lambda+\mu}(x) = \omega_\lambda(x) + \omega_\mu(y) \\
&\omega_{\lambda\mu}(x) = \omega_\lambda(\omega_\mu(x)) \\
&\omega_1(x) = x
\end{aligned}$$

3.2 Zakladne pojmy teorie grup

Sucin - Bud $(G, \cdot)$ grupoid, $a_1, ..., a_n \in G (n \in \mathbb{N})$. *Sucin* $a_1, ..., a_n$ je definovany indukciou vztahom $a_1 ... a_n := (a_1 ... a_{n-1}) a_n$
Mocnina - Bud $(G, \cdot)$ grupoid, mocnina prvku a je definovana ako $a^1 := a, a^{n+1} := (a^n) a (n \in \mathbb{N})$
Bud $(G, \cdot, e, ^{-1})$ grupa, $a, b \in G$, potom plati $(ab)^{-1} = b^{-1} a^{-1}$
Bud $(G, \cdot, e, ^{-1})$ grupa, $a \in G$, potom plati $a^0 = e$ a $a^{-n} = (a^{-1})^n$
Pravidla pre pocitanie s mocninami v grupach

$$\begin{aligned}
a^n a^m &= a^{n+m} \\
(a^n)^m &= a^{nm} \\
(ab)^n &= a^n b^n \text{pokial je } \cdot \text{ komutativna}
\end{aligned}$$

Rad prvku - bud $(G, \cdot, e, ^{-1})$ grupa, $a \in G$, potom kardinalne cislo $o(a) = |\{a^0 = e, a^1, a^{-1}, a^2, a^{-2}, ...\}| = |\{a^k \mid k \in \mathbb{Z}\}|$ sa nazyva rad prvku a
Delenie so zvyskom - $\forall k, l \in \mathbb{Z}, l \neq 0, \exists q, r \in \mathbb{Z} : 0 \leq r < |l| \wedge k = lq + r$
Symetricka grupa - Bud M mnozina a $S_M = \{f : M \to M \mid f \text{bijektivne}\}$. $(S_M, \circ, id_M, ^{-1})$ je grupa, ktora sa nazyva symetricka grupa na M. Prvky mnoziny S_M sa nazyvaju permutacie mnoziny M. Ak $M = \{1, 2, ..., n\}$ tak piseme S_n. Napr

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

Cyklicky zapis:

$$S_3 = \{(1), (123), (132), (23), (13), (12)\}$$

3.3 Podalgebry

Uzavrena mnozina - Bud A mnozina, $\omega : A^n \to A$ n-arna operacia na A a $T \subseteq A$. T sa nazyva uzavrena vzhladom k $\omega \Leftrightarrow \omega(T^n) \subseteq T$ (tj $t_1...t_n \in T \Rightarrow \omega t_1...t_n \in T$)
Podalgebra - Bud $\mathcal{A} = (A, (\omega_i)_{i\in I})$ algebra typu $(n_i)_{i\in I})$, $T \subseteq A$. Mnozina T je uzavrena vzhladom k $(\omega_i)_{i\in I}$, iff je uzavrena voci ω_i pre kazde $i \in I$. Definujeme $\omega_i^* x_1...x_n = \omega_i x_1...x_n, (x_1, ..., x_n) \in T^n$ a mozme zapisat $\omega_i^* = \omega_i|T^{n_i}$ (zuzenie operacie ω_i na T^{n_i}). Algebra $(T, (\omega_i^*)_{i\in I})$ je potom podalgebra algebry $\mathcal{A}$.
Podpologrupa - Bud $(H, \cdot)$ pologrupa a $T \subseteq H$. Ak je mnozina T uzavrena voci $\cdot$, tak zavedieme $\cdot = \cdot|T \times T$ a $(T, \cdot)$ je podpologrupa grupy $(H, \cdot)$.
Subor podalgebier - Bud (A, Ω) algebra a $(T_j)_{j\in J}$ subor podalgebier. Potom je $\bigcap_{j\in J} T_j$ je tiez podalgebra.
Najmensia podalgebra algebry - Bud (A, Ω) algebra a $S \subseteq A$. Potom je

$$\langle S\rangle = \bigcap\{T \mid S \subseteq T, T \text{ je podalgebra algebry } (A, \Omega)\}$$

najmensia podalgebra algebry, ktora S obsahuje. $\langle S\rangle$ sa nazyva **podalgebra generovana mnozinou** S. S sa nazyva **system generatorov** podalgebry $\langle S\rangle$.
Cyklicka grupa - Grupa $(G, \cdot, e, ^{-1})$ je cyklicka $\Leftrightarrow \exists x \in G : G = \langle x\rangle$. Prvok x sa nazyva generator.

3.4 Relacia ekvivalencie a rozklad na triedy ekvivalencie

Binarna relacia - Ak je M mnozina, potom sa podmnozina R mnoziny $M \times M$ nazyva binarna relacia na M. Piseme $(x, y) \in R$ alebo xRy. Univerzalna relacia je pripad kedy $R = M \times M$. Identicka relacia je relacia $R = \{(x, x) \mid x \in M\}$.
Relacia $R \subseteq M \times M$ sa nazyva

- **reflexivna** - $\forall x \in M : (x, x) \in R$
- **symetricka** - $\forall x, y \in M : (x, y) \in R \Rightarrow (y, x) \in R$
- **antisymetricka** - $\forall x, y \in M : ((x, y) \in R) \wedge ((y, x) \in R) \Rightarrow x = y$
- **tranzitivna** - $\forall x, y, z \in M : ((x, y) \in R) \wedge (y, z) \in R)) \Rightarrow (x, z) \in R$

Ekvivalencia - relacia reflexivna, symetricka, tranzitivna
Usporiadanie - relacia reflexivna, antisymetricka, tranzitivna
Rozklad mnoziny - Bud M mnozina, $\mathcal{P} \subseteq 2^M$ sa nazyva rozklad mnoziny ak

- $\bigcup_{C\in\mathcal{P}} C = M$
- $\varnothing \notin \mathcal{P}$
- $A, B \in \mathcal{P} \Rightarrow (A = B) \vee (A \cap B = \varnothing)$

Faktorova mnozina - Bud π relacia ekvivalencie na mnozine M, $a \in M, [a]_\pi = \{b \in M \mid b\pi a\}$ tzv. trieda ekvivalencie prvku a. $M/\pi = \{[a]_\pi \mid a \in M\}$ tzv. faktorova mnozina mnoziny M podla ekvivalencie π. Potom M/π je rozklad mnoziny M na triedy ekvivalencie.

Nech su M, N mnoziny a $f : M \to N$. Nech je π_f relacia na M taka, ze $x\pi_f y \Leftrightarrow f(x) = f(y)$. Potom plati, ze

- π_f je relacia ekvivalencie na M, ktora sa nazyva $jadrof$
- Zobrazenie $M/\pi_f \to f(M) \subseteq N$ je definovane a bijektivne

Zobrazenie $\nu : M \to M/\pi_f$ sa nazyva *faktorove* zobrazenie

Bud $(G, \cdot, e, ^{-1})$ grupa a $(H, \cdot, e, ^{-1})$ podgrupa. Nech $\pi \subseteq G \times G$, pricom $x\pi y \Leftrightarrow x^{-1}y \in H$ kde $x, y \in G$. Relacia π je potom relacia ekvivalencie na G.
Bud $(G, \cdot, e, ^{-1})$ grupa, $A, B \subseteq G$. $AB = \{ab \mid a \in A \wedge b \in B\}$ sa nazyva **zlozeny sucin**. Specialne pripady $A = \{a\} : AB = aB = \{ab \mid b \in B\}$ (a analogicky pre $B = \{b\}$). Pre podgrupu H grupy G sa nazyva aH **lava trieda rozkladu grupy** G podla H a Ha **prava trieda rozkladu grupy** G podla H.
Rozklad grupy - $\{aH \mid a \in G\}$ - **lavy rozklad grupy** a analogicky pravy rozklad grupy

3.5 Izomorfizmy a homomorfizmy

Nech su algebry $\mathcal{A} = (A, (\omega_i)_{i\in I})$ a $\mathcal{A}^* = (A^*, (\omega_i^*)_{i\in I})$ rovnakeho typu. Zobrazenie $f : A \to A^*$ sa nazyva *homomorfizmus* algebty $\mathcal{A}$ do $\mathcal{A}^*$ $:\Leftrightarrow$

- Pre n-arne operacie $n \geq 1$ plati $\forall x_1, ..., x_n : f(\omega_i x_1...x_n) = \omega_i^* f(x_1)...f(x_n)$
- Pre nularne operacie $f(\omega_i) = \omega_i^*$

Linearne zobrazenie - nech su $\mathcal{V} = (V, +, 0, -, K)$ a $\mathcal{W} = (W, +, 0, -, K)$ vektorove priestory nad polom K. $f : V \to W$ je homomorfizmus $\mathcal{V}$ do $\mathcal{W} \Leftrightarrow f$ je linearne zobrazenie teda

- $f(x + y) = f(x) + f(y)$
- $f(\lambda x) = \lambda f(x)$

Typy homomorfizmov:

- **izomorfizmus** - pokial je f bijektivne
- **endomorfizmus** - pokial $\mathcal{A} = \mathcal{A}^*$
- **automorfizmus** - pokial $\mathcal{A} = \mathcal{A}^*$ a f je bijektivne
- **epimorfizmus** - pokial je f surjektivne
- **monomorfizmus** - pokial je f injektivne

3.6 Relacia kongruencie a faktorove algebry

Relacia kongruencie - Bud $\mathcal{A} = (A, (\omega_i)_{i \in I})$ algebra typu $(n_i)_{i \in I}$ a π relacia ekvivalencie na A. π sa nazyva relacia kongruencie $\Leftrightarrow$ pre vsetky $i \in I$,kde $n_i > 0 a_1, ..., a_{n_i}, b_1, ..., b_{n_i} \in A$ plati

$$a_1 \pi b_1 \wedge ... \wedge a_{n_i} \pi b_{n_i} \Rightarrow \omega_i a_1 ... a_{n_i} \pi \omega_i b_i ... b_{n_i}$$

Nech $\mathcal{A} = (A, (\omega_i)_{i \in I})$ je algebra a π kongruencia na $\mathcal{A}$. Potom su vztahmi

$$\omega_i^*[a_1]_\pi ... [a_n]_\pi = [\omega a_1 ... a_n]_\pi \text{ pre } n \geq 1$$

$$\omega_i^* = [\omega_i]_\pi \text{ pre } n = 0$$

definovane operacie $(\omega_i^*)_{i \in I}$ na faktorovej mnozine A/π
Faktorova algebra - Algebra $\mathcal{A}/\pi = (A/\pi, (\omega_i^*)_{i \in I})$ sa nazyva faktorova algebra algebry $\mathcal{A}$ podla kongruencie π. Napr ak $(\mathbb{Z}, +, 0, -, \cdot, 1)$ je algebra, a $\pi = \equiv \mod n$. Faktorova algebra je potom $(\mathbb{Z}_n, +^*, 0^*, -^*, \cdot^*, 1^*)$ - okruh zbytkovych tried modulo n

3.7 Relacia kongruencie na grupach a okruhoch

Bud $(G, \cdot, e, ^{-1})$ grupa π relacia ekvivalencie na G. Potom

- π je kongruencia na $(G, \cdot, e, ^{-1})$ iff je kongruencia na $(G, \cdot)$
- Ak je π kongruencia na G a $[e]_\pi = N$ potom
  - N je podgrupa G
  - $xNx^{-1} = \{xyx^{-1} \mid y \in N\} \subseteq N$
  - $x \pi y \Leftrightarrow x^{-1} y \in N$

Normalna podgrupa - N sa nazyva normalna podgrupa grupy G $(N \lhd G) \Leftrightarrow \forall x \in G :$ $xNx^{-1} \subseteq N$
Ideal - Bud $(R, +, 0, -, \cdot)$ okruh a I polokruh. Potom I sa nazyva

- Lavy ideal okruhu $R \Leftrightarrow \forall r \in R : rI = \{ri \mid \ \in I\} \subseteq I$
- Pravy ideal okruhu $R \Leftrightarrow \forall r \in R : Ir = \{ir \mid \ \in I\} \subseteq I$
- Ideal $I \lhd R \Leftrightarrow \forall r \in R : rI \subseteq I \wedge Ir \subseteq I$

3.8 Priame suciny algebier

Nech su $\mathcal{A}_k = (A_k, (\omega_i^{(k)})_{i \in I)}), k \in K$ algebry rovnakeho typu, potom

$$A = \prod_{k \in K} A_k = \{(a_k)_{k \in K} \mid a_k \in K\}$$

Kartezsky sucin vsetkych A_k. Operacie sa vytvaraju ako nove operacie, ktore operuju nad relaciou.

4 Polynomy

Polynom – Bud $(R, +, 0, -, \cdot, 1)$ komutativny okruh s jednotkovym prvkom. Vyraz tvaru $\sum a_k x^k$, kde $a_k \in R$ sa nazyva polynom
Stupen polynomu – maximalna mocnina n polynomu (grad$p(x)$)

5 Metricke priestory

Metricky priestor – dvojica $\chi = (X, \varrho)$, kde X je mnozina ktorej prvy nazyva **body** a ϱ je nezaporna realna funkcia $\varrho(x, y)$ ktoru nazyvame **metrika** ($\varrho : X \times X \to \mathbb{R}_0^+$), ktora splnuje 3 podmienky

- $\forall x, y \in X : \varrho(x, y) = 0 \Leftrightarrow x = y$
- $\forall x, y \in X : \varrho(x, y) = \varrho(y, x)$
- $\forall x, y \in X : \varrho(x, y) + \varrho(y, z) \geq \varrho(x, z)$

Diskretny metricky priestor

$$\varrho(x, y) = \begin{cases} 0 & x = y \\ 1 & x \neq y \end{cases}$$

Metricky priestor $\mathbb{R}^1$

$$\varrho(x, y) = |x - y|$$

Metricky priestor $\mathbb{R}^n$

$$x = (x_1, x_2, ..., x_n)$$

$$\varrho(x, y) = \sqrt{\sum (y_k - x_k)^2}$$

Metricky priestor $\mathbb{R}_1^n$

$$x = (x_1, x_2, ..., x_n)$$

$$\varrho(x, y) = \sum |y_k - x_k|$$

Metricky priestor $\mathbb{R}_0^n$

$$x = (x_1, x_2, ..., x_n)$$

$$\varrho(x, y) = \max |y_k - x_k|$$

Metricky priestor $C(\langle a, b\rangle)$ – vsetky spojite realne funkcie definovane na intervale $\langle a, b\rangle$

$$\varrho(f, g) = \max |g(t) - f(t)|$$

Otvorena gula $S(x_0, r)$ v metrickom priestore χ – mnozina bodov x pre ktore plati

$$\varrho(x, x_0) < r$$

Uzavreta gula $S[x_0, r]$

$$\varrho(x, x_0) \leq r$$

5.1 Linearne normovane priestory

Nech $\mathcal{L}$ je neprazdna mnozina prvkov $x, y, z, ...$ a nech su splnene tieto podmienky

- $\mathcal{L}$ je komutativna grupa (asociatvita, neutralny prvok θ, inverzne prvky $-x$, komutativita)
- Ku kazdemu cislu α nejakeho telesa T a ku kazdemu prvku $x \in \mathcal{L}$ je jednoznacne priradeny prvok $\alpha x \in \mathcal{L}$) pricom plati
  - $(\alpha\beta)x = \alpha(\beta x)$
  - $1.x = x$
- Obe operacie su zviazane distribucnymi zakonmi
  - $(\alpha + \beta)x = \alpha x + \beta x$
  - $\alpha(x + y) = \alpha x + \alpha y$

Mnozinu $\mathcal{L}$ potom nazyva **linearnym/vektorovym priestorom nad telesom** T. Prvky T $\alpha, \beta, ...$ nazyvame **skalary**. Prvky $\mathcal{L}$ $x, y, ...$ nazyvame **vektormi**.
Linearny priestor $\mathcal{L}$ sa nazyva **normovany** ak kazdemu prvku $x \in \mathcal{L}$ je priradene nezaporne cislo $||x||$, ktore sa nazyva **norma k prvku** x, pricom pre kazde $x, y \in \mathcal{L}$ a $\alpha \in T$ plati

- $||x|| = 0 \Leftrightarrow x = \theta$
- $||\alpha x|| = |\alpha|.||x||$
- $||x + y|| \leq ||x|| + ||y||$

Norma v $\mathbb{R}^1$

$$||x|| = |x|$$

Norma v $\mathbb{R}^n$

$$||x||_2 = \sqrt{\sum x_k^2}$$
$$||x||_1 = \sum |x_k|$$
$$||x||_0 = \max |x_k|$$

Norma v $\mathbb{C}^n$

$$||x||_2 = \sqrt{\sum |x_k|^2}$$

Vseobecny vztah pre normu v n-rozmernom linearnom priestore

$$||x||_p = (\sum |x_k|^p)^{\frac{1}{p}}$$

Norma v $C\langle a,b\rangle$

$$||f|| = \max|f(t)|$$
$$||f|| = \sqrt{\int_a^b [f(t)]^2 dt}$$

Linearna zavislost – mnozina vektorov $\{x_1, x_2, ..., x_n\}$ sa nazyva linearne zavisla, pokial existuju take konstanty $\alpha_1, \alpha_2, ..., \alpha_n$, z ktorych aspon 1 je nenulova, ze

$$\alpha_1 x_1 + \alpha_2 x_2 + ... + \alpha_n x_n = \theta$$

V opacnom pripade sa nazyva linearne nezavisla
Linearna kombinacia – lin. kombinacia $x_1, x_2, ..., x_n$ je vyraz $\alpha_1 x_1 + \alpha_2 x_2 + ... + \alpha_n x_n$
Dimenzia – pokial v priestore $\mathcal{L}$ vieme najst n lin. nezavislich vektorov, ale u $n+1$ su uz vsetky linearne zavisle, tak vravime ze priestor ma dimenziu n
Baza – V n rozmernom priestore sa lubovolny system n linearne nezavislych vektorov nazyva **baza**
Skalarny sucin – zobrazenie $(-,-) : R \times R \to \mathbb{R}$

- $(x, y) = (y, x)$
- $(x_1 + x_2, y) = (x_1, y) + (x_2, y)$
- $(\lambda x, y) = \lambda(x, y)$
- $(x, x) \geq 0$ pricom $(x, x) = 0$ len ak $x = \theta$

Unitarny priestor – linearny priestor v ktorom je definovany skalarny sucin, norma sa v nom zavadza ako
$$||x|| = \sqrt{(x, x)}$$

Kosinus uhlu dvoch nenulovych vektorov

$$cos\varphi = \frac{(x, y)}{||x||.||y||}$$

Ortogonalne vektory – Pokial $(x, y) = 0$ tak dostavame $\varphi = \frac{\pi}{2}$ a take vektory nazyvame **ortogonalne**
Ortogonalna sustava – Mnozina vektorov $\{x_\alpha\}$, kde $(x_\alpha, x_\beta) = 0$ pre $\alpha \neq \beta$
Ortonormalna sustava
$$(x_\alpha, x_\beta) = \begin{cases} 0 & \alpha \neq \beta \\ 1 & \alpha = \beta \end{cases}$$
Ak je $\{x_\alpha\}$ ortogonalna sustava, tak $\{x_\alpha/||x_\alpha||\}$ je ortonormalna sustava
Skalarny sucin v $\mathbb{R}^n$
$$(x, y) = \sum x_i y_i$$

Skalarny sucin v $C\langle a,b\rangle$
$$(f, g) = \int_a^b f(t)g(t)dt$$

Schmidtova veta o ortogonalizacii
Nech $f_1, f_2, ..., f_n, ...$ je linearne nezavisly system prvkov v unitarnom priestore, potom v tomto priestore existuje system prvkov $\varphi_1, \varphi_2, ..., \varphi_n, ...$, ktory splnuje tieto podmienky

- Tento system je ortonormalny
- Kazdy prvok φ_n je linearnou kombinaciou prvkov $f_1, f_2, ..., f_n$

$$\varphi_n = a_{n1} f_1 + ... + a_{nn} f_n$$

- Kazdy prvok f_n mozno vyjadrit v tvare

$$f_n = b_{n1} \varphi_1 + ... + b_{nn} \varphi_n$$

Dokaz

- $\varphi_1 = a_{11} f_1 = \frac{f_1}{||f_1||}$
- $a_{11} = \frac{1}{b_{11}} = \frac{1}{\sqrt{(f_1, f_1)}} = \frac{1}{||f_1||}$
- $h_n = f_n - b_{n1}\varphi_1 - ... - b_{nn-1}\varphi_{n-1}$
- $\varphi_n = \frac{h_n}{||h_n||}$