MATEMATICKÁ LOGIKA A DISKRÉTNE ŠTRUKTÚRY

MARTIN KNOR

S T U

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE

Recenzenti: RNDr. Tomáš Madaras, PhD.
Doc. RNDr. Ľudovít Niepl, CSc.

Schválilo vedenie Stavebnej fakulty STU v Bratislave dňa 2. 3. 2007 pre študijné programy
Matematicko-počítačové modelovanie.

http://www.svf.stuba.sk
ISBN 978-80-227-2837-9

Doc. RNDr. Martin Knor, PhD.

MATEMATICKÁ LOGIKA A DISKRÉTNE ŠTRUKTÚRY

Vydala Slovenská technická univerzita v Bratislave vo Vydavateľstve STU,
Bratislava, Vazovova 5, v roku 2008.

Edícia skrípt

Rozsah 95 strán, 7 obrázkov, 8 tabuliek, 6,427 AH, 6,588 VH, 1. vydanie,
edičné číslo 5358. Vydané v elektronickej forme, umiestnenie skrípt na http://www.svf.stuba.sk.

85 – 223 – 2008

http://www.svf.stuba.sk
ISBN 978-80-227-2837-9

MATEMATICKÁ LOGIKA

A

DISKRÉTNE ŠTRUKTÚRY

MARTIN KNOR

Predhovor

Tento učebný text je určený študentom prvého ročníka stavebnej fakulty Slovenskej technickej univerzity, študujúcim na zameraní Matematické a počítačové modelovanie. Predstavuje spísané a po formálnej stránke značne rozšírené prednášky z predmetu „Matematická logika a diskrétne štruktúry“.

Štruktúra tohoto textu je upravená tak, že každá kapitola tvorí jednu prednášku. Čitateľovi predkladáme 11 kapitol, čo je podľa našich skúseností maximálny možný počet prednášok, ktorý sa dá stihnúť počas 13-týždňového semestra. Keďže v „zlých rokoch“ sa často nestihne ani 11 prednášok, tak za pomoci tejto učebnice si študenti môžu doplniť svoje vedomosti samoštúdiom.

Po obsahovej stránke možno obsah tohoto textu rozdeliť na tri rôzne veľké časti, z ktorých každá sa venuje inej matematickej disciplíne.

Prvá časť sa zaoberá matematickou logikou. Kapitoly 1 až 3 sa venujú výrokovej logike, čiže tautológiám a formuliam dokázateľným pomocou troch axióm a jedného odvodzovacieho pravidla (modus ponens). V tretej kapitole dokážeme, že dokázateľné sú práve tie formuly, ktoré sú tautológiami. Nasledujú dve kapitoly venované predikátovej logike. Štvrtá kapitola sa zaoberá všeobecne platnými formulami, zatiaľ čo v piatej popisujeme dokázateľné formuly. Táto časť je ukončená jednou veľmi peknou aplikáciou predikátovej logiky v teórii grafov.

Druhú časť, venovanú teórii množín, tvorí jediná kapitola. Uvádzame tu základné pojmy intuitívnej teórie množín, pričom po formálnej stránke si pomáhame formulami predikátovej logiky. Spomenieme tu asociatívny, komutatívny, distributívny a niektoré iné zákony, s ktorými sa stretávame v nasledujúcich kapitolách.

Nasleduje časť venovaná štrukturálnej algebre. V kapitolách 7 a 8 sa zaoberáme grupami, v kapitolách 9 a 10 poľami a v kapitole 11 zväzmi. Spomenieme tu charakterizáciu konečných komutatívnych grúp, popíšeme vytvorenie Galoisovho poľa a v jedenástej kapitole sa pomocou Booleových algebier opäť vrátime k výrokovej logike a k tautológiám.

Ako vidno z predchádzajúceho, predmet „Matematická logika a diskrétne štruktúry“ má veľmi široký záber. Predstavuje úvod do niekoľkých (minimálne troch) matematických disciplín. To nás postavilo pred dva problémy. Ten prvý je záplava definícií, ktoré sú nutné na exaktné vybudovanie základov v každej oblasti matematiky. Tento problém sme riešili tým spôsobom, že definujeme len to, čo v ďalšom nevyhnutne potrebujeme. Napriek tomu tvorí Index asi 4 percentá textu. Druhý problém bolo zladenie textu po formálnej stránke. Potrebovali sme, aby slovník, členenie na stránke aj argumentácia, boli podobné vo všetkých kapitolách. Kvôli tomu sme upravovali najmä dôkazy v algebre. Podriadili sme ich štýlu, akým sa prezentuje výroková logika. Dúfame, že sa nám takto podarilo vytvoriť relatívne homogénnu učebnicu, v ktorej sa budú študenti dobre orientovať.

Záverom tohoto úvodu chcem poďakovať recenzentom, Doc. RNDr. Ľudovítovi Nieplovi, CSc. a RNDr. Tomášovi Madarasovi, PhD., za pripomienky, ktorými zlepšili čitateľnosť textu. Tiež chcem poďakovať Mgr. Gabriele Kubičkovej za jazykovú úpravu.

Autor

1 VÝROKOVÁ LOGIKA 1

Logické paradoxy

Pred 2000 rokmi zaskočil Kréťan Epimenides svojich učených kolegov touto otázkou. Čo možno súdiť o platnosti tvrdenia:

Čo hovorí Kréťan je lož. (1)

Ak je tvrdenie (1) pravdivé, tak ja som Kréťan a teda tiež klamem. Preto (1) neplatí.

Ak je tvrdenie (1) nepravdivé, tak potom nie je pravda, že čo hovorí Kréťan je lož. Preto Kréťan hovorí pravdu a keďže ja som Kréťan tvrdiaci (1), tak (1) platí.

Obdobný problém by sme mali, keby sme chceli určiť pravdivosť tvrdenia:

Táto veta neplatí.

Výrokové formuly

Vyššie spomenuté paradoxy ťažia z bohatosti nášho jazyka – máme rovnaké pojmy pre rôzne skutočnosti a naopak. Preto je mimoriadne užitočné zaviesť formálny, umelý jazyk, dovoľujúci pomerne dobre obsiahnuť skutočnosť, ktorý sa vyhýba rozporom. Takýto jazyk zaviedli lekári, chemici a vlastne všetci vedci, ktorí sa potrebujú presne vyjadrovať. Potrebujeme tiež poznať isté základné tvrdenia v danom jazyku, o ktorých pravdivosti nebudeme nikdy pochybovať, akési základné kamene našej teórie. Do tretice, potrebujeme poznať pravidlá, pomocou ktorých z už platných tvrdení budeme schopní odvodiť nové tvrdenia v našom jazyku.

Teda vo všeobecnosti, pre ľubovoľnú matematickú teóriu potrebujeme poznať:

1. Jazyk, v ktorom sa formulujú vety a v ktorom prebiehajú dôkazy.
2. Axiómy – tvrdenia predstavujúce základné vety v danom jazyku.
3. Odvodzovacie pravidlá – syntaktické pravidlá dovoľujúce z niekoľkých viet odvodiť novú vetu.

V prvých troch statiach tejto učebnice sa zaoberáme výrokovou logikou, ktorá má v matematike veľmi špeciálne postavenie. Ide o časť matematiky, ktorá je obsiahnutá v podstate vo všetkých matematických disciplínach. To znamená, že jazyk, axiómy aj odvodzovacie pravidlá ľubovoľnej matematickej disciplíny obsahujú v sebe jazyk, axiómy a odvodzovacie pravidlá výrokovej logiky.

Čo to však výroková logika je a čo je to výrok? Uvažujme vety:

Nespím.
Ak študent zaspáva, tak prednáška je zlá. (2)
Dobrý deň.
Pomóc!

Prvé dve vety sú výroky, zatiaľ čo posledné dve výroky nie sú. To preto, lebo výrok bude veta, o pravdivosti ktorej má zmysel uvažovať. Nás však nebude zaujímať, či daný výrok platí alebo neplatí takto priamo. Bude nás zaujímať, čo môžeme povedať o pravdivosti celého výroku, ak poznáme pravdivostnú hodnotu jeho podvýrokov (prvotných formúl), z ktorých sa skladá. Teda ak študent nespí a prednáška je zlá, čo môžeme povedať o pravdivosti výroku (2)? Budú nás teda zaujímať takzvané výrokové formuly – schémy súvetí, do ktorých možno dosadzovať tvrdenia za prvotné výroky.

Definícia. **Výroková formula** s množinou prvotných formúl P vznikne ak použijeme konečne veľakrát nasledujúce pravidlá:

(a) Každá prvotná formula p z množiny P je výroková formula.
(b) Ak sú A a B formuly, tak $(\neg A)$, $(A \,\&\, B)$, $(A \vee B)$, $(A \Rightarrow B)$ a $(A \Leftrightarrow B)$ sú výrokové formuly.

Príklad. $(p\Rightarrow)$ ani $\neg\Rightarrow p$ nie sú formuly, ale $((p \,\&\, q) \Rightarrow (\neg(p) \vee q))$ je formula.

Poznámka 1. Symbol $\neg$ je symbolom negácie, $\&$ konjunkcie, $\vee$ disjunkcie, $\Rightarrow$ implikácie a $\Leftrightarrow$ ekvivalencie.

Poznámka 2. Keď hovoríme o výrokoch, tak pod pojmom formula rozumieme vždy výrokovú formulu.

Dohoda. Posledné vonkajšie zátvorky budeme pri formulách vždy vynechávať, teda namiesto $((A\Rightarrow B)\vee C)$ budeme písať len $(A\Rightarrow B)\vee C$. Budeme tiež vynechávať vonkajšie zátvorky pri negáciách, čiže namiesto $((\neg A)\Rightarrow(\neg(\neg B)))\Rightarrow C$ budeme písať $(\neg A\Rightarrow\neg\neg B)\Rightarrow C$. To preto, lebo negácia má najvyššiu prioritu, čiže ak by sme mali viac možností, tak vždy aplikujeme najprv negáciu.

Teraz už môžeme povedať, čo je to výroková logika. Je to matematická disciplína, ktorej predmetom skúmania sú výrokové formuly. Pritom najviac nás bude zaujímať, kedy sú tieto formuly „dobré“ (pravdivé).

Tautológie

V tejto časti budeme skúmať výroky tým spôsobom, na ktorý sme si zvykli na strednej škole. Budeme skúmať ohodnotenia formúl výrokového počtu, pričom opäť nás bude zaujímať súvis medzi pravdivostnou hodnotou celej formuly a jej jednoduchších zložiek.

DEFINÍCIA. **Pravdivostné ohodnotenie** množiny P prvotných formúl je ľubovoľné zobrazenie ν množiny P do množiny $\{0,1\}$ (lož, pravda). Prvotná formula p je **pravdivá** pri ohodnotení ν ak $\nu(p)=1$.

Ak poznáme $\nu(A)$ a $\nu(B)$, čo vieme povedať o $\nu(\neg A)$, alebo $\nu(A \Rightarrow B)$ a podobne? Na to nám slúžia pravdivostné tabuľky:

A	$\neg A$
0	1
1	0

čítame

ak $\nu(A)=0$, tak $\nu(\neg A)=1$
ak $\nu(A)=1$, tak $\nu(\neg A)=0$

Podobný význam má nasledujúca tabuľka:

A	B	$A \,\&\, B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

Pomocou týchto tabuliek možno rozšíriť pravdivostné ohodnotenie prvotných formúl a vyhodnotiť všetky formuly.

DEFINÍCIA. Nech je ν ohodnotenie množiny prvotných formúl P a $\overline{\nu}$ je jeho rozšírenie na množinu všetkých výrokových formúl uvažovaného jazyka. Potom A je **pravdivá pri ohodnotení** ν (respektíve $\overline{\nu}$) ak $\overline{\nu}(A)=1$.

Je zrejmé, že rozšírenie $\overline{\nu}$ je definované jednoznačne. Teda ak máme dve ohodnotenia prvotných formúl ν a μ, pre ktoré $\nu(p)=\mu(p)$ pre každé $p \in P$, tak aj $\overline{\nu}(A)=\overline{\mu}(A)$ pre ľubovoľnú formulu A, ktorej prvotné formuly sú z P.

PRÍKLAD. Skúmajme pravdivostné hodnoty formúl $\neg(A \vee B)$ a $\neg A \,\&\, \neg B$. Pri vyhodnocovaní pravdivostného ohodnotenia týchto formúl budeme vlastne postupovať induktívne podľa ich konštrukcie. Postup je zachytený v nasledujúcej tabuľke:

A	B	$A \vee B$	$\neg(A \vee B)$	$\neg A$	$\neg B$	$\neg A \;\&\; \neg B$
0	0	0	1	1	1	1
0	1	1	0	1	0	0
1	0	1	0	0	1	0
1	1	1	0	0	0	0

Vidíme, že ohodnotenia formúl $\neg(A \vee B)$ a $\neg A \,\&\, \neg B$ sú vždy rovnaké a teda podľa tabuľky pre ekvivalenciu vždy platí $\neg(A \vee B) \Leftrightarrow (\neg A \,\&\, \neg B)$. Takéto vždy platné formuly sú vo výrokovej logike zvlášť dôležité.

DEFINÍCIA. **Tautológia** je výroková formula, ktorej ohodnotenie je vždy 1, nezávisle od ohodnotenia prvotných formúl, zatiaľ čo **kontradikcia** je taká formula, ktorej ohodnotenie je vždy 0, nezávisle od ohodnotenia prvotných formúl. Skutočnosť, že A je tautológia, zapisujeme $\models A$, pričom ak A nie je tautológia, tak píšeme $\not\models A$.

PRÍKLAD. Tautológia je napríklad $A \vee \neg A$, zatiaľ čo $A \,\&\, \neg A$ je kontradikcia.

POZNÁMKA. Všimnime si, že ak $\not\models A$, tak A ešte nemusí byť kontradikcia.

Na tomto mieste zdôraznime, že na zistenie, či formula je, alebo nie je tautológia, používame pravdivostné tabuľky.

DEFINÍCIA. Formuly A a B nazývame **ekvivalentnými**, ak nie sú od seba odlíšiteľné pomocou žiadneho ohodnotenia prvotných formúl, teda ak pre ľubovoľné pravdivostné ohodnotenie ν platí $\overline{\nu}(A) = \overline{\nu}(B)$. Zapisujeme $\models A \Leftrightarrow B$ (overte si, že ide naozaj o tautológiu).

Zamyslime sa nad tým, čo vlastne zapisujeme do pravdivostných tabuliek. Možno pozorovať, že logické spojky (symboly $\neg$, $\&$, $\vee$, $\Rightarrow$ a $\Leftrightarrow$) sú vlastne funkcie, ktoré nadobúdajú hodnotu 0, alebo 1, podľa pravdivostnej hodnoty argumentov.

DEFINÍCIA. **Booleova funkcia n argumentov** je zobrazenie $\{0,1\}^n \to \{0,1\}$.

POZNÁMKA 1. $\neg$ je Booleova funkcia jedného argumentu, zatiaľ čo $\&$, $\vee$, $\Rightarrow$ a $\Leftrightarrow$ sú Booleove funkcie dvoch argumentov.

POZNÁMKA 2. Presnú definíciu zobrazenia (funkcie) uvedieme v časti zaoberajúcej sa množinami. Zatiaľ tento pojem chápme intuitívne, v zmysle nasledujúcich príkladov.

PRÍKLAD. Booleove funkcie môžeme opäť zadať pomocou pravdivostných tabuliek. Ako príklad uvádzame funkcie Nor a Nand (funkcia Nor je tzv. Pierceova funkcia a Nand je Shefferova funkcia):

A	B	$A \,\mathrm{Nor}\, B$	$A \,\mathrm{Nand}\, B$
0	0	1	1
0	1	0	1
1	0	0	1
1	1	0	0

Zjavne existujú $(2^1)^2 = 4$ Booleove funkcie jedného argumentu, $(2^2)^2 = 16$ Booleových funkcií dvoch argumentov, $(2^3)^2 = 64$ Booleovych funkcií troch argumentov atď.

DEFINÍCIA. Výroková formula je v **disjunktívnom normálnom tvare**, ak je disjunkciou niekoľkých formúl (disjunktov), o ktorých platí:

(a) každá je konjunkciou konečne veľa prvotných formúl, prípadne ich negácií;
(b) v žiadnej sa nevyskytuje súčasne prvotná formula aj jej negácia;
(c) ak sa naviac v každej formuli vyskytujú všetky prvotné formuly, potom je formula v **úplnom disjunktívnom normálnom tvare**.

PRÍKLAD. Majme formulu f s množinou prvotných formúl $\{a, b, c\}$, o ktorej vieme:

a	b	c	f
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

Potom f je ekvivalentná s nasledujúcou formulou v úplnom disjunktívnom normálnom tvare:

$$(\neg a \,\&\, b \,\&\, c) \vee (a \,\&\, \neg b \,\&\, c) \vee (a \,\&\, b \,\&\, \neg c)$$

DOHODA. Budeme používať skrátený zápis $\bigvee_{i=1}^{n} T_i$ pre $T_1 \vee T_2 \vee \cdots \vee T_n$ a $\&_{i=1}^{n} T_i$ pre $T_1 \,\&\, T_2 \,\&\, \ldots \,\&\, T_n$.

VETA 1.1. *Každá výroková formula, ktorá nie je kontradikcia, je ekvivalentná istej formule v úplnom disjunktívnom normálnom tvare.*

DÔKAZ. Budeme postupovať tak, ako v príklade pred vetou. Nech je A formula výrokovej logiky, v ktorej vystupujú len prvotné formuly $p_1, p_2, \ldots, p_n$. Zostrojme pravdivostnú tabuľku pre A v závislosti od ohodnotenia prvkov $p_1, p_2, \ldots, p_n$. Booleovu funkciu popísanú touto tabuľkou označme $f_A(x_1, x_2, \ldots, x_n)$, pričom argument x_i zodpovedá prvotnej formule p_i. Teda $x_i = 1$ ak $\nu(p_i) = 1$ a $x_i = 0$ ak $\nu(p_i) = 0$.

Teraz pre $x_i \in \{0, 1\}$ definujme

$$p_i^{x_i} = \begin{cases} p_i & \text{ak} \quad x_i = 1, \\ \neg p_i & \text{ak} \quad x_i = 0. \end{cases}$$

Potom pre ľubovoľné ohodnotenie výrokových premenných ν platí

$$\overline{\nu}(p_i^{x_i}) = 1 \quad \text{práve vtedy, keď} \quad \nu(p_i) = x_i. \tag{3}$$

Totiž ak $x_i = 1$, tak (2) tvrdí: $\overline{\nu}(p_i) = 1$ práve vtedy, keď $\nu(p_i) = 1$; a keď $x_i = 0$, tak (2) tvrdí: $\overline{\nu}(\neg p_i) = 1$ práve vtedy, keď $\nu(p_i) = 0$. Je zrejmé, že tieto tvrdenia (pre $x_i = 1$, aj $x_i = 0$) sú pravdivé a preto (3) platí.

V ďalšom dokážeme, že

$$B = \bigvee_{f_A(x_1,\ldots,x_n)=1} (p_1^{x_1} \,\&\, p_2^{x_2} \,\&\, \ldots \,\&\, p_n^{x_n})$$

je hľadané vyjadrenie f_A v úplnom disjunktívnom normálnom tvare. (Na ujasnenie, disjunkcia ide cez všetky tie ohodnotenia $x_1, x_2, \ldots, x_n$ výrokových premenných, pre ktoré $f_A(x_1, x_2, \ldots, x_n) = 1$.)

Ak $\overline{\nu}(A) = 1$, tak $f_A(\nu(p_1), \nu(p_2), \ldots, \nu(p_n)) = 1$ a jeden z disjunktov z B má tvar $p_1^{\nu(p_1)} \,\&\, p_2^{\nu(p_2)} \,\&\, \ldots \,\&\, p_n^{\nu(p_n)}$. Potom pre $i = 1, 2, \ldots, n$ platí $\overline{\nu}(p_i^{\nu(p_i)}) = 1$ podľa (3). Preto $\overline{\nu}(p_1^{\nu(p_1)} \,\&\, p_2^{\nu(p_2)} \,\&\, \ldots \,\&\, p_n^{\nu(p_n)}) = 1$ a aj $\overline{\nu}(B) = 1$.

Naopak, ak $\overline{\nu}(B) = 1$, tak $\overline{\nu}(p_1^{x_1} \,\&\, p_2^{x_2} \,\&\, \ldots \,\&\, p_n^{x_n}) = 1$ platí pre aspoň jeden disjunkt z B a pre $x_1, x_2, \ldots, x_n$ z tohoto disjunktu potom $f_A(x_1, x_2, \ldots, x_n) = 1$. Keďže $\overline{\nu}(p_1^{x_1} \,\&\, p_2^{x_2} \,\&\, \ldots \,\&\, p_n^{x_n}) = 1$, tak $\overline{\nu}(p_i^{x_i}) = 1$ pre $i = 1, 2, \ldots, n$ a $\nu(p_i) = x_i$ podľa (3). Preto $f_A(\nu(p_1), \nu(p_2), \ldots, \nu(p_n)) = 1$, čiže $\overline{\nu}(A) = 1$. □

Predpoklad „A nie je kontradikcia“ bol v predošlom dôkaze nutný. Zistite, kde sme ho využili.

Definícia. Výroková formula je v **konjunktívnom normálnom tvare**, ak je konjunkciou niekoľkých formúl o ktorých platí:

(a) Každá je disjunkciou konečne veľa prvotných formúl, prípadne ich negácií.
(b) V žiadnej sa nevyskytuje súčasne prvotná formula aj jej negácia.

Keďže $\vDash \neg(A \vee B) \Leftrightarrow (\neg A \,\&\, \neg B)$ a tiež $\vDash \neg(A \,\&\, B) \Leftrightarrow (\neg A \vee \neg B)$, tak $\neg(\bigvee_{i\in I}(\,\&_{j\in J} A_{i,j})) \Leftrightarrow \,\&_{i\in I} \neg(\,\&_{j\in J} A_{i,j}) \Leftrightarrow \,\&_{i\in I}(\bigvee_{j\in J} \neg A_{i,j})$. Preto platí nasledujúci dôsledok Vety 1.1:

Dôsledok. *Každá výroková formula, ktorá nie je tautológia, je ekvivalentná istej formule v konjunktívnom normálnom tvare.*

Poznámka. Úvahy pred dôsledkom dávajú aj možný návod na to, ako vytvoriť formulu v konjunktívnom normálnom tvare pre danú formulu A. Najprv vytvoríme formulu v disjunktívnom normálnom tvare ekvivalentnú s $\neg A$ a túto potom znegovaním prevedieme na formulu v konjunktívnom normálnom tvare ekvivalentnú s A.

Definícia. Nech je S množina logických spojok. Ak k ľubovoľnej formule A možno nájsť takú formulu ekvivalentnú s A, ktorá využíva len spojky z S a prvotné formuly vyskytujúce sa v A, tak S je **funkčne úplná množina logických spojok**.

Ako sme ukázali vo Vete 1.1 a jej dôsledku, $\{\neg, \,\&\, , \vee\}$ je funkčne úplná množina spojok. Avšak funkčne úplné množiny spojok sú aj množiny $\{\neg, \,\&\,\}$, $\{\neg, \Rightarrow\}$, $\{\,\mathrm{Nor}\,\}$, $\{\,\mathrm{Nand}\,\}$ a podobne.

Cvičenia

Cvičenie 1.1. Dokážte, že nasledujúce tvrdenia sú tautológie:

a) $\models A \Rightarrow (B \Rightarrow A)$ b) $\models (A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$

c) $\models (\neg A \Rightarrow \neg B) \Rightarrow ((\neg A \Rightarrow B) \Rightarrow A)$

Cvičenie 1.2. Pomocou ohodnotení ν ukážte, že ak platí $\models A$ a $\models A \Rightarrow B$, tak platí $\models B$.

Cvičenie 1.3. Dokážte:

a) $\models A \Rightarrow A$ b) $\models \neg A \Rightarrow \neg A$

c) $\models A \vee \neg A$ d) $\models \neg A \Rightarrow (A \Rightarrow B)$

e) $\models \neg\neg A \Rightarrow A$ f) $\models A \Rightarrow \neg\neg A$

g) $\models (A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$ h) $\models (A \Rightarrow \neg B) \Rightarrow (B \Rightarrow \neg A)$

i) $\models (\neg A \Rightarrow B) \Rightarrow (\neg B \Rightarrow A)$ j) $\models (\neg A \Rightarrow \neg B) \Rightarrow (B \Rightarrow A)$

k) $\models (\neg A \Rightarrow B) \Rightarrow ((A \Rightarrow B) \Rightarrow B)$ l) $\models A \Rightarrow (B \Rightarrow (A \,\&\, B))$

m) $\models B \Rightarrow (A \vee B)$ n) $\models A \Rightarrow (A \vee B)$

o) $\models (A \,\&\, B) \Rightarrow B$ p) $\models (A \,\&\, B) \Rightarrow A$

q) $\models (A \,\&\, B) \Rightarrow (A \vee B)$ r) $\models (A \,\&\, B) \Rightarrow (B \,\&\, A)$

s) $\models A \Rightarrow (A \,\&\, A)$ t) $\models \neg(A \,\&\, B) \Rightarrow (\neg A \vee \neg B)$

u) $\models (A \,\&\, (A \vee B)) \Rightarrow A$ v) $\models A \Rightarrow (A \,\&\, (A \vee B))$

w) $\models ((A \Rightarrow A) \Rightarrow A) \Rightarrow A$ x) $\models (\neg A \Rightarrow A) \Rightarrow A$

y*) $\models (\ldots((\underbrace{A \Rightarrow A) \Rightarrow A) \Rightarrow \ldots) \Rightarrow A}_{2k\ A\text{-čiek}}$ z*) $\models (\ldots((\neg A \Rightarrow \underbrace{A) \Rightarrow A) \Rightarrow \ldots) \Rightarrow A}_{2k\ A\text{-čiek}}$

Cvičenie 1.4. Dokážte:

a) $\models A \Rightarrow (\neg B \Rightarrow \neg(A \Rightarrow B))$ b) $\models ((A \Rightarrow B) \Rightarrow A) \Rightarrow A$

c) $\models (A \vee (B \vee C)) \Rightarrow ((B \vee (A \vee C)) \vee A)$

d) $\models ((B \vee (A \vee C)) \vee A) \Rightarrow (A \vee (B \vee C))$

Cvičenie 1.5. Zostrojte formulu v disjunktívnom normálnom tvare ekvivalentnú s formulou:

a) $A \Rightarrow B$ b) $A \Leftrightarrow B$

c) $\neg(A \Rightarrow \neg B)$ d) $\neg A \Rightarrow B$

e) $\neg(A \Rightarrow (B \Rightarrow A)$ f) $((A \vee \neg B) \Rightarrow (C \vee B)) \vee (A \vee C)$

Cvičenie 1.6. Zostrojte formulu v konjunktívnom normálnom tvare ekvivalentnú s formulou:

a) $A \Rightarrow B$ b) $A \Leftrightarrow B$

c) $A \,\&\, (B \Rightarrow C)$ d) $B \Rightarrow (\neg A \Rightarrow B)$

e) $(A \,\&\, \neg B) \vee (\neg B \,\&\, C) \vee (A \,\&\, \neg C)$ f) $(A \Leftrightarrow \neg C) \Rightarrow (B \vee (C \Rightarrow \neg A))$

Cvičenie 1.7. Dokážte, že nasledujúce tvrdenia sú tautológie:

a) $\models (A \,\mathrm{Nor}\, A) \Leftrightarrow \neg A$ b) $\models (A \,\mathrm{Nand}\, A) \Leftrightarrow \neg A$

Cvičenie 1.8. Dokážte, že nasledujúce množiny logických spojok sú úplné:

a) $\neg, \vee$
b) $\neg, \&$
c) $\neg, \Rightarrow$
d) Nor
e) Nand

Cvičenie 1.9. Dokážte, že nasledujúce množiny logických spojok nie sú úplné:

a) $\&, \vee, \Rightarrow, \Leftrightarrow$
b*) $\neg, \Leftrightarrow$

2 VÝROKOVÁ LOGIKA 2

Pochybný dôkaz

Aj keď sa to môže zdať čudné, dokážeme, že každá n-tica reálnych čísel obsahuje len rovnaké čísla.

DÔKAZ (MATEMATICKOU INDUKCIOU). Označme danú n-ticu $a_1, a_2, \ldots, a_n$.
Pre $n = 1$ vlastne niet čo dokazovať, lebo zjavne $a_1 = a_1$.
Nech tvrdenie platí pre n, dokážeme ho pre $n{+}1$. Majme teda $(n{+}1)$-ticu $a_1, a_2, \ldots, a_n, a_{n+1}$. Podľa indukčného predpokladu platí $a_1 = a_2 = \cdots = a_n$ a rovnako tak $a_2 = \cdots = a_n = a_{n+1}$. Preto platí aj $a_1 = a_2 = \cdots = a_n = a_{n+1}$. □

Je zrejmé, že práve uvedený dôkaz nie je správny. Zo svojich skúseností vieme, že pre dvojicu $\{1, 2\}$ platí $1 \neq 2$. Ukazuje sa, že je potrebné vedieť, ako sa dokazujú (odvodzujú) pravdivé tvrdenia (vety).

Dokázateľné formuly

V predchádzajúcej kapitole sme opísali, ako sa konštruujú formuly výrokovej logiky. V tejto si jazyk trochu zjednodušíme a zavedieme axiómy a odvodzovacie pravidlá, pomocou ktorých budeme z jednoduchších viet odvodzovať zložitejšie.

DEFINÍCIA. **Základné výrokové spojky** sú $\neg$ a $\Rightarrow$, pričom ostatné spojky, ako napríklad $\&$, $\vee$ a $\Leftrightarrow$ sú **odvodené výrokové spojky**. Teda:
$A \,\&\, B$ je len skrátený zápis formuly $\neg(A \Rightarrow \neg B)$;
$A \vee B$ je skrátený zápis formuly $\neg A \Rightarrow B$;
$A \Leftrightarrow B$ je skrátený zápis formuly $(A \Rightarrow B) \,\&\, (B \Rightarrow A)$, čiže $\neg((A \Rightarrow B) \Rightarrow \neg(B \Rightarrow A))$.

DEFINÍCIA. **Formálny systém výrokovej logiky** tvoria:

Jazyk výrokovej logiky, ktorý pozostáva z množiny prvotných formúl, symbolov pre logické spojky $\neg$ a $\Rightarrow$ a pomocných symbolov (a).

Axiómy. Nech sú A, B a C ľubovoľné formuly. Potom

(A1) $A \Rightarrow (B \Rightarrow A)$
(A2) $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$
(A3) $(\neg A \Rightarrow \neg B) \Rightarrow ((\neg A \Rightarrow B) \Rightarrow A)$

Odvodzovacie pravidlo je jediné a volá sa **modus ponens**. Tvrdí: z formúl A a $A \Rightarrow B$ odvoď formulu B.

Z Cvičenia 1.1 už vieme, že A1, A2 a A3 sú tautológie. Podľa Cvičenia 1.2 je modus ponens (MP) korektné pravidlo. Teda práve opísaným systémom by sa mali dať odvodiť len tautológie.

DEFINÍCIA. Konečná postupnosť $A_1, A_2, \ldots, A_n$ je **dôkazom formuly** A, ak platí:

(a) A_n je práve A;
(b) pre každé $i = 1, 2, \ldots, n$ je A_i buď axióma tvaru A1, A2, prípadne A3, alebo je A_i modus ponens A_j a A_k, kde $j, k < i$.

Ak existuje dôkaz formuly A, tak A je **dokázateľná vo výrokovej logike**, čo zapisujeme $\vdash A$. Naopak, $\nvdash A$ znamená, že A nie je dokázateľná ($\nvdash A$ je vlastne len skrátený zápis tvrdenia $\neg(\vdash A)$).

POZNÁMKA. Kvôli lepšej prehľadnosti dôkazu budeme formuly, ktoré sa v ňom vyskytli, číslovať na ľavej strane, zatiaľ čo na pravú stranu vždy zaznačíme, ako príslušná formula vznikla.

LEMA 2.1. *Platí* $\vdash A \Rightarrow A$.

DÔKAZ.

1:	$(A \Rightarrow ((A \Rightarrow A) \Rightarrow A)) \Rightarrow ((A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A)))$	A2
2:	$A \Rightarrow ((A \Rightarrow A) \Rightarrow A)$	A1
3:	$(A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A)$	MP2,1
4:	$A \Rightarrow (A \Rightarrow A)$	A1
5:	$A \Rightarrow A$	MP4,3 $\square$

Dôsledkom Lemy 2.1 je **zákon vylúčenia tretieho**: $\vdash A \vee \neg A$ (je to len iný zápis formuly $\vdash \neg A \Rightarrow \neg A$).

DEFINÍCIA. Nech je T množina výrokových formúl. Postupnosť $A_1, A_2, \ldots, A_n$ je **dôkazom formuly** A z predpokladov T, ak platí:

(a) A_n je práve A;
(b) pre ľubovoľné $i = 1, 2, \ldots, n$ je A_i buď axióma, alebo je prvkom z T, alebo je Modus Ponens dvoch formúl z $A_1, A_2, \ldots, A_{i-1}$.

Formula A je **dokázateľná z predpokladov** T, ak existuje dôkaz A z T, čo zapisujeme $T \vdash A$.

POZNÁMKA. Kvôli lepšej prehľadnosti budeme i-ty riadok dôkazu zapisovať tak, že pred formulu vsunieme symbol $\vdash$ a ešte pred tento symbol uvedieme všetky predpoklady, ktoré sme využili pri odvodení tejto formuly. Z tohoto pravidla budeme robiť jedinú výnimku. V prípade, že A je predpoklad, budeme písať jednoducho A namiesto korektného $A \vdash A$.

LEMA 2.2. *Pre ľubovoľné formuly* A, B, C *platí* **pravidlo sylogizmu**, *teda* $A \Rightarrow B,\ B \Rightarrow C \vdash A \Rightarrow C$.

Dôkaz.

1:	$\vdash (A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$	A2
2:	$\vdash (B \Rightarrow C) \Rightarrow (A \Rightarrow (B \Rightarrow C))$	A1
3:	$B \Rightarrow C$	predpoklad
4:	$B \Rightarrow C \vdash A \Rightarrow (B \Rightarrow C)$	MP3,2
5:	$B \Rightarrow C \vdash (A \Rightarrow B) \Rightarrow (A \Rightarrow C)$	MP4,1
6:	$A \Rightarrow B$	predpoklad
7:	$A \Rightarrow B,\ B \Rightarrow C \vdash A \Rightarrow C$	MP6,5 $\square$

Lema 2.3 (**o zámene predpokladov**). *Pre ľubovoľné formuly A, B a C platí $A \Rightarrow (B \Rightarrow C) \vdash B \Rightarrow (A \Rightarrow C)$.*

Dôkaz.

1:	$\vdash (A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$	A2
2:	$A \Rightarrow (B \Rightarrow C)$	predpoklad
3:	$A \Rightarrow (B \Rightarrow C) \vdash (A \Rightarrow B) \Rightarrow (A \Rightarrow C)$	MP2,1
4:	$\vdash B \Rightarrow (A \Rightarrow B)$	A1
5:	$A \Rightarrow (B \Rightarrow C) \vdash B \Rightarrow (A \Rightarrow C)$	Syl4,3 $\square$

Veta 2.4 (**o dedukcii**). *Nech sú A a B formuly a nech je T množina formúl. Potom $T \vdash A \Rightarrow B$ práve vtedy, keď $T \cup \{A\} \vdash B$.*

Dôkaz. Nech platí $T \vdash A \Rightarrow B$ a nech je $C_1, C_2, \ldots, C_n$ dôkazom $A \Rightarrow B$ z T. Potom $C_1, C_2, \ldots, C_n, A, B$ je dôkazom B z $T \cup \{A\}$, lebo C_n je práve $A \Rightarrow B$, A je z $T \cup \{A\}$ a B je modus ponens formúl C_n a A.

Naopak, nech platí $T \cup \{A\} \vdash B$ a nech je $D_1, D_2, \ldots, D_m$ dôkazom B z $T \cup \{A\}$. Ukážeme, že pre každé $i = 1, 2, \ldots, m$ je $A \Rightarrow D_i$ dokázateľné z T. Postupujeme indukciou podľa i:

1° Pre $i = 1$ môžu nastať tri prípady:

(a) D_1 je axióma. Potom:

$1'$:	$\vdash D_1 \Rightarrow (A \Rightarrow D_1)$	A1
$2'$:	$\vdash D_1$	axióma
$3'$:	$\vdash A \Rightarrow D_1$	MP$2', 1'$

(b) D_1 je z T. Potom:

$1'$:	$\vdash D_1 \Rightarrow (A \Rightarrow D_1)$	A1
$2'$:	$T \vdash D_1$	predpoklad
$3'$:	$T \vdash A \Rightarrow D_1$	MP$2', 1'$

(c) D_1 je práve A. Potom podľa Lemy 2.1 $\vdash A \Rightarrow D_1$.

2° Nech tvrdenie $T \vdash A \Rightarrow D_i$ platí pre všetky $i = 1, \ldots, j-1$ ($j \leq m$). Dokážeme, že platí aj $T \vdash A \Rightarrow D_j$.

Prípady (a), (b) a (c) sme už rozobrali v prvom kroku indukcie. Avšak ak $j > 1$, môže nastať ešte jeden prípad, ktorý je potrebné rozobrať. Môže sa stať, že D_j je modus ponens formúl D_k a D_l, kde $k, l < j$. Potom však D_l má tvar $D_k \Rightarrow D_j$. Využijúc indukčný predpoklad (IP) dostávame:

$1'$:	$T \vdash A \Rightarrow D_k$	IP
$2'$:	$T \vdash A \Rightarrow (D_k \Rightarrow D_j)$	IP
$3'$:	$\vdash (A \Rightarrow (D_k \Rightarrow D_j)) \Rightarrow ((A \Rightarrow D_k) \Rightarrow (A \Rightarrow D_j))$	A2
$4'$:	$T \vdash (A \Rightarrow D_k) \Rightarrow (A \Rightarrow D_j)$	MP$2', 3'$
$5'$:	$T \vdash A \Rightarrow D_j$	MP$1', 4'$ □

Poznámka. Všimnime si, že Lemy 2.2, 2.3 a Veta 2.4 nám dávaju nové odvodzovacie pravidlá. V ďalšom teda môžeme okrem modus ponens využívať aj sylogizmus, vetu o zámene predpokladov a vetu o dedukcii. Modus ponens označujeme skrátene MP s číslami príslušných formúl v dôkaze. Podobne budeme používať skratky Syl4,3 (sylogizmus štvrtej a tretej formuly); VZP3 (veta o zámene predpokladov na tretiu formulu) a VD7 (veta o dedukcii na siedmu formulu).

Lema 2.5. $\vdash \neg A \Rightarrow (A \Rightarrow B)$.

Dôkaz.

1:	$\vdash (\neg B \Rightarrow \neg A) \Rightarrow ((\neg B \Rightarrow A) \Rightarrow B)$	A3
2:	$\vdash \neg A \Rightarrow (\neg B \Rightarrow \neg A)$	A1
3:	$\neg A \vdash \neg B \Rightarrow \neg A$	VD2
4:	$\neg A \vdash (\neg B \Rightarrow A) \Rightarrow B$	MP3,1
5:	$\vdash A \Rightarrow (\neg B \Rightarrow A)$	A1
6:	$A \vdash \neg B \Rightarrow A$	VD5
7:	$\neg A,\ A \vdash B$	MP6,4
8:	$\neg A \vdash A \Rightarrow B$	VD8
9:	$\vdash \neg A \Rightarrow (A \Rightarrow B)$	VD9 □

Lema 2.6. $\vdash \neg\neg A \Rightarrow A$.

Dôkaz.

1:	$\vdash (\neg A \Rightarrow \neg\neg A) \Rightarrow ((\neg A \Rightarrow \neg A) \Rightarrow A)$	A3
2:	$\vdash \neg\neg A \Rightarrow (\neg A \Rightarrow \neg\neg A)$	A1
3:	$\neg\neg A \vdash \neg A \Rightarrow \neg\neg A$	VD2
4:	$\neg\neg A \vdash (\neg A \Rightarrow \neg A) \Rightarrow A$	MP3,1
5:	$\vdash \neg A \Rightarrow \neg A$	Lema 2.1
6:	$\neg\neg A \vdash\ A$	MP5,4
7:	$\vdash \neg\neg A \Rightarrow A$	VD6 □

Lema 2.7. $\vdash A \Rightarrow \neg\neg A$.

Dôkaz.

1:	$\vdash (\neg\neg\neg A \Rightarrow \neg A) \Rightarrow ((\neg\neg\neg A \Rightarrow A) \Rightarrow \neg\neg A)$	A3
2:	$\vdash \neg\neg\neg A \Rightarrow \neg A$	Lema 2.6
3:	$\vdash (\neg\neg\neg A \Rightarrow A) \Rightarrow \neg\neg A$	MP2,1
4:	$\vdash A \Rightarrow (\neg\neg\neg A \Rightarrow A)$	A1
5:	$\vdash A \Rightarrow \neg\neg A$	Syl4,3 □

Poznámka 1. Predchádzajúce tri dôkazy mali spoločnú stratégiu, ktorá spočívala vo vhodnej aplikácii axiómy A3. Približne povedané, zvolili sme taký koniec A3, ktorý sa zhodoval s koncom dokazovanej formuly X. Potom prvé podformuly

X slúžili ako predpoklady, z ktorých sme sa snažili odvodiť prvé podformuly A3. V závere sme použili vetu o dedukcii.

Poznámka 2. V predchádzajúcich troch dôkazoch sme využili už dokázané tvrdenia (Lemy 2.1, 2.2, 2.6 a Vetu 2.4). Ak by sme však chceli byť presní v zmysle našej definície dôkazu, tak všade, kde sme sa odvolávali na pomocné tvrdenia, mali sme vsunúť celé dôkazy týchto tvrdení. Toto kvôli lepšej prehľadnosti nerobíme a aj v nasledujúcom texte nám bude stačiť odvolávka na príslušné už dokázané tvrdenie (ktoré je naviac dokázané v „základnej“ forme).

Veta 2.8 (**vety o obrátenej implikácii**). *Platia nasledujúce tvrdenia:*
$\vdash (\neg A \Rightarrow \neg B) \Rightarrow (B \Rightarrow A)$; $\vdash (\neg A \Rightarrow B) \Rightarrow (\neg B \Rightarrow A)$;
$\vdash (A \Rightarrow \neg B) \Rightarrow (B \Rightarrow \neg A)$; $\vdash (A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$.

Dôkazy si urobte ako jednoduché cvičenie. Pri dôkaze prvých dvoch stačí využiť A1, A3 a Vetu o dedukcii, pri dôkaze druhých dvoch ešte Lemu 2.6. Symbolom VOOI v ďalšom označujeme ľubovoľnú z viet o obrátenej implikácii.

Lema 2.9. $\vdash A \Rightarrow (\neg B \Rightarrow \neg(A \Rightarrow B))$.

Dôkaz.

1:	A	predpoklad
2:	$A \Rightarrow B$	predpoklad
3:	$A,\ A \Rightarrow B \vdash B$	MP1,2
4:	$A \vdash (A \Rightarrow B) \Rightarrow B$	VD3
5:	$\vdash ((A \Rightarrow B) \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg(A \Rightarrow B))$	VOOI
6:	$A \vdash \neg B \Rightarrow \neg(A \Rightarrow B)$	MP4,5
7:	$\vdash A \Rightarrow (\neg B \Rightarrow \neg(A \Rightarrow B))$	VD6 $\square$

Veta 2.10 (**o neutrálnej formuli**). *Ak* $T \cup \{A\} \vdash B$ *a* $T \cup \{\neg A\} \vdash B$, *tak* $T \vdash B$.

Dôkaz.

1:	$T \cup \{A\} \vdash B$	predpoklad
2:	$T \vdash A \Rightarrow B$	VD1
3:	$\vdash (A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$	VOOI
4:	$T \vdash \neg B \Rightarrow \neg A$	MP2,3
5:	$T \cup \{\neg A\} \vdash B$	predpoklad
6:	$T \vdash \neg A \Rightarrow B$	VD5
7:	$\vdash (\neg A \Rightarrow B) \Rightarrow (\neg B \Rightarrow A)$	VOOI
8:	$T \vdash \neg B \Rightarrow A$	MP6,7
9:	$\vdash (\neg B \Rightarrow \neg A) \Rightarrow ((\neg B \Rightarrow A) \Rightarrow B)$	A3
10:	$T \vdash (\neg B \Rightarrow A) \Rightarrow B$	MP4,9
11:	$T \vdash B$	MP8,10 $\square$

LEMA 2.11. $A \Rightarrow (B \Rightarrow C) \vdash (A \,\&\, B) \Rightarrow C$.

DÔKAZ.

1:	$A \Rightarrow (B \Rightarrow C)$	predpoklad
2:	$\vdash (B \Rightarrow C) \Rightarrow (\neg C \Rightarrow \neg B)$	VOOI
3:	$A \Rightarrow (B \Rightarrow C) \vdash A \Rightarrow (\neg C \Rightarrow \neg B)$	Syl1,2
4:	$A \Rightarrow (B \Rightarrow C) \vdash \neg C \Rightarrow (A \Rightarrow \neg B)$	VZP3
5:	$\vdash (\neg C \Rightarrow (A \Rightarrow \neg B)) \Rightarrow (\neg (A \Rightarrow \neg B) \Rightarrow C)$	VOOI
6:	$A \Rightarrow (B \Rightarrow C) \vdash \neg (A \Rightarrow \neg B) \Rightarrow C$	MP4,5
6′:	$A \Rightarrow (B \Rightarrow C) \vdash (A \,\&\, B) \Rightarrow C$	$\square$

LEMA 2.12. $(A \,\&\, B) \Rightarrow C \vdash A \Rightarrow (B \Rightarrow C)$

DÔKAZ.

1:	$\vdash A \Rightarrow (\neg\neg B \Rightarrow \neg (A \Rightarrow \neg B))$	Lema 2.9
2:	$A \vdash \neg\neg B \Rightarrow \neg (A \Rightarrow \neg B)$	VD1
3:	$\vdash B \Rightarrow \neg\neg B$	Lema 2.7
4:	$A \vdash B \Rightarrow \neg (A \Rightarrow \neg B)$	Syl3,2
5:	$\neg (A \Rightarrow \neg B) \Rightarrow C$	predpoklad
6:	$\neg (A \Rightarrow \neg B) \Rightarrow C,\ A \vdash B \Rightarrow C$	Syl4,5
7:	$\neg (A \Rightarrow \neg B) \Rightarrow C \vdash A \Rightarrow (B \Rightarrow C)$	VD6
7′:	$(A \,\&\, B) \Rightarrow C \vdash A \Rightarrow (B \Rightarrow C)$	$\square$

VETA 2.13. *Nech sú $A_1, A_2, \ldots, A_n$ a B výrokové formuly. Potom tvrdenie $\{A_1, A_2, \ldots, A_n\} \vdash B$ platí práve vtedy, keď platí $\vdash (A_1 \,\&\, A_2 \,\&\, \ldots \,\&\, A_n) \Rightarrow B$.*

POZNÁMKA. Formula $(A_1 \,\&\, A_2 \,\&\, A_3 \,\&\, \ldots \,\&\, A_{n-1} \,\&\, A_n)$ je len iný zápis formuly $((\ldots((A_1 \,\&\, A_2) \,\&\, A_3) \,\&\, \ldots \,\&\, A_{n-1}) \,\&\, A_n)$.

DÔKAZ. Vetu 2.13 dokážeme indukciou podľa n.

1° Ak $n = 1$, potom $A_1 \vdash B$ práve vtedy, keď $\vdash A_1 \Rightarrow B$, podľa vety o dedukcii.

2° Nech tvrdenie vety platí pre všetky $i < n$, dokážeme jeho platnosť pre n. (Symbolom IP označujeme indukčný predpoklad.) Nech

1′:	$\{A_1, \ldots, A_{n-1}, A_n\} \vdash B$	predpoklad
2′:	$\{A_1, \ldots, A_{n-1}\} \vdash A_n \Rightarrow B$	VD1′
3′:	$\vdash (A_1 \,\&\, \ldots \,\&\, A_{n-1}) \Rightarrow (A_n \Rightarrow B)$	IP
4′:	$\vdash (A_1 \,\&\, \ldots \,\&\, A_{n-1} \,\&\, A_n) \Rightarrow B$	Lema 2.11

Naopak, nech

1′:	$\vdash (A_1 \,\&\, \ldots \,\&\, A_{n-1} \,\&\, A_n) \Rightarrow B$	predpoklad
2′:	$\vdash (A_1 \,\&\, \ldots \,\&\, A_{n-1}) \Rightarrow (A_n \Rightarrow B)$	Lema 2.12
3′:	$\{A_1, \ldots, A_{n-1}\} \vdash A_n \Rightarrow B$	IP
4′:	$\{A_1, \ldots, A_{n-1}, A_n\} \vdash B$	VD3′ $\square$

Cvičenia

Cvičenie 2.1. Prezrite si nasledujúci dôkaz a nájdite v ňom chybu. Vzápätí ho opravte.

Pre súčet geometrického radu platí:

$$1 + q + q^2 + \cdots + q^n = \frac{q^{n+1} - q}{q - 1}\,.$$

Dôkaz: Nech tvrdenie platí pre n, dokážeme ho pre $n{+}1$:

$$1 + q + q^2 + \cdots + q^n + q^{n+1} = \frac{q^{n+1} - q}{q - 1} + q^{n+1} = \frac{q^{n+2} - q}{q - 1}. \quad \square$$

Cvičenie 2.2. Preštudujte si nasledujúci dôkaz.

Prvočísel je nekonečne veľa.

Dôkaz sporom: Predpokladajme, že platí negácia tvrdenia, teda nech je prvočísel len konečne veľa. Označme si ich $p_1, p_2, \ldots, p_n$. Potom každé prirodzené číslo q možno zapísať v tvare $q = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$ (niektoré z čísel α_i môžu byť aj nuly).

Čo viete povedať o čísle $p = (p_1 \cdot p_2 \cdot \ldots p_n) + 1$? Zrejme p nie je deliteľné žiadnym z čísel $p_1, p_2, \ldots, p_n$. To však znamená, že $p = p_1^0 \cdot p_2^0 \cdot \ldots \cdot p_n^0 = 1$, čo je spor s tým, že $p \geq 3$, keďže 2 je istotne prvočíslo. $\square$

Všimli ste si, že sme v tomto dôkaze využili Lemu 2.1, teda zákon vylúčenia tretieho? Takýto dôkaz je v matematike (ktorá obsahuje ako svoju časť výrokovú logiku) korektný, avšak v bežnom živote sa toto nemusí prijímať. Napríklad ak nie je pravda, že politik v parlamente klame, tak nemusí byť pravdivé tvrdenie, že hovorí pravdu. Ešte môže aj napoly klamať a napoly hovoriť pravdu, respektíve môže hovoriť tak, že nikto nepochopí, čo chcel povedať (a následne sa nedá overiť pravdivosť jeho tvrdenia).

Cvičenie 2.3. S použitím vety o dedukcii odvoďte pravidlo sylogizmu a vetu o zámene predpokladov.

Cvičenie 2.4. Dokážte vety o obrátenej implikácii:

a) $\vdash (A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$ b) $\vdash (A \Rightarrow \neg B) \Rightarrow (B \Rightarrow \neg A)$
c) $\vdash (\neg A \Rightarrow B) \Rightarrow (\neg B \Rightarrow A)$ d) $\vdash (\neg A \Rightarrow \neg B) \Rightarrow (B \Rightarrow A)$

Cvičenie 2.5. S použitím vety o dedukcii odvoďte nasledujúce formuly:

a) $\vdash (\neg A \Rightarrow B) \Rightarrow ((A \Rightarrow B) \Rightarrow B)$ b) $\vdash A \Rightarrow (B \Rightarrow (A \,\&\, B))$
c) $\vdash B \Rightarrow (A \vee B)$ d) $\vdash A \Rightarrow (A \vee B)$
e) $\vdash (A \,\&\, B) \Rightarrow B$ f) $\vdash (A \,\&\, B) \Rightarrow A$
g) $\vdash (A \,\&\, B) \Rightarrow (A \vee B)$ h) $\vdash (A \,\&\, B) \Rightarrow (B \,\&\, A)$
i) $\vdash A \Rightarrow (A \,\&\, A)$ j) $\vdash \neg(A \,\&\, B) \Rightarrow (\neg A \vee \neg B)$

k) $\vdash (A \,\&\, (A \vee B)) \Rightarrow A$

l) $\vdash A \Rightarrow (A \,\&\, (A \vee B))$

m) $\vdash ((A \Rightarrow A) \Rightarrow A) \Rightarrow A$

n) $\vdash (\neg A \Rightarrow A) \Rightarrow A$

o) $\vdash (\ldots((\underbrace{A \Rightarrow A) \Rightarrow A) \Rightarrow \ldots) \Rightarrow A}_{2k\ A\text{-čiek}}$

p) $\vdash (\ldots((\neg A \Rightarrow \underbrace{A) \Rightarrow A) \Rightarrow \ldots) \Rightarrow A}_{2k\ A\text{-čiek}}$

q) $\vdash ((A \Rightarrow B) \Rightarrow A) \Rightarrow A$

r) $A \Rightarrow B \vdash (C \vee A) \Rightarrow (C \vee B)$

s) $A \Rightarrow B \vdash (C \,\&\, A) \Rightarrow (C \,\&\, B)$

t) $A \Rightarrow B,\ B \Rightarrow C \vdash \neg(A \,\&\, \neg C)$

u) $\vdash (A \vee (B \vee C)) \Rightarrow ((B \vee (A \vee C)) \vee A)$

v) $\vdash ((B \vee (A \vee C)) \vee A) \Rightarrow (A \vee (B \vee C))$

x) $A \Rightarrow (B \Rightarrow C),\ A \Rightarrow B \vdash A \Rightarrow (A \Rightarrow C)$

y) $\vdash (A \Rightarrow C \Rightarrow ((B \Rightarrow C) \Rightarrow ((\neg A \Rightarrow B) \Rightarrow C))$

z) $A \Rightarrow B,\ C \Rightarrow D \vdash (A \,\&\, C) \Rightarrow (B \,\&\, D)$

3 VÝROKOVÁ LOGIKA 3

Medzi $\models$ a $\vdash$ nie je rozdiel

Doteraz sme skúmali „pravdivé“ formuly z dvoch hľadísk. Jednak sme skúmali tie, pre ktoré platí $\models A$ (tautológie) a potom tie, pre ktoré $\vdash A$ (dokázateľné formuly). Pripomeňme, že tautológie boli také formuly, ktoré pri ľubovoľnom ohodnotení ν prvotných formúl dávali $\overline{\nu}(A) = 1$, zatiaľ čo dokázateľné formuly sa dajú odvodiť z axióm pomocou pravidla modus ponens. V tejto časti ukážeme, že $\models A$ práve vtedy, keď $\vdash A$. Ináč povedané, ukážeme, že formuly odvodené čisto formálnym spôsobom sú práve tie, ktoré považujeme za pravdivé.

Postova veta

Nech je ν ohodnotenie prvotných formúl. Definujme

$$B^\nu = \begin{cases} B & \text{ak} \quad \overline{\nu}(B) = 1, \\ \neg B & \text{ak} \quad \overline{\nu}(B) = 0. \end{cases}$$

Lema 3.1. *Nech je ν ohodnotenie prvotných formúl $\{p_1, p_2, \ldots, p_n\}$ a nech všetky prvotné formuly, ktoré sa vyskytujú v A, sú medzi $\{p_1, p_2, \ldots, p_n\}$. Potom $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash A^\nu$.*

Poznámka. Napríklad ak A je $p_1 \Rightarrow p_2$, $\nu(p_1)=1$ a $\nu(p_2)=0$, potom $\overline{\nu}(A)=0$. Tu Lema 3.1 tvrdí: $p_1, \neg p_2 \vdash \neg(p_1 \Rightarrow p_2)$, ale to je práve tvrdenie Lemy 2.9 (po dvojnásobnej aplikácii Vety o dedukcii).

Dôkaz. Indukciou podľa konštrukcie A.

1° Ak je A prvotná formula p_i, $i \in \{1, 2, \ldots, n\}$, tak platí $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash p_i^\nu$.

2° (I) Nech A má tvar $\neg B$, pričom pre B tvrdenie lemy platí, teda platí $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash B^\nu$. Rozlíšime dva prípady:

(a) $\overline{\nu}(B) = 1$. Potom $\overline{\nu}(A) = \overline{\nu}(\neg B) = 0$, B^ν je B a A^ν je $\neg\neg B$. Teda:

$1'$:	$\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash B^\nu$	IP
$1''$:	$\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash B$	
$2'$:	$\vdash B \Rightarrow \neg\neg B$	Lema 2.7
$3'$:	$\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash \neg\neg B$	MP$1'', 2'$
$3''$:	$\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash A^\nu$	

(b) $\overline{\nu}(B) = 0$. Potom $\overline{\nu}(A) = \overline{\nu}(\neg B) = 1$, B^ν je $\neg B$ a A^ν je $\neg B$. Teda:

$1'$: $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash B^\nu$ IP
$1''$: $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash \neg B$
$1'''$: $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash A^\nu$

(II) Nech A má tvar $B \Rightarrow C$, pričom pre B aj C tvrdenie lemy platí, teda platí $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash B^\nu$ aj $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash C^\nu$. Rozlíšime tri prípady:

(a) $\overline{\nu}(B) = 0$. Potom $\overline{\nu}(A) = \overline{\nu}(B \Rightarrow C) = 1$, B^ν je $\neg B$ a A^ν je $B \Rightarrow C$. Teda:

$1'$: $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash B^\nu$ IP
$1''$: $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash \neg B$
$2'$: $\vdash \neg B \Rightarrow (B \Rightarrow C)$ Lema 2.5
$3'$: $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash B \Rightarrow C$ MP$1'', 2'$
$3''$: $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash A^\nu$

(b) $\overline{\nu}(C) = 1$. Potom $\overline{\nu}(A) = \overline{\nu}(B \Rightarrow C) = 1$, C^ν je C a A^ν je $B \Rightarrow C$. Teda:

$1'$: $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash C^\nu$ IP
$1''$: $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash C$
$2'$: $\vdash C \Rightarrow (B \Rightarrow C)$ A1
$3'$: $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash B \Rightarrow C$ MP$1'', 2'$
$3''$: $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash A^\nu$

(c) Zostáva posledný prípad $\overline{\nu}(B) = 1$ a $\overline{\nu}(C) = 0$. Potom $\overline{\nu}(A) = \overline{\nu}(B \Rightarrow C) = 0$, B^ν je B, C^ν je $\neg C$ a A^ν je $\neg(B \Rightarrow C)$. Teda:

$1'$: $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash B^\nu$ IP
$1''$: $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash B$
$2'$: $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash C^\nu$ IP
$2''$: $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash \neg C$
$3'$: $\vdash B \Rightarrow (\neg C \Rightarrow \neg(B \Rightarrow C))$ Lema 2.9
$4'$: $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash \neg C \Rightarrow \neg(B \Rightarrow C)$ MP$1'', 3'$
$5'$: $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash \neg(B \Rightarrow C)$ MP$2'', 4'$
$5''$: $\{p_1^\nu, p_2^\nu, \ldots, p_n^\nu\} \vdash A^\nu$ $\square$

VETA 3.2 (**Postova**). *Pre ľubovoľnú formulu A výrokovej logiky platí $\vdash A$ práve vtedy, keď $\vDash A$.*

DÔKAZ. Nech platí $\vdash A$. Z Cvičenia 1.1 vieme, že všetky axiómy sú tautológie a podľa Cvičenia 1.2 ak $\vDash B$ a $\vDash B \Rightarrow C$, tak aj $\vDash C$. Teda pre ľubovoľný dôkaz $A_1, A_2, \ldots, A_n$ formuly A platí $\vDash A_i$ pre všetky $i = 1, 2, \ldots, n$ a teda aj $\vDash A$. (Poznamenajme, že dôkaz $A_1, A_2, \ldots, A_n$ bol dôkaz v zmysle definície pred Lemou 2.1, čiže bez predpokladov. Vzhľadom na Poznámku 2 za Lemou 2.7 z každého dôkazu formuly A (aj z toho, ktorý využíva Vetu o dedukcii a iné pomocné tvrdenia) vieme vytvoriť dôkaz v zmysle definície pred Lemou 2.1.)

Naopak, majme danú tautológiu A. Ukážeme, že A je dokázateľná. Nech sú $\{p_1, p_2, \ldots, p_n\}$ všetky prvotné formuly vyskytujúce sa v A. Potom podľa Lemy 3.1 pre ľubovoľné ohodnotenie μ prvotných formúl platí $\{p_1^\mu, p_2^\mu, \ldots, p_n^\mu\} \vdash A$. (Keďže A je tautológiou, tak A^μ je vždy A.)

Nech je μ' ohodnotenie líšiace sa od μ len v hodnote pre p_n. Potom aj pre μ' platí Lema 3.1 a teda:

$1'$: $\{p_1^\mu, p_2^\mu, \ldots, p_{n-1}^\mu, p_n\} \vdash A$ Lema 3.1
$2'$: $\{p_1^\mu, p_2^\mu, \ldots, p_{n-1}^\mu, \neg p_n\} \vdash A$ Lema 3.1
$3'$: $\{p_1^\mu, p_2^\mu, \ldots, p_{n-1}^\mu\} \vdash A$ Veta 2.10 na $1'$ a $2'$

Teraz zvoľme μ'' také, že μ'' sa líši od μ len v hodnote priradenej p_{n-1}. Potom obdobne, ako v predchádzajúcom (μ bolo ľubovoľné), vieme odvodiť aj:

1^*: $\{p_1^{\mu''}, p_2^{\mu''}, \ldots, p_{n-1}^{\mu''}\} \vdash A$,

teda máme

$1'$: $\{p_1^\mu, p_2^\mu, \ldots, p_{n-2}, p_{n-1}\} \vdash A$
$2'$: $\{p_1^\mu, p_2^\mu, \ldots, p_{n-2}, \neg p_{n-1}\} \vdash A$
$3'$: $\{p_1^\mu, p_2^\mu, \ldots, p_{n-2}^\mu\} \vdash A$ Veta 2.10 na $1'$ a $2'$

Takto môžeme vylúčiť všetky prvotné formuly a dokážeme $\vdash A$. □

Definícia. Formálny systém je **sporný**, ak je v ňom dokázateľná ľubovoľná formula. Ak formálny systém nie je sporný, nazývame ho **bezosporný** (**konzistentný**).

Veta 3.3. *Výroková logika je bezosporný formálny systém.*

Dôkaz. Ak by bola výroková logika sporným formálnym systémom, tak potom by pre každú formulu A (hoci aj prvotnú) platilo $\vdash A$ aj $\vdash \neg A$. Ale podľa Postovej vety by potom malo platiť $\vDash A$ aj $\vDash \neg A$, čo zjavne neplatí. □

Splniteľnosť

Teraz sa budeme zaoberať tautologickými dôsledkami množín formúl (teórií).

Definícia. Nech je T množina výrokových formúl. Potom T je **splniteľná** (**konzistentná**), ak existuje ohodnotenie ν prvotných formúl vyskytujúcich sa v T také, že pre každú formulu A z T platí $\overline{\nu}(A) = 1$. Takéto ohodnotenie ν sa nazýva **model** množiny formúl T.

Ak T nie je splniteľná, tak je **nesplniteľná**.

Definícia. Nech je T množina výrokových formúl a nech je A výroková formula. Potom A je **tautologickým dôsledkom** T, zapisujeme $T \vDash A$, ak pre každý model ν množiny T platí $\overline{\nu}(A) = 1$.

Zápisom $T \nvDash A$ zapisujeme, že neplatí $T \vDash A$.

Poznámka 1. Modelom prázdnej množiny formúl je ľubovoľné ohodnotenie. Preto $\vDash A$ (čo je vlastne $\{\} \vDash A$) platí práve vtedy, keď je A tautológia. To znamená, že $\vDash A$ je korektné označenie aj v zmysle tejto definície.

Poznámka 2. Ak je T nesplniteľná, tak ľubovoľná formula je jej tautologickým dôsledkom.

Poznámka 3. Pre splniteľnú množinu formúl T a formulu A platí $T \models A$ práve vtedy, keď je $T \cup \{\neg A\}$ nesplniteľná.

Lema 3.4. *Nech sú $A_1, A_2, \ldots, A_n$ výrokové formuly. Potom B je tautologickým dôsledkom formúl $\{A_1, A_2, \ldots, A_n\}$ práve vtedy, keď je tautológiou formula $(A_1 \,\&\, A_2 \,\&\, \ldots \,\&\, A_n) \Rightarrow B$.*

Dôkaz. Nech $\{A_1, A_2, \ldots, A_n\} \models B$. Ak existuje ohodnotenie prvotných formúl vyskytujúcich sa v $A_1, A_2, \ldots, A_n, B$ také, že $\overline{\nu}((A_1 \,\&\, A_2 \,\&\, \ldots \,\&\, A_n) \Rightarrow B) = 0$, tak máme $\overline{\nu}(B) = 0$ a zároveň $\overline{\nu}(A_1 \,\&\, A_2 \,\&\, \ldots \,\&\, A_n) = 1$. To značí, že platí $\overline{\nu}(A_1) = \overline{\nu}(A_2) = \cdots = \overline{\nu}(A_n) = 1$, čo je spor s tým, že B je tautologickým dôsledkom $\{A_1, A_2, \ldots, A_n\}$.

Naopak, nech $\{A_1, A_2, \ldots, A_n\} \not\models B$. Potom pre $\{A_1, A_2, \ldots, A_n\}$ existuje model μ taký, že $\overline{\mu}(B) = 0$. Avšak potom $\overline{\mu}(A_1 \,\&\, A_2 \,\&\, \ldots \,\&\, A_n) = 1$, čo značí, že $\overline{\mu}((A_1 \,\&\, A_2 \,\&\, \ldots \,\&\, A_n) \Rightarrow B) = 0$, a teda $\not\models (A_1 \,\&\, A_2 \,\&\, \ldots \,\&\, A_n) \Rightarrow B$. □

Poznámka. Porovnajte Lemu 3.4 s Vetou 2.13.

Veta 3.5 (**o kompaktnosti**). *Množina výrokových formúl je splniteľná práve vtedy, keď je splniteľná každá jej konečná podmnožina.*

Dôkaz Vety 3.5 možno nájsť napríklad v [5]. Kvôli vyššej náročnosti ho vynechávame.

Veta o úplnosti

V tejto časti ukážeme, že pre ľubovoľnú množinu formúl T platí $T \models A$ práve vtedy, keď $T \vdash A$.

Definícia. Množina výrokových formúl T je **sporná**, ak je z T dokázateľná ľubovoľná výroková formula. V opačnom prípade je T **bezosporná** (**konzistentná**).

Poznámka. U tautológií sme pojem konzistentný stotožňovali s pojmom splniteľný. Nižšie ukážeme, že pojem splniteľný a bezosporný sú vo výrokovej logike synonymá.

Lema 3.6. *Nech je T množina výrokových formúl. Potom sú nasledujúce podmienky ekvivalentné tvrdeniu, že T je sporná:*

(a) *Existuje formula A taká, že $T \vdash A$ aj $T \vdash \neg A$.*
(b) *Existuje konečná podmnožina T_0 množiny T taká, že T_0 je sporná.*

DÔKAZ. Najprv dokážeme, že prvá podmienka je ekvivalentná tvrdeniu, že T je sporná. Nech $T \vdash A$ aj $T \vdash \neg A$. Potom pre ľubovoľnú formulu B platí:

1:	$T \vdash A$	predpoklad
2:	$T \vdash \neg A$	predpoklad
3:	$\vdash \neg A \Rightarrow (A \Rightarrow B)$	Lema 2.5
4:	$T \vdash A \Rightarrow B$	MP2,3
5:	$T \vdash B$	MP1,4

Teda T je sporná.

Naopak, ak T je sporná, tak $T \vdash B$ pre každú formulu. Teda $T \vdash A$ aj $T \vdash \neg A$.

Teraz dokážeme, že druhá podmienka je ekvivalentná tvrdeniu, že T je sporná. Nech T je sporná. Potom podľa (a) existuje formula A taká, že $T \vdash A$ aj $T \vdash \neg A$. Zvoľme za T_0 práve tú množinu predpokladov z T, ktoré sa používajú v dôkazoch A a $\neg A$. Keďže dôkaz je konečná postupnosť formúl, tak aj T_0 je konečná. Teda platí $T_0 \vdash A$ aj $T_0 \vdash \neg A$, a podľa (a) je T_0 sporná.

Naopak, ak existuje podmnožina T_0 množiny T taká, že T_0 je sporná, tak každý dôkaz z T_0 je aj dôkazom z T. Preto z T možno dokázať ľubovoľnú formulu a teda T je sporná. □

LEMA 3.7. *Konečná množina formúl T je bezosporná práve vtedy, keď je splniteľná, t. j. keď existuje ohodnotenie ν prvotných formúl také, ktorého rozšírenie $\overline{\nu}$ priradí každej formule z T hodnotu 1.*

DÔKAZ. Nech je $T = \{B_1, B_2, \ldots, B_n\}$ bezosporná množina formúl. Potom podľa definície bezospornosti existuje formula A taká, že $T \nvdash A$. Z Vety 2.13 plynie, že $\nvdash (B_1 \,\&\, B_2 \,\&\, \ldots \,\&\, B_n) \Rightarrow A$ a z Postovej vety $\not\models (B_1 \,\&\, B_2 \,\&\, \ldots \,\&\, B_n) \Rightarrow A$. To značí, že existuje ohodnotenie ν, pre ktoré $\overline{\nu}((B_1 \,\&\, B_2 \,\&\, \ldots \,\&\, B_n) \Rightarrow A) = 0$. Avšak potom $\overline{\nu}(B_1 \,\&\, B_2 \,\&\, \ldots \,\&\, B_n) = 1$, čiže $\overline{\nu}(B_i) = 1$ pre všetky $i = 1, 2, \ldots, n$.

Naopak, ak je $T = \{B_1, B_2, \ldots, B_n\}$ sporná, tak pre ľubovoľnú formulu A platí $T \vdash A \,\&\, \neg A$. Potom $\vdash (B_1 \,\&\, B_2 \,\&\, \ldots \,\&\, B_n) \Rightarrow (A \,\&\, \neg A)$ podľa Lemy 2.13 a $\models (B_1 \,\&\, B_2 \,\&\, \ldots \,\&\, B_n) \Rightarrow (A \,\&\, \neg A)$ podľa Postovej vety. Označme symbolom B formulu $(B_1 \,\&\, B_2 \,\&\, \ldots \,\&\, B_n) \Rightarrow (A \,\&\, \neg A)$. Keďže B je tautológia, tak pre ľubovoľné ohodnotenie prvotných formúl ν platí $\overline{\nu}(B) = 1$. Keďže však $A \,\&\, \neg A$ je kontradikcia, tak platí aj $\overline{\nu}(A \,\&\, \neg A) = 0$, a preto $\overline{\nu}(B_1 \,\&\, B_2 \,\&\, \ldots \,\&\, B_n) = 0$. To znamená, že pre každé ohodnotenie prvotných formúl ν existuje i, $1 \leq i \leq n$ také, že $\overline{\nu}(B_i) = 0$, čiže T nie je splniteľná. □

Nasledujúca veta je zovšeobecnením Postovej vety pre formuly dokázateľné z pevnej množiny predpokladov.

VETA 3.8 (**o úplnosti**). *Nech je T množina výrokových formúl. Potom*

(a) *T je bezosporná práve vtedy, keď je splniteľná;*
(b) *pre ľubovoľnú formulu A platí $T \vdash A$ práve vtedy, keď $T \models A$.*

DÔKAZ. Najprv dokážeme časť (a). Nech je T bezosporná. Potom je podľa Lemy 3.6.b bezosporná aj každá jej konečná podmnožina. Teda podľa Lemy 3.7 je každá konečná podmnožina T splniteľná a podľa Vety 3.5 o kompaktnosti je T splniteľná.

Naopak, ak je T sporná, tak podľa Lemy 3.6.b existuje konečná podmnožina T_0 množiny T, ktorá je sporná. Potom podľa Lemy 3.7 je T_0 nesplniteľná a teda ani T nemôže byť splniteľná.

Teraz dokážeme časť (b). Nech $T \vdash A$. Keďže dôkaz je konečná postupnosť formúl, tak existuje konečná podmnožina T_0 množiny T taká, že $T_0 \vdash A$. Nech $T_0 = \{B_1, B_2, \ldots, B_n\}$. Podľa Lemy 2.13 platí $\vdash (B_1 \,\&\, B_2 \,\&\, \ldots \,\&\, B_n) \Rightarrow A$ a podľa Postovej vety $\vDash (B_1 \,\&\, B_2 \,\&\, \ldots \,\&\, B_n) \Rightarrow A$. Avšak podľa Lemy 3.4 $\{B_1, B_2, \ldots, B_n\} \vDash A$, čiže $T_0 \vDash A$ a teda aj $T \vDash A$.

Naopak, ak $T \nvdash A$, potom tiež $T \cup \{\neg A\} \nvdash A$. Totiž v opačnom prípade by sme mali:

1:	$T \cup \{\neg A\} \vdash A$	predpoklad
2:	$T \vdash \neg A \Rightarrow A$	VD1
3:	$\vdash (\neg A \Rightarrow \neg A) \Rightarrow ((\neg A \Rightarrow A) \Rightarrow A)$	A3
4:	$\vdash \neg A \Rightarrow \neg A$	Lema 2.1
5:	$\vdash (\neg A \Rightarrow A) \Rightarrow A$	MP4,3
6:	$T \vdash A$	MP2,5

čo je v spore s $T \nvdash A$.

Teda keďže $T \nvdash A$, tak aj $T \cup \{\neg A\} \nvdash A$. To značí, že $T \cup \{\neg A\}$ je bezosporná a podľa časti (a) je $T \cup \{\neg A\}$ splniteľná. Avšak podľa Poznámky 3 pred Lemou 3.4 potom máme $T \nvDash A$. □

Veta o úplnosti ukazuje, že sa nám podarilo zostrojiť syntakticky teóriu výrokovej logiky, a to tak, že zostrojená teória presne zodpovedá našim skúsenostiam o výrokovej logike.

Cvičenia

Cvičenie 3.1. Pomocou ohodnotení ν, podobne ako v Cvičení 1.2, ukážte, že ak platí $T \vDash A$ a $T \vDash A \Rightarrow B$, tak platí $T \vDash B$.

Cvičenie 3.2. Dokážte nasledujúce tautologické dôsledky:

a) $A \Rightarrow B,\ B \Rightarrow C \vDash A \Rightarrow C$ b) $A \Rightarrow (B \Rightarrow C) \vDash B \Rightarrow (A \Rightarrow C)$

Cvičenie 3.3. Dokážte:

a) $A \Rightarrow B \vDash (C \vee A) \Rightarrow (C \vee B)$
b) $A \Rightarrow B \vDash (C \,\&\, A) \Rightarrow (C \,\&\, B)$
c) $A \Rightarrow B,\ B \Rightarrow C \vDash \neg(A \,\&\, \neg C)$
d) $A \Rightarrow (B \Rightarrow C),\ A \Rightarrow B \vDash A \Rightarrow (A \Rightarrow C)$
a) $A \Rightarrow B,\ C \Rightarrow D \vDash (A \,\&\, C) \Rightarrow (B \,\&\, D)$

Cvičenie 3.4*. Dokážte, že axióma A3 nezávisí od A1 a A2, teda že neexistuje dôkaz A3 využívajúci len A1, A2 a modus ponens. (Navod: Uvažujte zobrazenie φ vynechávajúce symboly negácie $\neg$ a jeho dopad na dôkaz A3 z prvotných formúl pomocou A1, A2 a MP.)

4 PREDIKÁTOVÁ LOGIKA 1

Čosi z analýzy

Zamyslime sa nad výrazom

$$(\forall\varepsilon)(\exists\delta)\Big(\big(x\in\langle x_0-\delta, x_0+\delta\rangle\big)\Rightarrow\big(f(x)\in\langle f(x_0)-\varepsilon, f(x_0)+\varepsilon\rangle\big)\Big)$$

Čo toto tvrdenie znamená? Všimnime si, že nie je zapísané v jazyku výrokovej logiky, pretože využíva značky $\forall$ a $\exists$. Nuž a rozšírením výrokovej logiky o takéto značky sa budeme zaoberať v tejto časti.

Relácie a zobrazenia

Prv než sa začneme venovať predikátovej logike, definujeme si zopár množín (pojem množiny chápeme intuitívne, množina je teda skupina objektov).

Definícia. **Karteziánsky súčin** n množín $A_1, A_2, \ldots, A_n$ je množina

$$A_1\times A_2\times\cdots\times A_n=\{(x_1,x_2,\ldots,x_n);\ (x_1\in A_1)\ \&\ (x_2\in A_2)\ \&\ \ldots\ \&\ (x_n\in A_n)\}.$$

Všimnime si, že ak majú množiny $A_1, A_2, \ldots, A_n$ postupne $a_1, a_2, \ldots, a_n$ prvkov, tak karteziánsky súčin $A_1\times A_2\times\cdots\times A_n$ má práve $a_1\cdot a_2\cdot\ldots\cdot a_n$ prvkov.

Definícia. **n-árna relácia** na množine A je ľubovoľná podmnožina karteziánskeho súčinu $\underbrace{A\times A\times\cdots\times A}_{n\,A\text{-čiek}}$. Prvky n-árnej relácie zapisujeme ako usporiadané n-tice.

Definícia. **n-árna funkcia** (**zobrazenie**) na množine A je ľubovoľná podmnožina karteziánskeho súčinu $\underbrace{A\times A\times\cdots\times A}_{(n+1)\,A\text{-čiek}}$ taká, že ak sú $(a_1,\ldots,a_n,a_{n+1})$ a $(b_1,\ldots,b_n,b_{n+1})$ prvkami tejto relácie, pričom $a_i=b_i$ pre $i=1,2,\ldots,n$, tak aj $a_{n+1}=b_{n+1}$. Skutočnosť, že $(a_1,\ldots,a_n,a_{n+1})$ je prvkom funkcie f, zapisujeme $f(a_1,\ldots,a_n)=a_{n+1}$. Pritom n-tica $a_1,\ldots,a_n$ je argumentom funkcie f a a_{n+1} je jej hodnotou v tomto argumente.

V nasledujúcom texte budeme uvažovať aj nekonečné množiny, avšak tieto nikdy nebudú „príliš veľké“.

Definícia. Množina A je **spočítateľná** ak nemá viac prvkov (presnejšie, nemá väčšiu mohutnosť) ako množina všetkých prirodzených čísel $\mathbb{N}$.

Mohutnostiam (veľkostiam množín) sa v tomto texte nevenujeme. Ale spomeňme aspoň to, že množina racionálnych čísel je spočítateľná (ináč povedané, má práve toľko prvkov ako $\mathbb{N}$), zatiaľ čo množina reálnych čísel je väčšia.

Definície

Zjednodušene povedané, predikátová logika je výroková logika obohatená o kvantifikátory. Avšak, ako bude vidno neskôr, už aj tak jednoduché obohatenie nám situáciu značne skomplikuje.

Definícia. **Jazyk predikátovej logiky** (**jazyk prvého rádu**) tvoria:

Logické symboly:

- spočítateľne veľa symbolov pre **premenné** $x, y, x_1, z_1, \ldots$;
- **symboly pre logické spojky** $\neg$, $\&$, $\vee$, $\Rightarrow$ a $\Leftrightarrow$;
- **symboly pre kvantifikátory** $\forall$ (všeobecný, veľký) a $\exists$ (existenčný, malý).

Špeciálne symboly jazyka:

- **symboly pre predikáty** p, q, p_1, ... (pre každý je daná jeho árnosť);
- **symboly pre funkcie** f, g, f_1, ... (pre každý je daná jeho árnosť).

Pomocné symboly (,), [,] a čiarka.

Medzi logické symboly sa často radí aj symbol pre rovnosť $=$ a vtedy hovoríme o **jazyku s rovnosťou**.

Poznámka 1. Pod n-árnym predikátom sa myslí n-árna relácia.

Poznmka 2. Nulárne funkčné symboly sú konštanty (sú to funkcie bez argumentu), zatiaľ čo nulárne predikátové symboly sú logické konštanty (pravda a lož).

Príklad 1. Jazyk teórie množín je jazyk s rovnosťou s jediným špeciálnym symbolom, a tým je binárny predikát $\in$.

Príklad 2. Jazyk elementárnej aritmetiky (na $\mathbb{N}$) je jazykom s rovnosťou, ktorý má nasledujúce špeciálne symboly:

0 – nulárny funkčný symbol pre nulu;
S – unárny funkčný symbol pre funkciu nasledovníka;
$+, \cdot$ – binárne funkčné symboly pre sčítanie a násobenie.

Príklad 3. Ak by sme opisovali jazyk príbuzenských vzťahov medzi ľuďmi, tak tento jazyk by asi obsahoval unárne predikáty ŽENA, MUŽ a binárne predikáty RODIČ, MANŽEL.

Teda jazyk predikátovej logiky treba voliť tak, aby čo najlepšie odrážal študované skutočnosti.

Definícia. **Termy** jazyka predikátovej logiky L vznikajú konečným počtom aplikácií nasledujúcich pravidiel:

(T1) Každá premenná a konštanta (nulárny funkčný symbol) je term.
(T2) Ak f je n-árny funkčný symbol jazyka L, $n \geq 1$ a $t_1, t_2, \ldots, t_n$ sú termy jazyka L, tak $f(t_1, t_2, \ldots, t_n)$ je term jazyka L.

Poznámka. Výsledkom termu (po dosadení za premenné) je jeden prvok skúmanej množiny.

Príklad. V jazyku elementárnej aritmetiky sú termami 0; $S(x)$; $S(S(y))$; $S(0)$ – to je zrejme číslo 1; $S(S(0))$ – to je zrejme 2. Termom je aj $(S(x) \cdot y) + x$, ale $S(0, x)$, $+S(0)$, ani $=$ nie sú termy.

Definícia. **Formuly** sa budujú z termov a ostatných symbolov jazyka prvého rádu L použitím konečného počtu týchto pravidiel:

(F1) Ak je P n-árny predikátový symbol a $t_1, t_2, \ldots, t_n$ sú termy jazyka L, tak $P(t_1, t_2, \ldots, t_n)$ je formula jazyka L. Takúto formulu nazývame **atomická formula**.
(F2) Ak sú A a B formuly jazyka L, tak $\neg A$, $A \,\&\, B$, $A \vee B$, $A \Rightarrow B$ a $A \Leftrightarrow B$ sú formuly jazyka L.
(F3) Ak je x premenná a A je formula, tak $(\forall x)A$ a $(\exists x)A$ sú formuly jazyka L.

Dĺžka vytvorenia formuly pomocou pravidiel F1 až F3 sa volá **zložitosť formuly**.

Poznámka 1. Ak máme jazyk s rovnosťou, tak túto považujeme za špeciálny binárny predikát.

Poznámka 2. Formula je vlastne tvrdením a môžeme už uvažovať o jej pravdivosti. Avšak ak sa pýtame, či je A formulou, tak nás zaujíma len to, či A možno vytvoriť z termov pomocou pravidiel F1 až F3 a vôbec nás nezaujíma, čo by takáto formula mohla vyjadrovať (a či táto formula vôbec má zmysel).

Príklad. V jazyku elementárnej aritmetiky sú $x = 0$, $(S(x) + y) = S(x + y)$ a $(x + S(y)) = 0$ atomické formuly, zatiaľ čo $(\forall x)(\exists y)((S(x) + y) = S(x + y))$ a $\neg(\exists x)(S(x) = 0)$ sú formuly.

Definícia. Nech je A formula. Potom výskyt premennej x je vo formule A **viazaný**, ak je súčasťou podformuly tvaru $(\forall x)B$, alebo $(\exists x)B$ formuly A. Ak výskyt premennej x nie je viazaný, tak je **voľný**. Formula A je **otvorená** ak neobsahuje žiaden viazaný výskyt žiadnej premennej a A je **uzavretá** ak neobsahuje žiaden voľný výskyt žiadnej premennej.

PRÍKLAD. V jazyku elementárnej aritmetiky uvažujme nasledujúce formuly:

a) $(\forall x)(\exists y)(S(x) = y)$ – ide o uzavretú formulu, x aj y majú len viazaný výskyt.
b) $x = y$ – otvorená formula.
c) $S(0) + 0 = S(0)$ – je aj uzavretá aj otvorená, lebo neobsahuje žiadne premenné.
d) $(x \neq 0) \Rightarrow (\forall x)(x \cdot z \neq 0)$ – tu x má v prvej časti voľný výskyt a v druhej viazaný. Tie premenné x v prvej a v druhej časti sú vlastne rôzne. Táto formula nie je ani otvorená ani uzavretá.

Za premenné v matematike často dosadzujeme rôzne konštanty, prípadne iné výrazy (termy):

DEFINÍCIA. Nech sú $x_1, x_2, \ldots, x_n$ rôzne premenné a $t, t_1, t_2, \ldots, t_n$ nech sú termy jazyka prvého rádu L. Symbolom $t_{x_1,x_2,\ldots,x_n}[t_1, t_2, \ldots, t_n]$ označujeme term jazyka L, ktorý vznikne z t nahradením každého výskytu premennej x_i termom t_i pre všetky $i = 1, 2, \ldots, n$.

PRÍKLAD. V jazyku elementárnej aritmetiky ak je t term tvaru $(x + y) \cdot x$ a t_1, t_2, t_3 sú postupne $x + x$, $z \cdot y$, $y + z$, tak $t_{x,y}[t_1, t_2]$ je $((x + x) + (z \cdot y)) \cdot (x + x)$, zatiaľ čo $t_{z,y}[t_3, t_2]$ je $((y + z) + (z \cdot y)) \cdot (y + z)$ a podobne.

DEFINÍCIA. Ak je A formula, $x_1, x_2, \ldots, x_n$ sú premenné a $t_1, t_2, \ldots, t_n$ sú termy v jazyku prvého rádu L, tak $A_{x_1,x_2,\ldots,x_n}[t_1, t_2, \ldots, t_n]$ vznikne z A nahradením každého voľného výskytu premennej x_i termom t_i pre všetky $i = 1, 2, \ldots, n$.

PROBLÉM. Nech je A formula v jazyku elementárnej aritmetiky $(\exists y)(x = y + y)$ a nech je t term $y + x$. Formulu A možno interpretovať ako: „x je párne“. Avšak $A_x[t]$ je formula $(\exists y)(y + x = y + y)$, pričom táto nie je špeciálnym prípadom tvrdenia „$y + x$ je párne“, ale tvrdí, že „existuje y pre ktoré $x = y$“. (Podobný problém by sme mali, keby sme sa snažili substituovať y za x do formuly $(\exists y)(x \neq y)$.) Takýmto problémom sa budeme snažiť vyhnúť, a preto má zmysel nasledujúca definícia:

DEFINÍCIA. Term t je **substituovateľný** za x do formuly A ak pre každú premennú y z t žiadna podformula A tvaru $(\forall y)B$ ani $(\exists y)B$ neobsahuje voľný výskyt x. My budeme substituovať len substituovateľné termy a $A_{x_1,x_2,\ldots,x_n}[t_1, t_2, \ldots, t_n]$ nazveme **inštanciou** (**špeciálnym prípadom**) formuly A.

Skúmajme teraz význam formúl predikátovej logiky.

PRÍKLAD. Formula $(\forall x)(\exists u)(\exists v)((u \neq v)$ & (RODIČ(u, x)) & (RODIČ(v, x))) v jazyku príbuzenských vzťahov je pravdivá ak hovoríme o stavovcoch, ale nie ak je reč o živočíchoch s vegetatívnym rozmnožovaním (napríklad o nezmaroch).

DEFINÍCIA. **Interpretácia** (**realizácia**) $\mathfrak{M}$ jazyka L prvého rádu je daná:

(I1) Neprázdnou množinou M, ktorú nazývame **univerzum** (**nosič**). Je to množina hodnôt, ktoré nadobúdajú premenné. Prvky množiny M voláme **indivíduá**.

(I2) Zobrazením, ktoré každému n-árnemu funkčnému symbolu f z L priradí funkciu $f_{\mathfrak{M}} : M^n \to M$.

(I3) Zobrazením, ktoré každému n-árnemu predikátovému symbolu P z L priradí n-árnu reláciu $P_{\mathfrak{M}} \subseteq M^n$.

PRÍKLAD. V realizácii $\mathfrak{M}$ jazyka elementárnej aritmetiky by sme za nosič zvolili práve $\mathbb{N}$, nulárnemu funkčnému symbolu by sme priradili 0, symboly $+$ a $\cdot$ by reprezentovali bežné sčítanie a násobenie a pre funkciu nasledovníka S by sme zrejme volili $S_{\mathfrak{M}} : x \to x+1$.

DEFINÍCIA. Zobrazenie e množiny všetkých premenných do univerza M interpretácie $\mathfrak{M}$ nazývame **ohodnotením premenných**.

Keď už máme ohodnotenie premenných e, tak hodnotu tohoto ohodnotenia na terme t, $t[e]$, môžeme definovať indukciou podľa konštrukcie termu t:

1° Ak je t premenná x, tak $t[e] = e(x)$ a ak je t symbol nulárnej funkcie (konštanty), tak $t[e]$ je hodnota priradená tejto funkcii v realizácii $\mathfrak{M}$.

2° Ak je t term $f(t_1, \ldots, t_n)$, tak $t[e] = f_{\mathfrak{M}}(t_1[e], \ldots, t_n[e])$.

DEFINÍCIA. Nech je e ohodnotenie premenných v realizácii $\mathfrak{M}$ jazyka L. Zvoľme pevne $m \in M$ a premennú x z L. Potom $e(x/m)$ je ohodnotenie, ktoré sa od e líši len v tom, že premennej x nutne priradí m.

DEFINÍCIA (**Tarski**). Majme jazyk prvého rádu L. Nech je $\mathfrak{M}$ jeho realizácia s nosičom M a e je ohodnotenie premenných. Indukciou podľa zložitosti formuly definujeme **pravdivosť formuly** pri ohodnotení e (ak je formula A je pri ohodnotení e pravdivá, tak zapisujeme $\mathfrak{M} \vDash A[e]$, zatiaľ čo v opačnom prípade zapisujeme $\mathfrak{M} \nvDash A[e]$) takto:

(R1) Ak sú $t_1, t_2, \ldots, t_n$ termy v L a P je n-árny predikátový symbol rôzny od $=$, tak $\mathfrak{M} \vDash P(t_1, t_2, \ldots, t_n)[e]$ práve vtedy, keď $(t_1[e], t_2[e], \ldots, t_n[e]) \in P_{\mathfrak{M}}$.

(R1)′ $\mathfrak{M} \vDash (t_1 = t_2)[e]$ práve vtedy, keď $t_1[e]$ a $t_2[e]$ sú tie isté indivíduá z M.

(R2) Ak sú B a C formuly v L, tak $\mathfrak{M} \vDash \neg B[e]$ práve vtedy, keď neplatí $\mathfrak{M} \vDash B[e]$ (t.j. keď $\mathfrak{M} \nvDash B[e]$). $\mathfrak{M} \vDash (B \Rightarrow C)[e]$ práve vtedy, keď $\mathfrak{M} \nvDash B[e]$, alebo $\mathfrak{M} \vDash C[e]$. (Podobne sa definuje aj pravdivosť $B \,\&\, C$, $B \vee C$ a $B \Leftrightarrow C$ pri $\mathfrak{M}$ a e.)

(R3) Ak je x premenná v L a B je formula, tak $\mathfrak{M} \vDash (\forall x)B[e]$ práve vtedy, keď pre každé indivíduum m z M platí $\mathfrak{M} \vDash B[e(x/m)]$. Ďalej $\mathfrak{M} \vDash (\exists x)B[e]$ platí práve vtedy, keď pre nejaké indivíduum m z M platí $\mathfrak{M} \vDash B[e(x/m)]$.

LEMA 4.1. *Nech je L jazyk predikátovej logiky, $\mathfrak{M}$ je jeho realizácia a e je ohodnotenie premenných. Potom pre ľubovoľnú formulu A v L platí buď $\mathfrak{M} \models A[e]$, alebo $\mathfrak{M} \not\models A[e]$, avšak nikdy nie súčasne.*

DÔKAZ. Z definície Tarského plynie, že $\mathfrak{M} \not\models A[e]$ platí práve vtedy, keď neplatí $\mathfrak{M} \models A[e]$. □

Splniteľnosť formúl

Podobne, ako sme sa vo výrokovej logike venovali najprv tautológiám a až potom dokázateľným formuliam, budeme sa aj v predikátovej logike venovať najprv splniteľným formuliam a v časti 5 formuliam dokázateľným.

DEFINÍCIA. Formula A je **splnená** v $\mathfrak{M}$, označujeme $\mathfrak{M} \models A$, ak je pravdivá v $\mathfrak{M}$ pri ľubovoľnom ohodnotení e.

LEMA 4.2. *Nech je L jazyk predikátovej logiky, $\mathfrak{M}$ je jeho realizácia, A je formula v L a x je premenná. Potom $\mathfrak{M} \models A$ platí práve vtedy, keď $\mathfrak{M} \models (\forall x)A$.*

DÔKAZ. Nech platí $\mathfrak{M} \models A$. Chceme ukázať, že $\mathfrak{M} \models (\forall x)A$, teda že pre ľubovoľné ohodnotenie e platí $\mathfrak{M} \models (\forall x)A[e]$. Nech je teda e_0 ľubovoľné pevne zvolené ohodnotenie premenných prvkami z nosiča M realizácie $\mathfrak{M}$. Podľa definície platí $\mathfrak{M} \models (\forall x)A[e_0]$ práve vtedy, keď pre ľubovoľné $m \in M$ platí $\mathfrak{M} \models A[e_0(x/m)]$. Avšak $e_0(x/m)$ je tiež ohodnotenie a keďže $\mathfrak{M} \models A$, tak aj $\mathfrak{M} \models A[e_0(x/m)]$. Teda $\mathfrak{M} \models (\forall x)A$.

Naopak, nech platí $\mathfrak{M} \models (\forall x)A$. Potom pre každé ohodnotenie e a pre každé $m \in M$ platí $\mathfrak{M} \models A[e(x/m)]$. Zvoľme m_e tak, aby $m_e = e(x)$. Potom musí platiť aj $\mathfrak{M} \models A[e(x/m_e)]$, čiže $\mathfrak{M} \models A[e]$. Teda $\mathfrak{M} \models A$ □

POZNÁMKA 1. Platí $\mathfrak{M} \models A \Leftrightarrow \mathfrak{M} \models (\forall x)A$, ale neplatí $\mathfrak{M} \models (A \Rightarrow (\forall x)A)$! Ako príklad môže slúžiť jazyk L s jediným unárnym predikátovým symbolom P, s interpretáciou $\mathfrak{N}$ a nosičom $N = \{a, b\}$. Nech $a \in P_{\mathfrak{N}}$, ale $b \notin P_{\mathfrak{N}}$. Potom v $\mathfrak{N}$ neplatí $(\forall x)P(x)$ pre ľubovoľné ohodnotenie premenných (v skutočnosti formula $(\forall x)P(x)$ nezávisí od ohodnotenia – viď Tarského definíciu). Avšak ak je e zvolené tak, že $e(x) = a$, tak $\mathfrak{N} \models P(x)[e]$ a teda $\mathfrak{N} \not\models (P(x) \Rightarrow (\forall x)P(x))[e]$, čiže aj $\mathfrak{N} \not\models (P(x) \Rightarrow (\forall x)P(x))$.

POZNÁMKA 2. Nech je L jazyk predikátovej logiky, $\mathfrak{M}$ je jeho realizácia a A je formula v L. Keďže každú formulu vieme zostrojiť aplikovaním pravidiel (F1) až (F3) konečne veľakrát, tak každá formula má len konečne veľa premenných. Nech sú $x_1, x_2, \ldots, x_k$ všetky voľné premenné formuly A. Podľa Lemy 4.2 (aplikovanej k-krát) $\mathfrak{M} \models A$ platí práve vtedy, keď $\mathfrak{M} \models (\forall x_1)(\forall x_2)\ldots(\forall x_k)A$. To znamená, že nám stačí zisťovať, či sú v $\mathfrak{M}$ splnené uzavreté formuly.

DEFINÍCIA. Formula A je **splniteľná** v realizácii $\mathfrak{M}$ jazyka L, ak existuje ohodnotenie e premenných také, že $\mathfrak{M} \models A[e]$. Ak A nie je splniteľná, tak je **nesplniteľná**, t.j. pre každé ohodnotenie premenných e platí $\mathfrak{M} \models \neg A[e]$. Ak je A splnená

pri všetkých realizáciách s k-prvkovými nosičmi uvažovaného jazyka, tak A je k-**všeobecne platná**. Ak je A splnená pri všetkých realizáciách, tak A je **všeobecne platná** (**logicky pravdivá**), čo zapisujeme $\models A$. Ak v každej realizácii, kde je splnená B, je splnená aj A, tak A je **logický dôsledok** B, čo zapisujeme $B \models A$.

LEMA 4.3. *Nech sú A a B formuly v jazyku prvého rádu L. Ak premenná x nemá voľný výskyt v A, tak platí $\models (\forall x)(A \Rightarrow B) \Rightarrow (A \Rightarrow (\forall x)B)$.*

DÔKAZ. Podľa definície Tarského $\models (\forall x)(A \Rightarrow B) \Rightarrow (A \Rightarrow (\forall x)B)$ platí práve vtedy, keď v ľubovoľnej realizácii $\mathfrak{M}$ pre ľubovoľné ohodnotenie premenných e platí $\mathfrak{M} \models ((\forall x)(A \Rightarrow B) \Rightarrow (A \Rightarrow (\forall x)B))[e]$.

Majme teda ľubovoľnú realizáciu $\mathfrak{M}$ jazyka L a ľubovoľné ohodnotenie e premenných prvkami z nosiča realizácie $\mathfrak{M}$. Ak by platilo $\mathfrak{M} \not\models (\forall x)(A \Rightarrow B)[e]$, alebo $\mathfrak{M} \not\models A[e]$ tak by formula pri $\mathfrak{M}$ a e platila. Predpokladajme teda, že platí $\mathfrak{M} \models (\forall x)(A \Rightarrow B)[e]$ aj $\mathfrak{M} \models A[e]$. Potom pre ľubovoľný prvok m z nosiča realizácie $\mathfrak{M}$ platí $\mathfrak{M} \models (A \Rightarrow B)[e(x/m)]$. Keďže x nie je voľná v A (to znamená, že buď je v A viazaná, alebo tam vôbec nie je), tak z platnosti $\mathfrak{M} \models A[e]$ plynie platnosť $\mathfrak{M} \models A[e(x/m)]$. Avšak potom modus ponens formúl $\mathfrak{M} \models (A \Rightarrow B)[e(x/m)]$ a $\mathfrak{M} \models A[e(x/m)]$ dáva $\mathfrak{M} \models B[e(x/m)]$. Keďže m bol ľubovoľný prvok z nosiča realizácie $\mathfrak{M}$, tak podľa definície Tarského máme $\mathfrak{M} \models (\forall x)B[e]$. To znamená, že platí $\mathfrak{M} \models ((\forall x)(A \Rightarrow B) \Rightarrow (A \Rightarrow (\forall x)B))[e]$, a keďže na $\mathfrak{M}$ ani na e sme nekládli žiadne obmedzujúce podmienky, tak platí $\models (\forall x)(A \Rightarrow B) \Rightarrow (A \Rightarrow (\forall x)B)$. □

POZNÁMKA. Ak by x bola voľná v A v predošlej vete, tak tvrdenie nemusí platiť. Uvažujme jazyk predikátovej logiky L s jediným unárnym predikátovým symbolom P, s interpretáciou $\mathfrak{N}$ a nosičom $N = \{a, b\}$. Nech $a \in P_{\mathfrak{N}}$, $b \notin P_{\mathfrak{N}}$ a nech $A = B = P(x)$. Potom platí $\mathfrak{N} \models (\forall x)(P(x) \Rightarrow P(x))$, ale $\mathfrak{N} \not\models (\forall x)P(x)$. Preto pre ohodnotenie $e : x \to a$ máme $\mathfrak{N} \not\models ((\forall x)(P(x) \Rightarrow P(x)) \Rightarrow (P(x) \Rightarrow (\forall x)P(x)))[e]$, čiže $\mathfrak{N} \not\models (\forall x)(P(x) \Rightarrow P(x)) \Rightarrow (P(x) \Rightarrow (\forall x)P(x))$.

LEMA 4.4. *Nech je A formula v jazyku predikátovej logiky L, x nech je premenná a t je term substituovateľný do A za x. Potom $\models (\forall x)A \Rightarrow A_x[t]$.*

DÔKAZ. Nech je $\mathfrak{M}$ ľubovoľná interpretácia L a nech je e ľubovoľné ohodnotenie premenných prvkami z nosiča realizácie $\mathfrak{M}$. Ak $\mathfrak{M} \not\models (\forall x)A[e]$, tak platí $\mathfrak{M} \models ((\forall x)A \Rightarrow A_x[t])[e]$ a niet čo dokazovať. Teda nech $\mathfrak{M} \models (\forall x)A[e]$. To však znamená, že pre každý prvok m z nosiča realizácie $\mathfrak{M}$ platí $\mathfrak{M} \models A[e(x/m)]$. Nech je m_0 to indivíduum, ktoré realizuje term t v ohodnotení e, teda $m_0 = t[e]$. Potom platí aj $\mathfrak{M} \models A[e(x/m_0)]$, čo je vlastne $\mathfrak{M} \models (A_x[t])[e]$. Keďže $\mathfrak{M}$ aj e boli volené ľubovoľne, platí $\models (\forall x)A \Rightarrow A_x[t]$. □

Cvičenia

CVIČENIE 4.1. $S((x+S(0))\cdot(y\cdot S(0)))$ je term v jazyku elementárnej aritmetiky. Popíšte jeho konštrukciu.

Cvičenie 4.2. V tejto kapitole je množstvo príkladov v jazyku elementárnej aritmetiky. Zostrojte pre každý príklad analógie v jazyku teórie množín.

Cvičenie 4.3. Podobne, ako sa v Tarského definícii (v bode R2) definuje pravdivosť negácie a implikácie, definujte pravdivosť $B \,\&\, C$, $B \vee C$ a $B \Leftrightarrow C$ pri realizácii $\mathfrak{M}$ a ohodnotení e.)

Cvičenie 4.4. Pomocou pravdivostných tabuliek ukážte, že nasledujúca formula v jazyku predikátovej logiky s rovnosťou je 2-všeobecne platná, ale nie je 3-všeobecne platná:

$$(\neg(z = y) \,\&\, (\exists x)P(x)) \Rightarrow (P(z) \vee P(y))$$

(Potrebujete uvažovať všetky možné ohodnotenia e voľných premenných a všetky možné interpretácie unárneho predikátu P.)

Cvičenie 4.5. Zostrojte formulu, ktorá je k-všeobecne platná, ale nie je $(k+1)$-všeobecne platná.

Cvičenie 4.6. Zostrojte formulu v jazyku predikátovej logiky bez rovnosti, ktorá je 2-všeobecne platná, ale nie je 3-všeobecne platná.

Cvičenie 4.7. Úvahou ukážte, že nasledujúce formuly sú logicky pravdivé:
a) $((\exists x)(A \Rightarrow B)) \Rightarrow ((\forall x)A \Rightarrow (\exists x)B)$
b) $((\forall x)A \Rightarrow (\exists x)B) \Rightarrow ((\exists x)(A \Rightarrow B))$

Cvičenie 4.8. Úvahou ukážte, že ak x nie je voľná v B, tak nasledujúce formuly sú logicky pravdivé:
a) $((\forall x)(A \Rightarrow B)) \Leftrightarrow (((\exists x)A) \Rightarrow B)$ b) $((\exists x)(A \Rightarrow B)) \Leftrightarrow (((\forall x)A) \Rightarrow B)$

5 PREDIKÁTOVÁ LOGIKA 2

Príklad na rozmyslenie

PRÍKLAD. Divadelného predstavenia sa zúčastnilo n pánov a všetci si odložili svoje klobúky v šatni. Po predstavení bola šatniarka „v nálade“ a klobúky rozdávala náhodne. Aká je pravdepodobnosť, že žiaden pán nedostane svoj vlastný klobúk?

Ak nemáte náladu na počítanie, tak sa aspoň pokúste odhadnúť, aká môže byť tá pravdepodobnosť keď je n „veľmi veľké“ číslo. Presnejšie, pre n idúce do nekonečna, k čomu daná pravdepodobnosť konverguje?

Formálny systém predikátovej logiky

DEFINÍCIA. Nech je L jazyk predikátovej logiky. Za axiómy predikátovej logiky považujeme:

Axiómy výrokovej logiky:

(A1) $A \Rightarrow (B \Rightarrow A)$,
(A2) $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$,
(A3) $(\neg A \Rightarrow \neg B) \Rightarrow ((\neg A \Rightarrow B) \Rightarrow A)$,

kde A, B a C sú ľubovoľné formuly jazyka L.

Schému špecifikácie, ktorá pre ľubovoľnú formulu A, premennú x a term t substituovateľný do A za x má tvar

(ASŠ) $(\forall x)A \Rightarrow A_x[t]$.

Schému kvantifikácie implikácie, ktorá pre formuly A, B a premennú x, ktorá nie je voľná v A má tvar

(ASKI) $(\forall x)(A \Rightarrow B) \Rightarrow (A \Rightarrow (\forall x)B)$.

Odvodzovacími pravidlami sú:

Modus ponens:

(MP) z formúl A a $A \Rightarrow B$ odvoď formulu B.

Pravidlo zovšeobecnenia:

(PZ) pre ľubovoľnú premennú x odvoď z formuly A formulu $(\forall x)A$.

POZNÁMKA 1. Formulu $(\exists x)A$ považujeme len za skrátený zápis formuly $\neg[(\forall x)\neg A]$ a spojky $\&$, $\vee$ a $\Leftrightarrow$ prepisujeme tak isto ako vo formálnom systéme výrokovej logiky.

Poznámka 2. Symbolom $\vdash A$ značíme, že A možno odvodiť (dokázať) z axióm predikátovej logiky pomocou MP a PZ.

Poznámka 3. Keďže vo formálnom systéme predikátovej logiky sú obsiahnuté všetky axiómy výrokovej logiky a aj pravidlo modus ponens, tak všetky pravdivé formuly výrokovej logiky možno dokázať aj v predikátovej logike.

Poznámka 4. Keď hovoríme o jazyku predikátovej logiky s rovnosťou, tak prijímame ešte nasledujúce axiómy:

(E1) $(\forall x)(x = x)$.

(E2) Pre každý n-árny funkčný symbol f platí $(\forall x_1)\dots(\forall x_n)(\forall y_1)\dots(\forall y_n)$ $([(x_1{=}y_1)\ \&\ \dots\ \&\ (x_n{=}y_n)] \Rightarrow [f(x_1,\dots,x_n) = f(y_1,\dots,y_n)])$.

(E3) Pre každý n-árny predikátový symbol p platí $(\forall x_1)\dots(\forall x_n)(\forall y_1)\dots(\forall y_n)$ $([(x_1{=}y_1)\ \&\ \dots\ \&\ (x_n{=}y_n)] \Rightarrow [p(x_1,\dots,x_n) \Leftrightarrow p(y_1,\dots,y_n)])$.

Všimnite si, že (E2) a (E3) nie sú formuly a teda to nie sú axiómy. Ide vlastne o schémy axióm, z ktorých vzniknú axiómy ak zvolíme za f (alebo p) konkrétnu funkciu (predikát).

Veta 5.1 (**o korektnosti**). *Nech je L jazyk predikátovej logiky a nech je A formula v L. Ak je A dokázateľná vo formálom systéme predikátovej logiky, tak je logicky pravdivá (všeobecne platná).*

Dôkaz. Axiómy A1 až A3 sú tautológie výrokovej logiky a sú splnené v ľubovoľnej realizácii $\mathfrak{M}$ jazyka L pri ľubovoľnom ohodnotení premenných. Preto sú A1, A2 a A3 logicky pravdivé a podľa Liem 4.3 a 4.4 sú logicky pravdivé aj zvyšné dve axiómy.

Podľa Tarského definície pravdivosti implikácie je modus ponens korektné pravidlo a podľa Lemy 4.2 je korektné aj pravidlo zovšeobecnenia. To znamená, že všetky formuly, ktoré tvoria dôkaz A sú logicky pravdivé a preto je logicky pravdivá aj posledná z nich, čiže A. □

Veta 5.1 tvrdí, že ak $\vdash A$, tak $\vDash A$. Platí však aj opačné tvrdenie: ak $\vDash A$, tak $\vdash A$, ako dokázal K. Gödel v tridsiatych rokoch dvadsiateho storočia. Veta 5.4 je zovšeobecnením tohoto výsledku.

Teraz si ukážeme niekoľko príkladov na dôkazy formúl predikátovej logiky.

Lema 5.2 (pravidlo zavedenia $\forall$). *Nech sú A a B formuly predikátovej logiky. Ak platí $\vdash A \Rightarrow B$ a x nemá voľný výskyt v A, tak platí $\vdash A \Rightarrow (\forall x)B$.*

Dôkaz.

1:	$\vdash A \Rightarrow B$	predpoklad
2:	$\vdash (\forall x)(A \Rightarrow B)$	PZ1
3:	$\vdash (\forall x)(A \Rightarrow B) \Rightarrow (A \Rightarrow (\forall x)B)$	ASKI
4:	$\vdash (A \Rightarrow (\forall x)B)$	MP2,3 □

Lema 5.3. *Pre ľubovoľnú formulu A a term t substituovateľný do A za x platí $\vdash A_x[t] \Rightarrow (\exists x)A$.*

Dôkaz.

1:	$\vdash (\forall x)\neg A \Rightarrow \neg A_x[t]$	ASŠ
2:	$\vdash \neg\neg(\forall x)\neg A \Rightarrow (\forall x)\neg A$	Lema 2.6
3:	$\vdash \neg\neg(\forall x)\neg A \Rightarrow \neg A_x[t]$	Syl2,1
3′:	$\vdash \neg(\exists x)A \Rightarrow \neg A_x[t]$	definícia $(\exists x)B$
4:	$\vdash (\neg(\exists x)A \Rightarrow \neg A_x[t]) \Rightarrow (A_x[t] \Rightarrow (\exists x)A)$	VOOI
5:	$\vdash A_x[t] \Rightarrow (\exists x)A$	MP3′,4 □

Poznámka. Dokazovanie formúl predikátovej logiky nemusí byť vždy tak triviálne ako dokazovanie formúl vo výrokovej logike. Vo výrokovej logike sme totiž s výhodou využívali vetu o dedukcii, ktorú nemožno mechanicky zovšeobecniť na predikátovú logiku.

Hoci platí $A \vdash (\forall x)A$ (pravidlo zovšeobecnenia), tak neplatí $\vdash A \Rightarrow (\forall x)A$. Totiž ak by bola posledná formula dokázateľná, tak podľa Vety 5.1 o korektnosti by platilo $\vDash A \Rightarrow (\forall x)A$, čiže $A \Rightarrow (\forall x)A$ by bola splnená v každej realizácii jazyka predikátovej logiky, čo je v spore s realizáciou, ktorú sme zostrojili v Poznámke 1 za Lemou 4.2.

Ak je však A uzavretá formula, tak potom je možné dokázať, že $T \cup \{A\} \vdash B$ platí práve vtedy, keď platí $T \vdash A \Rightarrow B$.

V ďalšom sformulujeme základnú vetu predikátovej logiky, Gödelovu vetu o úplnosti. Avšak potrebujeme nato definovať ešte niekoľko pojmov.

Definícia. Ľubovoľne zvolenú množinu T formúl jazyka L nazývame **teória** (**teória prvého rádu**) v jazyku L. Formuly z T nazývame **špeciálne** (**vlastné**) **axiómy** teórie T.

Realizáciu $\mathfrak{M}$ jazyka L nazývame **modelom** teórie T práve vtedy, keď sú v nej splnené všetky axiómy teórie T, teda keď pre každé A z T platí $\mathfrak{M} \vDash A$. Ak je formula B splnená v každom modeli teórie T, tak B je **sémantickým dôsledkom** teórie T, čo zapisujeme $T \vDash B$.

Ak existuje dôkaz formuly A využívajúci axiómy teórie T ako predpoklady, tak A je **dokázateľná** v T, čo zapisujeme $T \vdash A$.

Poznámka. Ak by sme chceli dokazovať tvrdenia v jazyku elementárnej aritmetiky, tak by sme dokazovali formuly A, pre ktoré $T \vdash A$, kde T obsahuje špeciálne axiómy elementárnej aritmetiky. Teda T by zrejme obsahovala formulu $(\forall x)(\forall y)(x{+}y{=}y{+}x)$ (komutatívny zákon pre sčítanie), ďalej formulu $(\forall x)(\forall y)(\forall z)$ $[z \cdot (x + y) = (z \cdot x) + (z \cdot y)]$ (distributívny zákon) a podobne.

Definícia. Teória, v ktorej je dokázateľná každá formula jazyka tejto teórie sa nazýva **sporná**. Ak teória nie je sporná, tak je **bezosporná** (**konzistentná**).

Nech je T teória v jazyku L predikátovej logiky a nech je A formula v L. Potom ak $T \vdash A$, tak $T \vDash A$ (ide o jednoduché zovšeobecnenie Vety 5.1 o korektnosti). Teraz ak je teória T sporná, tak pre ľubovoľnú formulu B v jazyku L platí $T \vdash B$ aj $T \vdash \neg B$ a preto $T \vDash B$ aj $T \vDash \neg B$. To znamená, že v každej realizácii $\mathfrak{M}$ teórie T

je splnená aj formula B aj $\neg B$, a preto podľa Lemy 4.1 T nemá model. Zaujímavou je opačná implikácia: Ak teória T nie je sporná, tak má model.

VETA 5.4 (**Gödelova veta o úplnosti**). *V jazyku predikátovej logiky je teória bezosporná práve vtedy, keď má model.*

Dôkaz tohoto tvrdenia je ďaleko nad rámec nášho výkladu. Podobne bez dôkazu uvádzame aj nasledujúci dôsledok:

DÔSLEDOK. *Nech je T bezosporná teória a nech je A uzavretá formula v jazyku predikátovej logiky. Potom $T \models A$ platí práve vtedy, keď platí $T \vdash A$.*

POZNÁMKA. Dá sa dokázať dokonca viac, ako tvrdí Gödelova veta o úplnosti. Dá sa dokázať, že ak je teória bezosporná, tak má spočítateľný model (t. j. existuje jej model s nosičom M, ktorý je spočítateľnou množinou). Toto tvrdenie sa nazýva Lowenheim-Skolemova veta.

Záverom poznamenajme, že predikátová logika sa niekedy nazýva aj **logika prvého rádu**. Jazyk logiky prvého rádu obsahuje len premenné pre indivíduá, ale už nie pre skupiny indivíduí, a preto takéto skupiny nemožno v jazyku prvého rádu ani kvantifikovať. Ak však rozšírime jazyk prvého rádu o premenné pre skupiny indivíduí, dostaneme jazyk logiky druhého rádu. Jazyk logiky tretieho rádu už obsahuje premenné pre skupiny skupín indivíduí a podobne.

PRÍKLAD. V jazyku elementárnej aritmetiky nie sme schopní sformulovať tvrdenie: Každá konečná podmnožina množiny prirodzených čísel je ohraničená. To preto, lebo nemáme premenné pre skupiny prirodzených čísel.

Zákon nula-jedna pre grafy

Výklad venovaný predikátovej logike zakončíme veľmi peknou aplikáciou. Najprv si však zavedieme jednu matematickú štruktúru.

DEFINÍCIA. **Graf** G je usporiadaná dvojica množín, $G = (V(G), E(G))$, kde $V(G)$ je ľubovoľná konečná množina a $E(G)$ je nejaká množina (neusporiadaných) dvojíc prvkov z $V(G)$. Prvky $V(G)$ sa obyčajne nazývajú **vrcholy grafu** a prvky $E(G)$ sú **hrany grafu**.

POZNÁMKA. Hranovú množinu grafu G môžeme definovať aj tak, že $E(G)$ je podmnožinou karteziánskeho súčinu $V(G) \times V(G)$, pričom $(v, v) \notin E(G)$ pre žiadne $v \in V(G)$ a ak $(v, u) \in E(G)$ tak aj $(u, v) \in E(G)$. Potom každé dva páry dvojíc (u, v) a (v, u) predstavujú jednu hranu.

Teraz sa môžeme vrátiť k predikátovej logike.

Definícia. Jazyk teórie grafov prvého rádu L_G je jazyk predikátovej logiky s rovnosťou s jediným špeciálnym symbolom, ktorým je binárny predikát I. Zápis $I(x,y)$ interpretujeme „x je spojené hranou s y“ ((x,y) je hranou grafu).

Špeciálne axiómy sú dve:

(ŠA1) $(\forall x)\neg I(x,x)$ (čiže v grafe nie sú slučky);
(ŠA2) $(\forall x)(\forall y)[I(x,y) \Leftrightarrow I(y,x)]$ (hrany sú neorientované).

Poznámka. Všimnime si, že axiómy ŠA1 a ŠA2 sme už spomínali, keď sme definovali $E(G)$ ako podmnožinu karteziánskeho súčinu $V(G) \times V(G)$.

Vlastnosti, ktorými sa budeme zaoberať, sú uzavreté formuly v jazyku L_G.

Príklady vlastností sformulovaných v L_G.

(a) $(\forall x)(\exists y)I(x,y)$ (každý vrchol grafu je v aspoň jednej hrane);
(b) $[(\exists x)(\exists y)\neg I(x,y)] \,\&\, [(\forall x)(\forall y)(I(x,y) \vee (\exists z)[I(x,z) \,\&\, I(z,y)])]$
(graf má priemer 2, čiže z každého vrchola sa vieme dostať do ľubovoľného iného vrchola tak, že sa pri tom „prejdeme“ po nanajvýš dvoch hranách).

Príklady vlastností, ktoré nevieme sformulovať v jazyku L_G.

(a) graf je Hamiltonovský, čiže obsahuje takú cyklickú prechádzku, počas ktorej navštívime každý vrchol práve raz (vieme zapísať podmienku, že všetky vrcholy sú stupňa 2, ale nevieme zapísať, že takto dostaneme jedinú cyklickú prechádzku);
(b) n-vrcholový graf má aspoň $\binom{n}{2}/2$ hrán (nevieme zapísať počet vrcholov grafu).

Keďže naša aplikácia sa bude zapodievať náhodnými grafmi, potrebujeme definovať pravdepodobnostný priestor, v ktorom sa budeme pohybovať.

Definícia. Náhodný graf $G_{n,p}$, $n \in \mathbb{N}$ a $0 < p < 1$, je graf na n vrcholoch, v ktorom je každá dvojica vrcholov spojená hranou s pravdepodobnosťou p. (Teda s pravdepodobnosťou $1-p$ sú dva vrcholy nesusedné.)

My samozrejme nevieme, ako vyzerá graf $G_{n,p}$, ani aké má vlastnosti. Vieme však, že pravdepodobnosť toho, že $G_{n,p}$ má všetky možné hrany (čiže graf je kompletný) je $p^{\binom{n}{2}}$; $G_{n,p}$ nemá vôbec žiadnu hranu (je diskrétny) s pravdepodobnosťou $(1-p)^{\binom{n}{2}}$ atď.

Veta 5.5 (Zákon nula-jedna pre grafy). *Nech je A uzavretá formula v jazyku prvého rádu L_G a nech je p konštanta, $0 < p < 1$. Potom platí:*

$$\lim_{n\to\infty} Pr[G_{n,p} \text{ má vlastnosť } A] = \begin{cases} 0 \\ 1 \end{cases}$$

Ináč povedané, pre n idúce do nekonečna buď „skoro všetky grafy“ majú vlastnosť A, alebo ju nemá „skoro žiaden“ graf. Takto platí, že skoro všetky grafy majú

priemer 2, skoro všetky grafy obsahujú daný k-vrcholový graf ako svoju časť (podgraf), skoro žiaden graf neobsahuje izolované vrcholy (také, ktoré nie sú v žiadnej hrane), atď.

POZNÁMKA. Dôkaz Vety 5.5 pomocou Lowenheim-Skolemovej vety nie je ťažký. Avšak využíva grafy, pre ktoré je $V(G)$ nekonečná (hoci spočítateľná) množina.

Teraz sa môžeme vratiť k príkladu zo začiatku kapitoly. Podľa našich skúseností väčšina študentov háda, že pre n idúce do nekonečna sa pravdepodobnosť javu, že žiaden pán nedostane svoj vlastný klobúk, blíži k 1, respektíve k 0. Je to dobrý odhad, lebo tvrdenia podobné zákonu nula-jedna pre grafy sa dajú sformulovať aj pre iné oblasti matematiky. Bohužiaľ, na klobúky sa toto napasovať nedá. V nasledujúcom riešení využívame čosi z kombinatoriky a čosi z matematickej analýzy.

RIEŠENIE. Ak označíme P_n pravdepodobnosť udalosti, že predstavenia sa zúčastnilo n pánov a žiaden z nich nedostal svoj vlastný klobúk, tak aplikáciou princípu inklúzie a exklúzie dostaneme relatívnu početnosť:

$$P_n = \frac{1}{n!}\sum_{i=0}^{n}(-1)^i\binom{n}{i}(n-i)! = \sum_{i=0}^{n}\frac{(-1)^i}{i!}, \qquad \text{čiže} \qquad \lim_{n\to\infty}(P_n) = \sum_{i=0}^{\infty}\frac{(-1)^i}{i!},$$

čo je známy McLaurinov rad funkcie e^{-x} v bode $x = 1$. Teda

$$\lim_{n\to\infty}(P_n) = \frac{1}{e},$$

kde $e = 2,718281828\ldots$ je známa Eulerova konštanta.

Cvičenia

CVIČENIE 5.1. V jazyku L_G sformulujte vlastnosť: Graf má každý vrchol stupňa aspoň 2 (každý vrchol patrí aspoň 2 rôznym hranám).

CVIČENIE 5.2. Vytvorte si ľubovoľný graf H a následne v L_G sformulujte vlastnosť: Graf obsahuje H ako svoju časť (podgraf).

CVIČENIE 5.3. Akým formuliam zodpovedajú základné typy matematických dôkazov, čiže dôkaz priamo, nepriamo a sporom? Pokúste sa v rozličných dôkazoch, prezentovaných na ďalších prednáškach, vystopovať formuly výrokovej, respektíve predikátovej logiky.

6 TEÓRIA MNOŽÍN

Holičov problém

Istý holič v jednom malom mestečku si vyvesil nad dvere nápis: „Holím práve tých ľudí v našom meste, ktorí sa neholia sami“. Nápis vypadá na pohľad rozumne, ale existuje množina takýchto ľudí? (Uvažujte, či do tejto množiny holič patrí, alebo nepatrí.)

Intuitívna teória množín a jej paradoxy

Definícia. Pod **množinou** M rozumieme súbor objektov určených buď nejakou vlastnosťou, alebo vymenovaním. O týchto objektoch potom tvrdíme, že sú **prvkami** množiny M, čo zapisujeme $x \in M$ a čítame „x je prvkom množiny M“. Skutočnosť, že neplatí x je prvkom množiny M zapisujeme $x \notin M$ a čítame „x nie je prvkom množiny M“.

Poznamenajme, že pojem množina sme takto intuitívne chápali už v predošlej kapitole, kde sme tento pojem používali.

Príklady množín.

a) $A_1 = \{\text{Jano, Juro, Jožo}\}$ – je daná vymenovaním svojich troch prvkov, pričom pomocné symboly { a } sa volajú **množinové zátvorky**.
b) $A_2 = \{x;\ x \text{ je človek a } x \text{ býva v Bratislave}\}$ – je daná vlastnosťou, ktorú spĺňajú všetky jej prvky.

Niektoré množiny označujeme špeciálnymi symbolmi:

c) $\mathbb{N}$ – množina prirodzených čísel $\{0, 1, 2, \dots\}$
d) $\mathbb{Z}$ – množina celých čísel
e) $\mathbb{Q}$ – množina racionálnych čísel
f) $\mathbb{R}$ – množina reálnych čísel
g) $\mathbb{C}$ – množina komplexných čísel

Niektoré množiny môžeme opísať viacerými spôsobmi:

h) $A_3 = \{2x |\ x \in \mathbb{Z}\} = \{2x;\ x \in \mathbb{Z}\} = \{\dots, -4, -2, 0, 2, 4, \dots\}$

Vo všeobecnosti môžeme písať $A = \{x|\, P(x)\}$, kde $P(x)$ je „rozumná“ vlastnosť. Má to však háčik. Uvedieme takzvaný

Russelov paradox. Prvkami množiny A môžu byť opäť množiny. Napríklad $a \in \{a, b, c\}$, kde a, b aj c sú množiny. Podobne $\{a, b, c\} \in \{\{a, b, c\}, \{u, v\}\}$ atď. Pritom $\{a, b, c\} \notin \{a, b, c\}$. Čiže existuje množina x, pre ktorú $x \notin x$. Vlastnosť $P(x) :\ x \notin x$ vyzerá teda ako rozumná vlastnosť. Utvorme $M = \{x|\, P(x)\}$, čiže $M = \{x|\, x \notin x\}$. Zjavne do M patria všetky známe množiny: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{C}$, $A_1, \ldots$ Ako je to však so samotnou množinou M? Rozoberme obidva možné prípady:

(1) ak $M \in M$, tak M spĺňa vlastnosť, ktorou je M definovaná, čiže $M \notin M$;
(2) ak $M \notin M$, tak M opäť spĺňa vlastnosť, ktorou je M definovaná a preto $M \in M$.

Teda neplatí ani $M \in M$ ani $M \notin M$, z čoho plynie, že M nemôže byť množina. Preto vlastnosťou $P(x)$ nemožno definovať množinu.

Poznámka 1. Ak by množina M v predošlom príklade existovala, tak by bola „množinou všetkých množín“.

Poznámka 2. Russelovmu paradoxu sa možno vyhnúť axiomatickou výstavbou teórie množín. Takýto prístup sme volili pri výrokovej logike a nemali sme s ním väčšie problémy. Pri predikátovej logike sa axiomatická výstavba ukázala byť už o dosť náročnejšia. Nuž a pri teórii množín je axiomatický systém taký komplikovaný, že na jeho vybudovanie by sme potrebovali sériu niekoľkých prednášok.

Poznámka 3. My Russelov paradox (množinu všetkých množín) obídeme tak, že všetky naše množiny budú podmnožinami istého **univerza** $\mathcal{U}$, pričom toto $\mathcal{U}$ bude definitoricky množina. Napriek tomu sa ešte stále môže stať, že množina M nebude existovať, ak vlastnosť P nie je „dostatočne rozumná“ (pozri príklad v úvode tejto state.)

Základné množinové vzťahy, operácie a identity

V tejto časti zavedieme základné množinové operácie. Budeme dôsledne využívať predikátovú logiku a skutočnosť, že s výrokmi už vieme dobre narábať.

Definícia. Nech sú A a B množiny. Potom A **sa rovná** B práve vtedy, keď A aj B obsahujú rovnaké prvky. Teda:

$$A = B \Leftrightarrow [(\forall x)((x \in A) \Leftrightarrow (x \in B))]\,.$$

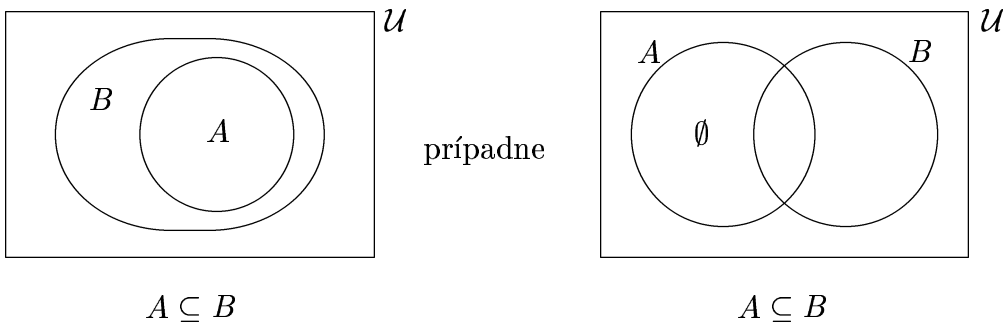
Ďalej A je **podmnožinou** B, ak každý prvok množiny A je aj prvkom B:

$$A \subseteq B \Leftrightarrow [(\forall x)((x \in A) \Rightarrow (x \in B))]\,.$$

Ak $A \subseteq B$ a $A \neq B$, tak A je **vlastnou podmnožinou** B, čo zapisujeme $A \subset B$.

Poznámka 1. Všimnime si, že $A = B \Leftrightarrow ((A \subseteq B)\ \&\ (B \subseteq A))$.

Poznámka 2. Vzťah $A \subseteq B$ možno znázorniť (podobne ako ďalšie množinové vzťahy) pomocou **Vennových diagramov**. V týchto diagramoch množiny reprezentujeme oblasťami (pokiaľ možno súvislými) roviny. Na Obrázku 1 sú dva rôzne Vennove diagramy pre $A \subseteq B$.



$A \subseteq B$ $\qquad\qquad$ $A \subseteq B$

Obrázok 1

Definíca. Nech sú A a B množiny. **Zjednotením** A a B nazveme množinu všetkých tých prvkov, ktoré patria aspoň do jednej z nich:

$$A \cup B = \{x;\ (x \in A) \vee (x \in B)\}$$

prípadne

$$(\forall x)[(x \in A \cup B) \Leftrightarrow ((x \in A) \vee (x \in B))].$$

Prienikom A a B nazveme množinu tých prvkov, ktoré patria do obidvoch množín:

$$A \cap B = \{x;\ (x \in A)\ \&\ (x \in B)\}.$$

Prázdna množina je taká, ktorá neobsahuje žiaden prvok. Označujeme ju $\emptyset$, alebo $\{\}$. Ak $A \cap B = \emptyset$, tak množiny A a B sú **disjunktné**.

Veta 6.1. *(a) Prázdna množina je podmnožinou ľubovoľnej množiny.*
(b) Existuje práve jedna prázdna množina.

Dôkaz. Najprv dokážeme časť (a) sporom. Nech existuje množina X taká, že neplatí $\emptyset \subseteq X$. Teda podľa definície podmnožiny neplatí $(\forall x)((x{\in}\emptyset) \Rightarrow (x{\in}X))$, a teda existuje nejaký prvok, označme si ho x_0, taký, že $(x_0{\in}\emptyset)\ \&\ \neg(x_0{\in}X)$. (Takýto prvok x_0 budeme nazývať svedkom daného vzťahu.) Keďže však $\emptyset$ neobsahuje žiaden prvok, tak nemôže platiť $x_0 \in \emptyset$. Dostali sme spor, a preto je prázdna množina podmnožinou ľubovoľnej množiny.

Teraz dokážeme časť (b) priamo. Nech sú A_1 a A_2 dve prázdne množiny. Potom podľa už dokázanej časti (a) platí $A_1 \subseteq A_2$ a aj $A_2 \subseteq A_1$. Teda pre ľubovoľné x platí $(x{\in}A_1) \Rightarrow (x{\in}A_2)$ a aj $(x{\in}A_2) \Rightarrow (x{\in}A_1)$. Podľa definície z kapitoly 2 však $B \Leftrightarrow C$ platí práve vtedy, keď platí $(B{\Rightarrow}C)\ \&\ (C{\Rightarrow}B)$, a preto $(x{\in}A_2) \Leftrightarrow (x{\in}A_1)$. Keďže na voľbu x sme nekládli žiadne obmedzenia, dostali sme $(\forall x)((x{\in}A_1) \Leftrightarrow (x{\in}A_2))$, čo podľa definície rovnosti dvoch množín znamená, že $A_1 = A_2$. $\square$

Definícia. Nech je A množina, $A \subseteq \mathcal{U}$. **Doplnkom** A vzhľadom na $\mathcal{U}$ je množina tých prvkov z $\mathcal{U}$, ktoré nepatria do A:

$$A^c = \{x;\ \neg(x \in A)\} = \{x;\ x \notin A\}.$$

Nech sú A a B množiny. **Rozdielom** A a B nazývame množinu tých prvkov A, ktoré nepatria do B:

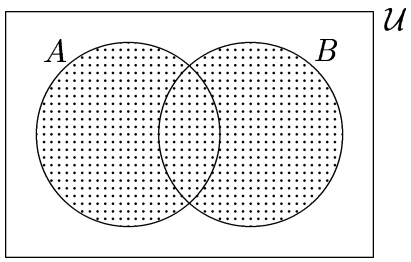
$$A - B = \{x;\ (x \in A)\ \&\ (x \notin B)\}.$$

Symetrická diferencia množín A a B je:

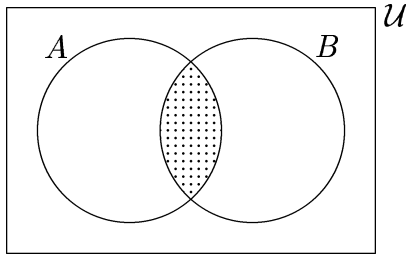
$$A \div B = \{x;\ [(x \in A)\ \&\ (x \notin B)] \vee [(x \notin A)\ \&\ (x \in B)]\}.$$

Poznámka. Priamo z definície možno nahliadnuť, že pre rozdiel a symetrický rozdiel platí $A - B = A \cap B^c$ a $A \div B = (A - B) \cup (B - A)$.

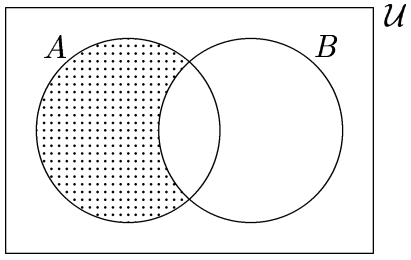
Na Obrázku 2 uvádzame Vennove diagramy práve definovaných pojmov.



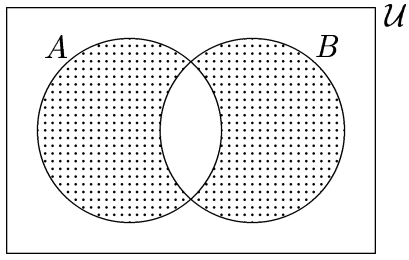
$A \cup B$



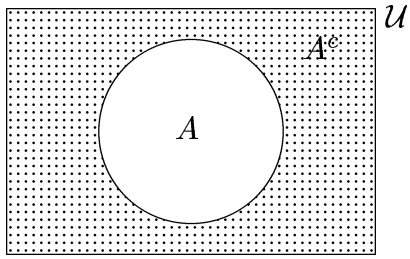
$A \cap B$



$A - B$



$A \div B$



A^c

Obrázok 2

VETA 6.2. *Nech sú A, B a C ľubovoľné množiny. Potom platí:*

(a)	$A \cup A = A$		*idempotentnosť*
(b)	$A \cap A = A$		*idempotentnosť*
(c)	$A \cup B = B \cup A$		*komutatívnosť*
(d)	$A \cap B = B \cap A$		*komutatívnosť*
(e)	$A \cup (B \cup C) = (A \cup B) \cup C$		*asociatívnosť*
(f)	$A \cap (B \cap C) = (A \cap B) \cap C$		*asociatívnosť*
(g)	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$		*distributívnosť*
(h)	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$		*distributívnosť*
(ch)	$A \subseteq A \cup B$	$B \subseteq A \cup B$	
(i)	$A \cap B \subseteq A$	$A \cap B \subseteq B$	
(j)	$(A \cup B)^c = (A^c \cap B^c)$		*de Morganov zákon*
(k)	$(A \cap B)^c = (A^c \cup B^c)$		*de Morganov zákon*
(l)	$(A^c)^c = A$		*zákon involúcie*
(m)	$A \cup \mathcal{U} = \mathcal{U}$	$A \cap \emptyset = \emptyset$	*zákony nuly*
(n)	$A \cup \emptyset = A$	$A \cap \mathcal{U} = A$	*zákony jednotky*
(o)	$A \cap A^c = \emptyset$	$A \cup A^c = \mathcal{U}$	*zákony doplnku*
(p)	$A \cap (A \cup B) = A$		*absorbčný zákon*
(q)	$A \cup (A \cap B) = A$		*absorbčný zákon*

DÔKAZ. Všetky tvrdenia možno dokázať tak, že rozpíšeme obidve strany danej identity až na výroky, ktoré budú ekvivalentné. Z estetických dôvodov však budeme rozpisovať len jednu stranu na výrok, ktorý nahradíme výrokom s týmto ekvivalentným a upravíme na druhú stranu požadovanej rovnosti.

Dokážeme tvrdenia (j), (p) a (q). Dôkazy ostatných tvrdení sú analogické, urobte si ich ako cvičenie.

Dôkaz (j): Podľa definície doplnku $x \in (A \cup B)^c$ platí práve vtedy, keď $\neg(x \in A \cup B)$ a toto platí podľa definície zjednotenia práve vtedy, keď $\neg((x{\in}A) \vee (x{\in}B))$. To sme však už prešli k výroku tvaru $\neg(a \vee b)$, ktorý je ekvivalentný výroku $\neg a \;\&\; \neg b$. Preto $\neg((x{\in}A) \vee (x{\in}B))$ platí práve vtedy, keď $\neg(x{\in}A) \;\&\; \neg(x{\in}B)$. Avšak to platí podľa definície doplnku práve vtedy, keď $(x{\in}A^c) \;\&\; (x{\in}B^c)$. Posledný vzťah je podľa definície prieniku len iným zápisom vzťahu $x \in A^c \cap B^c$. Keďže na voľbu x sme nekládli žiadne obmedzenia, dokázali sme $(\forall x)[x \in (A \cup B)^c \Leftrightarrow x \in (A^c \cap B^c)]$, čo podľa definície rovnosti množín znamená, že $(A \cup B)^c = (A^c \cap B^c)$.

Dôkaz (p): Nasledujúce tvrdenia sú navzájom ekvivalentné: $[x{\in}A{\cap}(A{\cup}B)] \Leftrightarrow$ $\Leftrightarrow [(x{\in}A) \;\&\; (x{\in}A{\cup}B)] \Leftrightarrow [(x{\in}A) \;\&\; ((x{\in}A) \vee (x{\in}B))] \Leftrightarrow (x{\in}A)$, pričom posledná ekvivalencia je ekvivalenciou medzi výrokmi: $a \;\&\; (a \vee b) \Leftrightarrow a$ (dokážte, že ide o tautológiu). Teda $(\forall x)[(x{\in}A{\cap}(A{\cup}B)) \Leftrightarrow (x{\in}A)]$, čo značí $A \cap (A \cup B) = A$.

Dôkaz (q): Tu využijeme predchádzajúce identity, hoci aj túto identitu možno dokázať priamo. Platí $A \cup (A \cap B) = (A \cup A) \cap (A \cup B) = A \cap (A \cup B) = A$, pričom pri prvej rovnosti sme použili identitu (h), pri druhej (a) a pri tretej (p). □

DEFINÍCIA. Nech je A množina. **Potenčná množina** množiny A, $\mathcal{P}(A)$, je množina všetkých podmnožín množiny A.

PRÍKLAD. Ak $A = \{\square, \triangle\}$, tak $\mathcal{P}(A) = \{\emptyset, \{\square\}, \{\triangle\}, \{\square, \triangle\}\}$.

POZNÁMKA. Všimnime si, že ak je A konečná množina s n prvkami, tak $\mathcal{P}(A)$ má 2^n prvkov.

Binárne relácie a zobrazenia

DEFINÍCIA. **Binárna relácia** R z množiny A do množiny B je ľubovoľná podmnožina karteziánskeho súčinu $A \times B$. Množina A je **oborom** (**množinou vzorov**, **definičným oborom**) a B je **kooborom** (**množinou obrazov**, **množinou hodnôt**) relácie R.

POZNÁMKA. Ak je R relácia, tak niekedy namiesto presného $(a, b) \in R$ zapisujeme infixne aRb.

Relácia môže byť daná buď vymenovaním svojich prvkov, prípadne maticou, orientovaným grafom, alebo iným spôsobom.

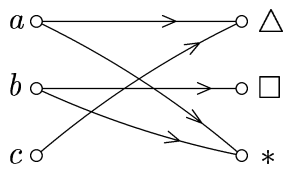
PRÍKLAD. Nech $A = \{a, b, c\}$, $B = \{\triangle, \square, *\}$ a nech $R = \{(a, \triangle), (a, *), (b, \square), (b, *), (c, \triangle)\}$.

Tejto relácii zodpovedá obdĺžniková tabuľka (**matica**) M_R, ktorej prvky majú len hodnoty 0 a 1, pozri Obrázok 3. V i-tom riadku a j-tom stĺpci je jednotka práve vtedy, keď je i-ty prvok A v relácii s j-tym prvkom z B. Takéto matice sa nazývajú **Booleove**.

Relácii R zodpovedá aj **orientovaný graf** na Obrázku 3. V tomto grafe idú šípy z vrcholov označeých prvkami A do vrcholov označených prvkami B. Pritom medzi dvoma prvkami je šíp práve vtedy, keď sú tieto prvky v relácii.

	$\triangle$	$\square$	$*$
a	1	0	1
b	0	1	1
c	1	0	0

matica pre R



graf pre R

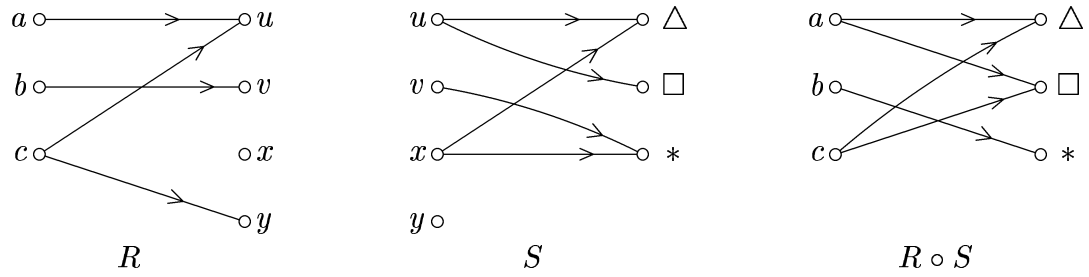
Obrázok 3

Uvažujme dve relácie. Prvá spočíva z predmetov, ktoré si študenti zapisujú (každý študent si zapíše nejaké predmety do indexu). Druhá relácia pozostáva z učiteľov, ktorí dostanú tieto predmety do svojho úväzku (každý predmet musí niekto učiť). Zložením týchto relácií dostávame reláciu medzi študentami a učiteľmi (každého študenta budú učiť nejakí učitelia).

Definícia. Nech je R binárna relácia z A do B a S je binárna relácia z B do C. Potom tieto relácie možno **zložiť** a týmto zložením dostávame reláciu $T = R \circ S$ z A do C:

$$T = R \circ S = \{(a, c);\ (\exists b)[(b \in B)\ \&\ ((a, b) \in R)\ \&\ ((b, c) \in S)]\}$$

Príklad 1. Majme dve relácie R a S definované pomocou orientovaných grafov, pozri Obrázok 4. Nech je R relácia z $\{a, b, c\}$ do $\{u, v, x, y\}$ a S je relácia z $\{u, v, x, y\}$ do $\{\triangle, \square, *\}$. „Zlepme“ grafy relácií R a S v prvkoch množiny $\{u, v, x, y\}$. Potom pre $k \in \{a, b, c\}$ a $l \in \{\triangle, \square, *\}$ platí $(k, l) \in R \circ S$ práve vtedy, keď v „zlepenom grafe“ existuje orientovaná cesta z k do l, viď Obrázok 4.



Obrázok 4

Príklad 2. Nech sú R a S tie isté relácie ako v predchádzajúcom príklade. Potom v maticovej reprezentácii

$$M_R = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \qquad \text{a} \qquad M_S = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Maticu zloženej relácie $M_{R \circ S}$ možno získať Booleovym súčinom matíc M_R a M_S. Nech $T = R \circ S$ a $r_{i,j}$ (resp. $s_{i,j}$ a $t_{i,j}$) je prvok v i-tom riadku a j-tom stĺpci matice M_R (resp. M_S a M_T). Potom $t_{i,j} = \bigvee_{k=1}^{n}(r_{i,k}\ \&\ s_{k,j})$, kde M_R je matica typu $m \times n$, M_S je typu $n \times o$ a M_T je typu $m \times o$. Teda:

$$M_R \cdot M_S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} = M_{R \circ S} = M_T\,.$$

Poznámka. Keď skladáme relácie, tak postupujeme zľava doprava, teda $R \circ S$ znamená „najprv R, potom S“. Občas sa stretneme aj s opačným skladaním, ktoré je mimoriadne vhodné pre funkcie, kde sa často zapisuje $f(g(x))$ a znamená to „na x aplikuj najprv g a potom f“.

VETA 6.3. *Nech sú A, B, C a D množiny a pre relácie R, S a T platí $R \subseteq A \times B$, $S \subseteq B \times C$ a $T \subseteq C \times D$. Potom $(R \circ S) \circ T = R \circ (S \circ T)$, čiže skladanie relácií je asociatívne.*

DÔKAZ. Stačí dokázať $(R \circ S) \circ T \subseteq R \circ (S \circ T)$ a $(R \circ S) \circ T \supseteq R \circ (S \circ T)$. Dokážeme prvú inklúziu, druhá sa dokazuje analogicky.

Nech $(a, d) \in (R \circ S) \circ T$. To značí, že existuje $c \in C$ také, že $(a, c) \in R \circ S$ a $(c, d) \in T$. Keďže $(a, c) \in R \circ S$, tak existuje $b \in B$ také, že $(a, b) \in R$ a $(b, c) \in S$. Teda $(a, b) \in R$, $(b, c) \in S$ a $(c, d) \in T$. Potom však $(b, d) \in S \circ T$, z čoho plynie $(a, d) \in R \circ (S \circ T)$. □

DEFINÍCIA. Nech je $R \subseteq A \times B$ binárna relácia. **Opačnou reláciou** (**inverznou reláciou**) k R je relácia

$$R^{-1} = \{(x, y);\ (y, x) \in R\}.$$

POZNÁMKA 1. Ak je R relácia, tak matica opačnej relácie $M_{R^{-1}}$ je transponovaná matica M_R. To značí, že $M_{R^{-1}}$ dostaneme preklopením M_R okolo hlavnej diagonály, čiže $M_{R^{-1}} = (M_R)^T$.

POZNÁMKA 2. Ak máme graf relácie R, tak graf relácie R^{-1} vznikne prevrátením všetkých šípok naopak.

DEFINÍCIA. Relácia $I_A = \{(x, x);\ x \in A\}$ sa nazýva **identická relácia** na A.

DEFINÍCIA. Nech je R relácia z A do B.

(a) R je **všade definovaná** ak $(\forall x)[(x \in A) \Rightarrow ((\exists y)(y \in B)\ \&\ (x, y) \in R)]$.
(b) R je **jednoznačná** ak $(\forall x)[[((x, y) \in R)\ \&\ ((x, z) \in R)] \Rightarrow (y = z)]$.

DEFINÍCIA. **Zobrazenie** (**funkcia**) f z A do B je všade definovaná jednoznačná relácia z A do B. Ak $x \in A$, tak symbolom $f(x)$ označujeme to $y \in B$, pre ktoré je (x, y) v relácii. Zobrazenie f z A do B zapisujeme $f : A \to B$.

PRÍKLADY ŠPECIÁLNYCH ZOBRAZENÍ.

(a) **Konštantná funkcia** je $f : A \to B$ také, že $(\exists b)[(b \in B)\ \&\ (\forall x)[(x \in A) \Rightarrow$ $\Rightarrow (f(x) = b)]]$.
(b) **Identické zobrazenie** je $I_A : A \to A$ také, že $(\forall x)[(x \in A) \Rightarrow (I_A(x) = x)]$.
(c) **Postupnosť** $a_0, a_1, a_2, \ldots$ prvkov z A je zobrazenie $f : \mathbb{N} \to A$ také, že $f(i) = a_i$.
(d) **Usporiadaná n-tica** prvkov z A je $f : \{1, 2, \ldots, n\} \to A$.
(e) **Charakteristická funkcia** množiny $A \subseteq M$ je funkcia $\chi_A : M \to \{0, 1\}$ taká, že

$$\chi_A(x) = \begin{cases} 1 & \text{ak } x \in A \\ 0 & \text{ak } x \notin A \end{cases}$$

(f) **Binárna operácia** na A je zobrazenie $f : A \times A \to A$.
(g) **Booleova funkcia** je $f : \{0, 1\}^n \to \{0, 1\}$.

DEFINÍCIA. Zobrazenie $f : A \to B$ sa nazýva:

(a) **injektívne** (**prosté**) ak je relácia f^{-1} jednoznačná;
(b) **surjektívne** (**na**) ak je f^{-1} všade definovaná;
(c) **bijektívne** (**jedno-jednoznačné**) ak je f injektívne aj surjektívne.

POZNÁMKA. Ak je f zobrazenie, tak f je bijekciou práve vtedy, keď je f^{-1} zobrazením.

Cvičenia

CVIČENIE 6.1. S využitím definícií dokážte, že $A = B \Leftrightarrow ((A \subseteq B)\ \&\ (B \subseteq A))$.

CVIČENIE 6.2. Dokážte zvyšné tvrdenia Vety 6.2.

CVIČENIE 6.3. Nech sú A, B a C ľubovoľné množiny. Dokážte nasledujuce vlastnosti rozdielu množín:
a) $(A \cap B) - C = A \cap (B - C)$
b) $(A \cap B) - C = (A - C) \cap (B - C)$
c) $(A \cup B) - C = (A - C) \cup (B - C)$
d) $C - (A \cap B) = (C - A) \cup (C - B)$
e) $C - (A \cup B) = (C - A) \cap (C - B)$
f) $A - B = A - (A \cap B) = (A \cup B) - B$
g) $A - (B - C) = (A - B) \cup (A \cap C)$
h) $(A - B) - C = A - (B \cup C)$

CVIČENIE 6.4. Nech $A \subseteq B$. Dokážte, že potom pre ľubovoľné C platia vzťahy:
a) $A \cup C \subseteq B \cup C$ b) $A \cap C \subseteq B \cap C$
c) $A - C \subseteq B - C$ d) $C - A \supseteq C - B$
e) $A^c \supseteq B^c$

CVIČENIE 6.5. Nech sú A, B a C ľubovoľné množiny. Dokážte nasledujuce vlastnosti symetrického rozdielu množín:
a) $A \div B = B \div A$ b) $A \div B = (A \cup B) - (A \cap B)$
c) $A \div (B \div C) = (A \div B) \div C$ d) $A \div A = \emptyset$
e) $A \div \emptyset = A$ f) rovnica $X \div A = B$ má jediné riešenie $X = A \div B$

CVIČENIE 6.6. Nech $A \subset B$ a C je ľubovoľná množina. Pomocou Vennových diagramov zistite, v akom vzťahu sú množiny $A \div C$ a $B \div C$

CVIČENIE 6.7. Nájdite množiny A, B a C také, aby platilo $A \cup B = A \cup C$ a zároveň $B \neq C$. (Tento príklad ukazuje, že pri množinovej spojke $\cup$ nemožno krátiť rovnice.)

Cvičenie 6.8. Nakreslite Vennove diagramy pre situácie:
a) $A \cup B \subset A \cup C$, ale $B \not\subseteq C$; b) $A \cap B \subset A \cap C$, ale $B \not\subseteq C$.

Cvičenie 6.9. Dokážte, že vzťah $A \cup B = \emptyset$ platí práve vtedy, keď platí vzťah $(A = \emptyset \ \& \ B = \emptyset)$.

Cvičenie 6.10. Nech $A_1 \subseteq A_2$ a $B_1 \subseteq B_2$. Dokážte, že potom platí
a) $A_1 \cap B_1 \subseteq A_2 \cap B_2$ b) $A_1 \cup B_1 \subseteq A_2 \cup B_2$

Cvičenie 6.11. Nech sú A a B ľubovoľné podmnožiny $\mathcal{U}$. Dokážte, že nasledujúce tvrdenia sú ekvivalentné:
a) $A \subseteq B$ b) $A \cap B = A$
c) $A \cup B = B$ d) $A - B = \emptyset$
e) $A^c \cup B = \mathcal{U}$ f) $A \div B = B - A$
(Návod: Postupne dokážte implikácie (a)⇒(b), (b)⇒(c), (c)⇒(d), (d)⇒(e), (e)⇒(f) a (f)⇒(a). Potom pre ľubovoľné x, y ∈ {a,b, ... ,f} podľa pravidla sylogizmu platí (x)⇒(y) aj (y)⇒(x) a teda (x)⇔(y).)

Cvičenie 6.12. Nech sú A, B a C ľubovoľné množiny. Dokážte, že potom
a) $C \subseteq A \cap B$ platí práve vtedy, keď $C \subseteq A$ a $C \subseteq B$;
b) $A \cup B \subseteq C$ platí práve vtedy, keď $A \subseteq C$ a $B \subseteq C$.

Cvičenie 6.13. Dokážte, že platí
a) $A \cup (B \cap C) = (A \cup B) \cap C \ \Leftrightarrow \ A \subseteq C$;
b) $A \cup B = A \cap C \ \Leftrightarrow \ B \subseteq A \subseteq C$.

Cvičenie 6.14. Ak existuje množina X taká, že $A \cap X = B \cap X$ a $A \cup X = B \cup X$, tak potom platí $A = B$. Dokážte.

Cvičenie 6.15. Dokážte, že platí $A \div B = A \cup B \ \Leftrightarrow \ A \cap B = \emptyset$.

Cvičenie 6.16. Čomu sa rovná $[B \div [(A \div B) \div C]] \div [[A \div (C \div A)] \div B]$?

Cvičenie 6.17. Zostrojte potenčné množiny pre nasledujúce množiny
a) $\{\emptyset\}$ b) $\{\emptyset, \{\emptyset\}\}$ c) $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$

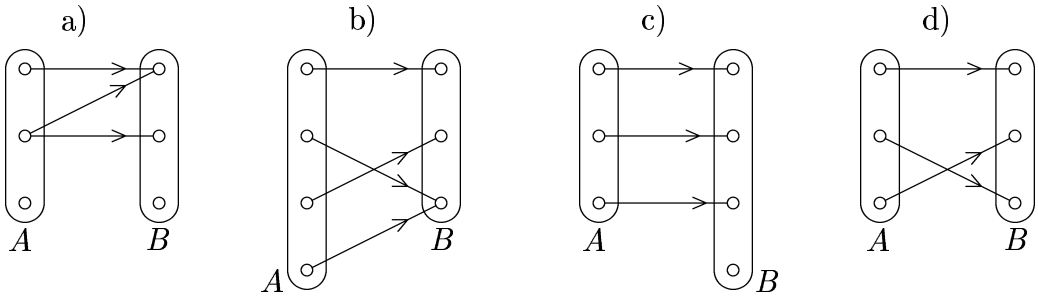
Cvičenie 6.18. Je skladanie relácií komutatívne? Svoje tvrdenie zdôvodnite.

Cvičenie 6.19. Dokážte, že I_A je jednotka vzhľadom na operáciu skladania relácií na množine A, zatiaľ čo prázdna množina je nula.

Cvičenie 6.20. Nech je R relácia z A do B a nech je S relácia z B do C. Potom platí:
a) Ak sú R aj S všade definované, tak je aj $R \circ S$ všade definovaná.
b) Ak sú R aj S jednoznačné, tak je aj $R \circ S$ jednoznačná.

Cvičenie 6.21. Napíšte charakteristické funkcie nasledujúcich podmnožín množiny $\mathbb{N}$:
a) $\emptyset$ b) $\{1, 2, 5\}$ c) štvorce celých čísel

Cvičenie 6.22. Ktoré z grafov z Obrázku 5 reprezentujú zobrazenia z A do B a ktoré zo zobrazení sú surjekcie, injekcie a bijekcie?



Obrázok 5

Cvičenie 6.23. Koľko je takých zobrazení z A do B, ktoré sú
a) bijektívne; b) injektívne; c*) surjektívne.

7 TEÓRIA GRÚP 1

Symetrie rovinných obrazcov

Uvažujme písmenká v slove HOSŤ. Každé z nich má nejaké symetrie. Symetrie sú zhodné zobrazenia roviny na seba, ktoré síce poprehadzujú body roviny, ale obrazom daného písmenka je ono samé a na tom istom mieste, kde stálo. Tak napríklad, H možno preklopiť okolo horizontálnej osi, idúcej stredom písmenka. Tiež ho možno otočiť okolo stredu o 180°. Majú nejaké z uvedených 4 písmen rovnaké všetky symetrie?

Definícia a príklady

V tejto časti sa budeme zaoberať binárnymi operáciami na množine (pozri definíciu v predchádzajúcej kapitole). S týmito operáciami je zviazaný pojem grupy, azda najdôležitejší pojem diskrétnej matematiky.

DEFINÍCIA. **Grupa** je dvojica $(G;*)$, kde G je neprázdna množina (**nosič**) a $*$ je binárna operácia na G, pričom platí

(a) $(\forall a)(\forall b)\big([(a \in G)\ \&\ (b \in G)] \Rightarrow [a * b \in G]\big)$ (uzavretosť vzhľadom na operáciu $*$);

(b) $(\forall a)(\forall b)(\forall c)\big([(a \in G)\ \&\ (b \in G)\ \&\ (c \in G)] \Rightarrow [(a*b)*c = a*(b*c)]\big)$ (pre prvky grupy platí asociatívny zákon);

(c) $(\exists e)\big((e \in G)\ \ \&\ \ [(\forall a)(a \in G) \Rightarrow (a * e = e * a = a)]\big)$ (v grupe existuje neutrálny prvok);

(d) $(\forall a)\big((a \in G) \Rightarrow (\exists b)(a*b = b*a = e)\big)$ (ku každému prvku v grupe existuje inverzný prvok – prvok b z predchádzajúceho vzťahu označujeme a^{-1}).

Grupa je **komutatívna**, ak naviac platí

(e) $(\forall a)(\forall b)\big([(a \in G)\ \&\ (b \in G)] \Rightarrow [a*b = b*a]\big)$ (pre prvky platí komutatívny zákon).

PRÍKLAD 1. Grupou je $(\mathbb{Z};+)$, množina celých čísel s operáciou sčítania. Neutrálnym prvkom tejto grupy je 0 a inverzným prvkom k a je prvok $-a$. Podobne sú grupami aj $(\mathbb{Q};+)$, $(\mathbb{R};+)$ a $(\mathbb{C};+)$. Avšak $(\mathbb{N};+)$ grupou nie je, lebo nie je splnená vlastnosť (d).

PRÍKLAD 2. Nech je n prirodzené číslo, $n \geq 1$. Grupou je dvojica $(\mathbb{Z}_n; \oplus)$, kde $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ a operácia $a \oplus b$ je zvyškom z čísla $a + b$ po delení n. Dá sa ukázať, že $\oplus$ je asociatívna operácia, neutrálnym prvkom je 0 a inverzným prvkom k a je $n-a$.

Všetky grupy z Príkladov 1 a 2 sú komutatívne, a keďže operáciou je (v podstate) $+$, voláme ich **aditívne grupy**. Zatiaľ čo grupy z Príkladu 1 sú nekonečné, v Príklade 2 máme iba konečné grupy.

Konečné grupy možno zadať tabuľkou grupovej operácie. Pre lepšiu názornosť uvádzame tabuľku $(\mathbb{Z}_4, \oplus)$. Ak chceme zistiť, koľko je $a \oplus b$, tak si v ľavom stĺpci nájdeme a a v hornom riadku b. Potom $a \oplus b$ sa nachádza v riadku prvku a a stĺpci prvku b.

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

PRÍKLAD 3. Grupou je $(\mathbb{Q} - \{0\}; \cdot)$, množina racionálnych čísel bez nuly s operáciou násobenia. Neutrálnym prvkom je 1 a inverzným prvkom k a je $\frac{1}{a}$. Podobne sú grupami aj $(\mathbb{Q}^+; \cdot)$ ($\mathbb{Q}^+$ je množina kladných racionálnych čísel), $(\mathbb{R} - \{0\}; \cdot)$, $(\mathbb{C} - \{0\}; \cdot)$. Avšak $(\mathbb{Z} - \{0\}; +)$ grupou nie je, lebo nie je splnená vlastnosť (d).

PRÍKLAD 4. Nech je p prvočíslo. Grupou je $(\mathbb{Z}_p - \{0\}; \odot)$, kde operácia $a \odot b$ je zvyškom z čísla $a \cdot b$ po delení n.

Aj grupy z Príkladov 3 a 4 sú komutatívne, a keďže operáciou je (v podstate) $\cdot$, voláme ich **multiplikatívne grupy**. Nižšie uvádzame tabuľku grupy $(\mathbb{Z}_5 - \{0\}; \odot)$.

$\odot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Hoci táto tabuľka vypadá ináč, ako tabuľka pre $(\mathbb{Z}_4; \oplus)$, grupy $(\mathbb{Z}_5 - \{0\}; \odot)$ a $(\mathbb{Z}_4; \oplus)$ sú „rovnaké“ (viď pojem izomorfizmu v nasledujúcej kapitole). Presvedčíme sa o tom, keď prvky v záhlaviach tabuľky pre $(\mathbb{Z}_5 - \{0\}; \odot)$ trochu poprehadzujeme:

$\odot$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

Niet pochýb o tom, že táto tabuľka je, až na označenie prvkov, rovnaká ako tabuľka grupy $(\mathbb{Z}_4; \oplus)$.

Nosičom grupy nemusí byť vždy množina čísel. Koniec-koncov, grupy samotné sa začali študovať kvôli potrebe popisu symetrií „pravidelných“ útvarov.

PRÍKLAD 5. Grupu je $(G; \circ)$, kde G sú všetky možné symetrie písmenka H a $\circ$ je operáciou skladania symetrií. Potom nosič G pozostáva z **i**dentity, **s**tredovej symetrie podľa stredu písmenka, preklopenia okolo **v**ertikálnej osi idúcej stredom písmenka a preklopenia okolo **h**orizontálnej osi idúcej stredom H. Tabuľkou pre operáciu $\circ$ je

$\circ$	i	s	v	h
i	i	s	v	h
s	s	i	h	v
v	v	h	i	s
h	h	v	s	i

Hoci je grupa $(G; \circ)$ z Príkladu 5 komutatívna, je iná ako $(\mathbb{Z}_4; \oplus)$. To preto, lebo pre každý prvok a v grupe $(G; \circ)$ platí $a \circ a = i$, čiže $a = a^{-1}$. Túto vlastnosť mali len dva prvky grupy $(\mathbb{Z}_4; \oplus)$.

PRÍKLAD 6. Grupu tvoria všetky možné symetrie pravidelného n-uholníka s operáciou skladania symetrií. Táto grupa sa volá **dihedrálna** a označuje sa skrátene D_n, lebo je zrejmé, o akú operáciu ide. Má $2n$ prvkov, z čoho je n rotácií (včítane identity) a n preklopení. Grupa D_n nie je komutatívna. O tom sa presvedčíme vtedy, keď zložíme ľubovoľné dve preklopenia, povedzme p_1 a p_2, ktorých osi zvierajú uhol π/n. Potom $\{p_1 \circ p_2, p_2 \circ p_1\} = \{r_1, r_1^{-1}\}$, pričom r_1 je otočenie o uhol $2\pi/n$.

Doteraz sme uvádzali príklady dvojíc, ktoré tvorili grupu. Teraz si ukážeme, čo grupu netvorí.

PRÍKLAD 7. Grupu netvorí $(\mathbb{R}^+; *)$, kde $\mathbb{R}^+$ je množina kladných reálnych čísel a $*$ je operácia umocňovania. To preto, lebo $*$ nie je ani len asociatívna. Napríklad $(2 * 3) * 2 = (2^3)^2 = 8^2 = 64$, zatiaľ čo $2 * (3 * 2) = 2^{3^2} = 2^9 = 512$.

PRÍKLAD 8. Grupu netvorí $(\mathbb{Z}_4 - \{0\}; \odot)$. To preto, lebo k prvku 2 v tejto štruktúre nemáme inverzný prvok. Pre žiadne číslo a zo $\mathbb{Z}_4 - \{0\}$ neplatí $2 \odot a = 1$.

Základné tvrdenia

VETA 7.1. *Nech je daná grupa $(G; *)$ a $a, b \in G$. Potom má každá z rovníc $a * x = b$ a $y * a = b$ (s neznámou x, respektíve y) práve jedno riešenie.*

DÔKAZ. Dokážeme tvrdenie pre prvú rovnicu, pre druhú sa dokáže analogicky.

Ak si zvolíme $x = a^{-1} * b$, tak $a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b$. Čiže $a^{-1} * b$ je riešením. Ešte dokážeme, že toto riešenie je jediné. Ak je c iným riešením našej rovnice, tak platí $a * c = b$. Prvky na obidvoch stranách rovnice sú rovnaké, a preto na ne aplikujme násobenie prvkom a^{-1} zľava. Dostávame $a^{-1} * (a * c) = a^{-1} * b$, čo po úprave dáva $c = a^{-1} * b$. Teda riešenie je jediné. □

Veta 7.1 má pekné dôsledky.

DÔSLEDOK 1. *V grupe existuje jediný neutrálny prvok.*

DÔKAZ. Podľa Vety 7.1 má pre ľubovoľný prvok a rovnica $a * x = a$ jediné riešenie. □

DÔSLEDOK 2. *Ku každému prvku a existuje v grupe jediný inverzný prvok.*

DÔKAZ. Podľa Vety 7.1 má $a * x = e$ jediné riešenie. □

DÔSLEDOK 3. *V grupe $(G; *)$ pre každé $a, b \in G$ platí $(a * b)^{-1} = b^{-1} * a^{-1}$ a naviac $(a^{-1})^{-1} = a$.*

DÔKAZ. Podľa Vety 7.1 má $(a*b)*x = e$ jediné riešenie. Teraz $(a*b)*(a*b)^{-1} = e$ z definície, zatiaľ čo $(a*b)*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1} = a*e*a^{-1} = a*a^{-1} = e$. Druhá časť plynie z toho, že $a^{-1} * x = e$ má jediné riešenie. □

DÔSLEDOK 4. *V grupe $(G; *)$ pre každé $a, b, c \in G$ platí*

(a) *ak $a * c = b * c$, tak $a = b$ (zákon o krátení sprava);*
(b) *ak $c * a = c * b$, tak $a = b$ (zákon o krátení zľava).*

DÔKAZ. V prípade (a) stačí uvažovať rovnicu $y*c = a*c$ a v prípade (b) rovnicu $c * x = c * a$. Podľa Vety 7.1 majú obidve tieto rovnice jediné riešenie. □

Priamy súčin

Pomocou súčinu vieme vytvoriť z dvoch menších grúp grupu väčšiu. Uvedieme tu priamy súčin, ktorý je najjednoduchší.

DEFINÍCIA. Nech sú $(G_1; *_1)$ a $(G_2; *_2)$ grupy. Potom **priamy súčin** týchto grúp je $(G_1 \times G_2; *)$, kde $*$ je definovaná

$$(a_1, a_2) * (b_1, b_2) = (a_1 *_1 b_1, a_2 *_2 b_2)$$

VETA 7.2. *Priamy súčin grúp $(G_1; *_1)$ a $(G_2; *_2)$ je opäť grupa. Naviac, ak sú $(G_1; *_1)$ a $(G_2; *_2)$ komutatívne, tak aj priamy súčin je komutatívnou grupou.*

DÔKAZ. Postupne overíme všetky vlastnosti grupy.
Nech sú (a_1, a_2) a (b_1, b_2) dva prvky z $G_1 \times G_2$. Potom podľa definície platí $(a_1, a_2) * (b_1, b_2) = (a_1 *_1 b_1, a_2 *_2 b_2)$, a keďže G_1 aj G_2 sú grupy, tak $a_1 *_1 b_1 \in G_1$

a $a_2 *_2 b_2 \in G_2$. To značí že $(a_1 *_1 b_1, a_2 *_2 b_2) \in G_1 \times G_2$, čiže priamy súčin je uzavretý vzhľadom na operáciu $*$.

Nech sú (a_1, a_2), (b_1, b_2) a (c_1, c_2) prvky $G_1 \times G_2$. Potom

$$\begin{gathered}[(a_1, a_2) * (b_1, b_2)] * (c_1, c_2) = (a_1 *_1 b_1, a_2 *_2 b_2) * (c_1, c_2) = \\ = ([a_1 *_1 b_1] *_1 c_1, [a_2 *_2 b_2] *_2 c_2)) = (a_1 *_1 [b_1 *_1 c_1], a_2 *_2 [b_2 *_2 c_2])) = \\ = (a_1, a_2) * (b_1 *_1 c_1, b_2 *_2 c_2) = (a_1, a_2) * [(b_1, b_2) * (c_1, c_2)],\end{gathered}$$

čiže $*$ je asociatívna operácia.

Pre ľubovoľné $(a_1, a_2) \in G_1 \times G_2$ platí

$$\begin{gathered}(e_1, e_2) * (a_1, a_2) = (e_1 *_1 a_1, e_2 *_2 a_2) = (a_1, a_2) = \\ = (a_1 *_1 e_1, a_2 *_2 e_2) = (a_1, a_2) * (e_1, e_2),\end{gathered}$$

čiže (e_1, e_2) je neutrálny prvok.

Konečne, pre ľubovoľné $(a_1, a_2) \in G_1 \times G_2$ platí

$$\begin{gathered}(a_1, a_2) * (a_1^{-1}, a_2^{-1}) = (a_1 *_1 a_1^{-1}, a_2 *_2 a_2^{-1}) = (e_1, e_2) = \\ = (a_1^{-1} *_1 a_1, a_2^{-1} *_2 a_2) = (a_1^{-1}, a_2^{-1}) * (a_1, a_2),\end{gathered}$$

kde a_1^{-1} je prvok inverzný k a_1 v G_1 a a_2^{-1} je prvok inverzný k a_2 v G_2. Teda $(a_1^{-1}, a_2^{-1}) \in G_1 \times G_2$. To znamená, že priamy súčin obsahuje s každým prvkom aj prvok k tomuto inverzný.

Teda $(G_1 \times G_2; *)$ je grupou. Nech $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$, pričom $(G_1; *_1)$ aj $(G_2; *_2)$ sú komutatívne grupy. Potom

$$(a_1, a_2) * (b_1, b_2) = (a_1 *_1 b_1, a_2 *_2 b_2) = (b_1 *_1 a_1, b_2 *_2 a_2) = (b_1, b_2) * (a_1, a_2),$$

čiže aj priamy súčin je komutatívny. □

Nasledujúcu vetu uvádzame bez dôkazu.

VETA 7.3. *Nech je $(G; *)$ konečná komutatívna grupa. Potom existuje k a mocniny prvočísel $q_1 \leq q_2 \leq \cdots \leq q_k$ také, že $(G; *)$ je izomorfná (rovnaká ako) priamy súčin $(\mathbb{Z}_{q_1}; \oplus) \times (\mathbb{Z}_{q_2}; \oplus) \times \cdots \times (\mathbb{Z}_{q_k}; \oplus)$. Naviac, tento priamy súčin je (pri vyššie uvedených podmienkach) určený jednoznačne.*

(Presnú definíciu izomorfizmu uvádzame v nasledujúcej kapitole.)

POZNÁMKA. Veta 7.3 charakterizuje konečné komutatívne grupy. V podstate tvrdí, že komutatívne grupy nie sú zaujímavé, lebo sú príliš jednoduché, priehľadné.

Podgrupy

DEFINÍCIA. Grupa $(G_1; *_1)$ je **podgrupou** grupy $(G; *)$ ak $G_1 \subseteq G$ a pre ľubovoľné $a, b \in G_1$ platí $a *_1 b = a * b$.

POZNÁMKA. Ak je $(G_1; *_1)$ podgrupou grupy $(G; *)$, tak sa operácie $*_1$ a $*$ správajú na nosiči G_1 rovnako. Preto obyčajne používame pre operáciu podgrupy ten istý symbol, ako pre operáciu grupy.

VETA 7.4. *Nech je $(G; *)$ grupa a $G_1 \subseteq G$, $G_1 \neq \emptyset$. Potom $(G_1; *)$ tvorí podgrupu $(G; *)$ práve vtedy keď*

(a) *G_1 je uzavretá vzhľadom na operáciu $*$;*
(b) *G_1 je uzavretá vzhľadom na inverzné prvky.*

DÔKAZ. Podľa definície grupy sú podmienky (a) a (b) nutné nato, aby bola $(G_1; *)$ grupou. Ukážeme, že sú aj postačujúce.

Nato stačí overiť, že sú splnené vlastnosti (a) až (d) z definície grupy. Lenže uzavretosť splýva s vlastnosťou (a). Asociativita je splnená pre všetky prvky G, a teda ju spĺňajú aj prvky G_1. Existencia inverzného prvku splýva s vlastnosťou (b), takže nám stačí ukázať, že v G_1 existuje neutrálny prvok.

Keďže $G_1 \neq \emptyset$, existuje $a \in G_1$. Potom aj $a^{-1} \in G_1$ podľa (b) a $a * a^{-1} \in G_1$ podľa (a). Avšak $a * a^{-1} = e$. □

POZNÁMKA. Ak je $(G; *)$ grupa, tak $(\{e\}, *)$ aj $(G; *)$ sú jej podgrupy. Tieto dve podgrupy sa nazývajú **triviálne**. Ostatné podgrupy $(G; *)$ sú **netriviálne**.

Dá sa ukázať, že prienikom dvoch podgrúp grupy je opäť grupa. Avšak zjednotením dvoch podgrúp grupa byť nemusí.

DEFINÍCIA. Nech je $(G; *)$ grupa a $X \subseteq G$. Symbolom $[X]$ označujeme najmenšiu podgrupu $(G_1; *)$ grupy $(G; *)$ takú, že $X \subseteq G_1$. Hovoríme, že $(G_1; *)$ je podgrupa **generovaná** množinou X.

Občas je výhodné zadať celú grupu pomocou malej generujúcej množiny. V takom prípade, aby sme aspoň čosi vedeli o operácii, zadávame spolu s generátormi aj identity, ktoré tieto generátory spĺňajú. Žiadne iné vzťahy nepredpokladáme.

PRÍKLAD 1. Nech $G = (a; a^4 = e)$. Tu symbolom a^4 označujeme $a * a * a * a$. Táto grupa má len prvky generované a. Teda obsahuje $e = a^0$, a, a^2, a^3 a to je všetko, lebo $a^4 = e$. Inverzným prvkom k a je a^3 a a^2 je inverzný sám sebe. Teda táto grupa je vlastne $(\mathbb{Z}_4; \oplus)$.

PRÍKLAD 2. Nech $G = (a; \emptyset)$. Táto grupa obsahuje $e = a^0, a, a^2, \ldots$ a kvôli uzavretosti na inverzné prvky aj $a^{-1}, a^{-2}, \ldots$ To znamená, že $G = (a; \emptyset)$ je vlastne grupou $(\mathbb{Z}; +)$.

PRÍKLAD 3. Nech $G_n = (a, b; a^2 = b^2 = (ab)^n = e)$, kde ab značí $a * b$. Táto grupa obsahuje prvky $a, b, ab, ba, aba, bab, \ldots$ Tieto reťazce môžu obsahovať iba alternujúce sekvencie a a b, lebo $a^2 = b^2 = 1$. Naviac, ich dĺžka je menšia ako $2n$, lebo $(ab)^n = e$ a po vynásobení $(ba)^n$ dostávame že aj $(ba)^n = e$. Táto dĺžka musí byť vlastne ešte kratšia, pretože keď je jeden reťazec prvkom, povedzme c, tak c^{-1} nezískame doplnením reťazca na dĺžku $2n$ do vzťahu $(ab)^n = e$, ale prevrátením reťazca pre c. Teda G_n má presne $2n$ prvkov. Ešte si všimnime, že všetky reťazce nepárnej dĺžky sú inverzné sami k sebe a začneme tušiť, že G_n by mohla byť dihedrálnou grupou D_n. A naozaj. Preklopenia opísané v príklade, v ktorom sme dihedrálnu grupu uviedli, spĺňajú naše identity. Keďže počet prvkov G_n sme už stanovili, G_n je naozaj práve D_n.

POZNÁMKA. Keď chceme grupu zadať pomocou generátorov, tak obyčajne máme viacero možností. Napríklad dihedrálnu grupu D_n možno zadať nielen tak ako v predošlom príklade. Inou možnosťou je $D_n = (a, b; a^n = b^2 = baba = e)$.

Cvičenia

CVIČENIE 7.1. Tvorí grupu množina všetkých párnych (respektíve nepárnych) celých čísel spolu s operáciou sčítania?

CVIČENIE 7.2. Je $(\mathbb{Z}; \square)$ grupou ak $a \square b = a + b - 2$?

CVIČENIE 7.3. Nech je M množina. Dokážte, že $(\mathcal{P}(M); \div)$, kde $\mathcal{P}(M)$ je množina všetkých podmnožín M a $\div$ je symetrická diferencia, tvorí grupu. Čo je neutrálnym prvkom a ako vyzerá množina inverzná k A?

CVIČENIE 7.4. Dokážte, že ak má grupa $(G; *)$ práve $2n$ prvkov, tak v nej existuje prvok a rôzny od neutrálneho prvku e taký, že $a * a = e$.

CVIČENIE 7.5. Dokážte, že ak v grupe $(G; *)$ pre každé $a \in G$ platí $a * a = e$, tak $(G; *)$ je komutatívna grupa.

CVIČENIE 7.6. Určte, či je H podgrupou grupy G ak

a) $H = \mathbb{N}$ a $G = (\mathbb{Z}; +)$; b) $H = \mathbb{Z}_2$ a $G = (\mathbb{Z}_4; \oplus)$;
c) $H = \mathbb{Q}^+$ a $G = (\mathbb{Q}; +)$; d) $H = \mathbb{Q}^+$ a $G = (\mathbb{Q} - \{0\}; \cdot)$.

CVIČENIE 7.7. Nájdite všetky podgrupy týchto grúp

a) $(\mathbb{Z}; +)$; b) $(\mathbb{Z}_6; \oplus)$; c) $(\mathbb{Z}_2; \oplus) \times (\mathbb{Z}_4; \oplus)$; d) D_4.

CVIČENIE 7.8. Nech je $(G; *)$ grupa. Dokážte, že $X \subseteq G$ je podgrupou $(G; *)$ práve vtedy, keď je X neprázdna množina, ktorá s každými dvoma prvkami $a, b \in X$ obsahuje aj $a * b^{-1}$.

8 TEÓRIA GRÚP 2

Izomorfizmus grúp

S nasledujúcim pojmom sme sa v intuitívnej podobe stretli už v predchádzajúcej kapitole.

DEFINÍCIA. Grupa $(G_1; *_1)$ je **izomorfná** (rovnaká) s grupou $(G_2; *_2)$, ak existuje bijekcia $\varphi : G_1 \to G_2$ taká, že

$$(\forall a)(\forall b)\big([(a \in G_1)\ \&\ (b \in G_1)] \Rightarrow [(a *_1 b)\varphi = (a\varphi) *_2 (b\varphi)]\big),$$

teda ak φ zachováva grupové operácie.

Je zrejmé, že ak je $(G_1; *_1)$ izomorfná s $(G_2; *_2)$, tak je aj $(G_2; *_2)$ izomorfná s $(G_1; *_1)$. (Stačí uvažovať bijekciu φ^{-1}.) Teda relácia izomorfizmu na grupách je symetrická.

PROBLÉM NA ROZMYSLENIE. Čo myslíte, sú grupy $(\mathbb{R}; +)$ a $(\mathbb{R}^+; \cdot)$ izomorfné? Obidve grupy sú nekonečné, avšak prvá je aditívna, zatiaľ čo druhá je multiplikatívna.

Podgrupy a rozklady

DEFINÍCIA. Nech je $(G; *)$ grupa, a H je jej podgrupa. **Pravou triedou** grupy G podľa H, určenou prvkom $a \in G$, nazývame množinu $H * a = \{h * a;\ h \in H\}$. Podobne, **ľavou triedou** nazývame množinu $a * H = \{a * h;\ h \in H\}$.

Nasledujúcu vetu uvádzame pre pravé triedy. Pre ľavé platí analogické tvrdenie a dôkaz je takmer totožný.

VETA 8.1. *Triedy grupy $(G; *)$ podľa jej podgrupy tvoria rozklad množiny G. To znamená, že každý prvok $a \in G$ patrí práve do jednej pravej triedy. Naviac, ak je H konečná, tak každá trieda má práve toľko prvkov, ako H.*

DÔKAZ. Nech $a \in G$. Potom a patrí do triedy $H * a$. To preto, lebo $e \in H$ a $a = e * a$.

Teraz ukážeme, že a patrí do jedinej pravej triedy. Nech $a \in H * b$ pre nejaké b. Potom existuje $h \in H$ také, že $a = h * b$, z čoho plynie $H * a \subseteq H * b$, pretože pre

ľubovoľné $g \in H$ a $g * a \in H * a$ máme $g * h \in H$ a teda $(g * h) * b \in H * b$. Lenže prvok $(g * h) * b$ je práve $g * a$. Na druhej strane, $b = h^{-1} * a$, z čoho sa analogicky odvodí $H * b \subseteq H * a$. To znamená, že $H * b = H * a$, čiže a patrí do jedinej pravej triedy.

Zostáva nám dokázať, že ak je H konečná, tak každá trieda má práve toľko prvkov, ako H. Sporom predpokladajme, že $H * a$ má menej prvkov ako H (viac ich mať nemôže, lebo je k dispozícii len $|H|$ prvkov na súčiny $h * a$). Potom však musia existovať $h, g \in H$ také, že $h * a = g * a$. Lenže to je v spore s Vetou 7.1, ktorá tvrdí, že rovnica $y * a = b$ má v grupe jediné riešenie. □

Dôsledkom Vety 8.1 sú nasledujúce dve tvrdenia.

Veta 8.2 (**Lagrangeova**). *Nech je $(G; *)$ konečná grupa. Potom počet prvkov jej ľubovoľnej podgrupy H delí počet prvkov G.*

Dôkaz. Nech má H práve k prvkov. Podľa Vety 8.1 pravé triedy G podľa H tvoria rozklad grupy G, a podľa tej istej vety má každá trieda presne k prvkov. Teda ak je tých tried povedzme l, tak G má práve $k \cdot l$ prvkov. □

Definícia. Nech je a prvok grupy $(G; *)$. Potom najmenšie prirodzené číslo k, také že $a^k = \underbrace{a * a * \cdots * a}_{k\ a\text{-čiek}} = e$ nazývame **rád** prvku a v G. Ak také k neexistuje, hovoríme, že rád prvku a je ∞.

Poznámka 1. Všimnime si, že jediným prvkom rádu 1 je e. Každý iný prvok má väčší rád.

Poznámka 2. Ak je rád prvku a práve k, tak všetky prvky $a, a^2, a^3, \ldots, a^k$ sú rôzne. Totiž ak by platilo $a^{k_1} = a^{k_2}$ pre $0 < k_1 < k_2 \leq k$, tak by sme mali $e = a^{k_1} * a^{-k_1} = a^{k_2} * a^{-k_1} = a^{k_2 - k_1}$, čo by bolo v spore s definíciou rádu a, keďže $0 < k_2 - k_1 < k$.

Veta 8.3. *Rád každého prvku konečnej grupy delí počet prvkov grupy.*

Dôkaz. Ak je k rád prvku a v $(G, *)$, tak $[a]$ (podgrupa generovaná prvkom a) obsahuje práve prvky $A = \{a, a^2, a^3, \ldots, a_k = e\}$. To preto, lebo A je uzavretá na operáciu $*$ a s každým prvkom a^l obsahuje aj inverzný prvok a^{k-l}. Podľa Vety 7.4 tieto dve vlastnosti stačia na to, aby bola $(A; *)$ podgrupou grupy $(G; *)$. Keďže $(A; *)$ má k prvkov, tvrdenie je dôsledkom Lagrangeovej vety. □

Definícia. Nech je H podgrupa grupy $(G; *)$. Hovoríme, že H je **normálna podgrupa** $(G; *)$ ak pre každé $g \in G$ platí $H * g = g * H$.

Poznámka 1. Ak je G komutatívna grupa, tak každá jej podgrupa je normálna.

Poznámka 2. Ak je G priamym súčinom $(G_1; *_1)$ a $(G_2; *_2)$, tak obidve tieto grupy sú normálne v G.

Nasledujúcu vetu považujeme v algebre za jednu z najzákladnejších. Táto veta umožňuje (v istom zmysle) tvrdenie obrátené k Poznámke 2, avšak už nie pre priamy súčin. Symbolom Ha označujeme $H * a$.

VETA 8.4. *Nech je $(G; *)$ grupa a H je jej normálna podgrupa. Množina pravých tried rozkladu G podľa H spolu s operáciou $\square$ definovanou $(Ha)\square(Hb) = H(a*b)$ tvorí grupu. Táto grupa sa nazýva* **faktorová** *a označuje sa G/H.*

DÔKAZ. Najprv overíme jednoznačnosť operácie $\square$ v G/H. Nech $a_1 \in Ha$ a $b_1 \in Hb$. Dokážeme, že $H(a_1*b_1) = H(a*b)$. Keďže $b_1 \in Hb$, tak existuje $h \in H$ také, že $b_1 = h * b$. Teraz $a_1 * h \in a_1H = Ha_1 = Ha$ podľa Vety 8.1. Teda existuje $g \in H$ také, že $g*a = a_1*h$. Potom $a_1*b_1 = a_1*h*b = g*a*b$, čiže $a_1*b_1 \in H(a*b)$, čo podľa Vety 8.1 znamená, že $H(a_1*b_1) = H(a*b)$. Poznamenajme, že keby H nebola normálna, tak by operácia $\square$ nemusela byť v G/H dobre definovaná. V ďalšom dokážeme, že G/H je grupa.

Uzavretosť na operáciu $\square$ je zrejmá z definície a z toho, že $(G, *)$ je uzavretá vzhľadom na $*$.

Nech sú $a, b, c \in G$. Potom asociatívnnosť G/H plynie zo vzťahu

$$\begin{aligned}(Ha \square Hb) \square Hc = H(a * b) \square Hc = H((a*b) * c) = \\ = H(a * (b*c)) = Ha \square H(b * c) = Ha \square (Hb \square Hc).\end{aligned}$$

Neutrálny prvok je H (čo je He), pretože pre ľubovoľné $a \in G$ máme

$$Ha \square He = H(a * e) = Ha = H(e * a) = He \square Ha.$$

Na záver, inverzným prvkom k Ha je Ha^{-1}, lebo

$$Ha \square Ha^{-1} = H(a * a^{-1}) = He = H(a^{-1} * a) = Ha^{-1} \square Ha. \quad \square$$

V ďalších častiach tejto kapitoly sa budeme venovať špeciálnym typom (reprezentáciám) grúp.

Cyklické grupy

DEFINÍCIA. Grupa $(G; *)$ sa nazýva **cyklická** ak existuje prvok $a \in G$, ktorý ju generuje, čiže pre ktorý platí $G = [a]$. Prvok a sa nazýva **generátor grupy**.

POZNÁMKA 1. Už z definície je zrejmé, že $(G; *)$ je cyklická práve vtedy, keď má ľubovoľný jej prvok tvar a^k (respektíve a^{-k}) pre vhodné $k \in \mathbb{N}$. Ak má generátor a rád n, tak cyklická grupa má n prvkov, označuje sa C_n, a ako bolo uvedené v Príklade 1 na konci Kapitoly 7, táto grupa je izomorfná s grupou $(\mathbb{Z}_n; \oplus)$. (Izomorfizmom je $\varphi : a^k \to k$.) Ak má a rád ∞, tak grupa je izomorfná s $(\mathbb{Z}; +)$, ako bolo uvedené v Príklade 2 na konci Kapitoly 7. (Izomorfizmom je opäť $\varphi : a^k \to k$.)

Poznámka 2. V inej reprezentácii, cyklická grupa je podgrupou dihedrálnej grupy D_n. Môžeme si ju predstaviť ako grupu takých symetrií pravidelného n-uholníka, ktoré zachovávajú orientáciu, čiže ako grupu rotácií.

Poznámka 3. Každá cyklická grupa je komutatívna. To preto, lebo pre ľubovoľné $b = a^k$ a $c = a^l$ platí $b * c = a^k * a^l = a^{k+l} = a^{l+k} = a^l * a^k = c * b$.

Všimnime si, že ak je n prvočíslo, tak C_n je generovaná ľubovoľným svojim prvkom a takým, že $a \neq e$. Ak je však C_6 generovaná povedzme prvkom a, tak žiaden z prvkov a^2, a^3 ani a^4 ju negeneruje. To preto, lebo ako a^2, tak a^4 generujú podgrupu izomorfnú s C_3 v C_6, zatiaľ čo a^3 generuje podgrupu C_6 izomorfnú s C_2. Z tohoto pozorovania plynie nasledujúce tvrdenie:

Veta 8.5. *Ak je n prvočíslo a grupa $(G; *)$ má práve n prvkov, tak táto grupa je izomorfná s C_n a každý prvok G, rôzny od e, je generátorom $(G; *)$.*

Dôkaz. V konečnej grupe má každý prvok konečný rád, a keďže iba e má rád 1 a n je prvočíslo, podľa Vety 8.3 je rád každého prvku a, $a \neq e$, práve n. Teda každý prvok a, $a \neq e$, generuje grupu $(G; *)$, keďže jeho rôznych mocnín je práve toľko, koľko prvkov má táto grupa. Podľa definície je grupa generovaná jediným svojim prvkom cyklická. □

Zdôraznime, že Veta 8.5 tvrdí, že pre ľubovoľné prvočíslo existuje jediná grupa, ktorej počet prvkov je práve toto prvočíslo.

Grupy transformácií

Definícia. **Grupa transformácií** $(G; \circ)$ na množine X je taká neprázdna množina bijekcií X na X, ktorá je uzavretá vzhľadom na skladanie bijekcií (čiže transformácií) a vzhľadom na inverzné bijekcie.

Poznámka. Všimnime si, že grupa transformácií je naozaj grupou. To preto, lebo skladanie bijekcií $\circ$ je binárnou operáciou a sú splnené všetky podmienky na to, aby $\circ$ s nosičom tvorila grupu:

Uzavretosť vzhľadom na operáciu (podmienka (a)) je splnená z definície, rovnako ako uzavretosť na inverzné prvky (podmienka (d)). Existencia neutrálneho prvku (podmienka (c)) plynie z neprázdnosti grupy, teda je v nej prvok, povedzme a, uzavretosti na inverzné prvky, čiže aj a^{-1} je v grupe, a uzavretosti vzhľadom na skladanie bijekcií, z čoho plynie že aj $a \circ a^{-1} = e$ je v grupe. Zostáva overiť asociativitu (podmienku (b)). Lenže podľa Vety 6.3 je skladanie binárnych relácií asociatívne. Keďže zobrazenia, respektíve bijektívne zobrazenia, sú špeciálnymi binárnymi reláciami (všade definovanými a jednoznačnými), je asociatívne aj skladanie bijekcií.

Špeciálnymi grupami transformácií sú symetrie geometrických útvarov. Teda grupou transformácií sú napríklad D_n a C_n. Platí však všeobecnejšie tvrdenie:

VETA 8.6 (**Cayleyho**). *Každá grupa je izomorfná s nejakou grupou transformácií.*

DÔKAZ. Nech je $(G;*)$ ľubovoľná grupa. Zostrojíme grupu transformácií $(T_G;\circ)$ a dokážeme, že táto grupa je izomorfná s $(G;*)$.

Prvkami T_G budú bijekcie $\varphi_a : G \to G$, kde $a \in G$. Teda pre každé $a \in G$ definujeme bijekciu φ_a vzťahom: $\varphi_a(x) = x * a$ pre každé $x \in G$. Všimnime si, že φ_a je naozaj bijekcia. To plynie z Vety 7.1, ktorá tvrdí, že rovnica $x * a = b$ má pre každé $a, b \in G$ jediné riešenie.

Teraz ukážeme, že $(T_G;\circ)$ je grupou. Ak sú $\varphi_a, \varphi_b \in T_G$, tak pre ľubovoľné $x \in G$ platí $(\varphi_a \circ \varphi_b)(x) = \varphi_b(x*a) = (x*a)*b = x*(a*b) = \varphi_{a*b}(x)$, čiže $\varphi_a \circ \varphi_b = \varphi_{a*b}$. To znamená, že T_G je uzavretá vzhľadom na operáciu $\circ$. Asociativita plynie z poznámky pred touto vetou. Neutrálnym prvkom je φ_e, pretože (využijúc vzťah odvodený vyššie) pre každé $a \in G$ máme $\varphi_e \circ \varphi_a = \varphi_{e*a} = \varphi_a = \varphi_{a*e} = \varphi_a \circ \varphi_e$. Napokon, pre každé $a \in G$ máme $\varphi_a^{-1} = \varphi_{a^{-1}}$, lebo $\varphi_a \circ \varphi_{a^{-1}} = \varphi_{a*a^{-1}} = \varphi_e = \varphi_{a^{-1}*a} = \varphi_{a^{-1}} \circ \varphi_a$.

V ďalšom dokážeme, že zobrazenie $\psi : G \to T_G$ definované $\psi(a) = \varphi_a$, je izomorfizmom grupy $(G,*)$ na grupu $(T_G;\circ)$. Zobrazenie ψ je injektívne (prosté), pretože $\varphi_a(e) = a$ a $\varphi_b(e) = b$. Čiže ak $a \neq b$ pre dva prvky grupy G, tak $\varphi_a \neq \varphi_b$. Ďalej zobrazenie ψ je surjektívne (na) a to už z definície, pretože do nosiča T_G sme dali len také prvky φ_a, ktoré zodpovedali prvkom $a \in G$. To značí, že ψ je bijekcia. Napokon, zobrazenie ψ zachováva operáciu, lebo pre ľubovoľné a a b z grupy G platí $\psi(a*b) = \varphi_{a*b} = \varphi_a \circ \varphi_b = \psi(a) \circ \psi(b)$. □

Grupy permutácií

DEFINÍCIA. **Grupou permutácií** je grupa transformácií (permutácií) na konečnej množine X.

POZNÁMKA. Podľa Cayleyho vety je každá konečná grupa izomorfná s nejakou grupou permutácií.

Maticová reprezentácia permutácie. Ak je X „malé“, tak príslušné permutácie môžeme zapísať ako matice s dvoma riadkami. V takejto matici sú v hornom riadku vymenované všetky prvky X (v nejakom poradí) a pod každým prvkom je jeho obraz v permutácii. Napríklad ak $X = \{A, B, C, D, E, F\}$, tak pre permutáciu

$$\alpha = \begin{pmatrix} A & B & C & D & E & F \\ B & D & F & A & E & C \end{pmatrix}$$

platí $\alpha(A) = B$, $\alpha(B) = D$ a podobne.

Reprezentácia permutácie pomocou súčinu cyklov. Permutácia α z predchádzajucej poznámky pozostáva z troch cyklov. Jedným je (ABD), a to preto, lebo $\alpha(A) = B$, $\alpha(B) = D$ a $\alpha(D) = A$. Druhým cyklom je (CF) a posledným je (E). Teda α môžeme zapísať ako súčin troch cyklov $\alpha = (ABD)(CF)(E)$, respektíve $\alpha = (ABD)(CF)$, keďže E zostáva na mieste, a teda α na tento prvok „nepôsobí".

Všimnime si, že ak je pevne stanovené poradie prvkov v prvom riadku, tak maticová reprezentácia permutácie je určená jednoznačne. Podobne je jednoznačne určená reprezentácia pomocou cyklov (až na poradie disjunktných cyklov a prvok, ktorým cyklus „začíname"). Avšak každá permutácia sa dá reprezentovať aj ako súčin len cyklov (už nie nutne disjunktných) dĺžky 2. To preto, lebo pre ľubovoľné n vieme cyklus dĺžky n prepísať ako súčin cyklov dĺžky 2. Platí

$$(a_1 a_2 \dots a_n) = (a_1 a_2)(a_1 a_3) \dots (a_1 a_n).$$

Definícia. Cyklus dĺžky 2 nazývame **transpozícia**. Permutácia je **párna**, ak je súčinom párneho počtu transpozícií. Nech je daná permutácia α množiny $X = \{1, 2, \dots, n\}$. Dvojica (i, j) taká, že $i < j$ a $\alpha(i) > \alpha(j)$, sa nazýva **inverzia**.

Poznámka. Ak máme permutáciu množiny $\{1, 2, \dots, n\}$ a v maticovej reprezentácii máme v prvom riadku prvky v štandardnom poradí, čiže $1, 2, \dots, n$, tak inverziu tvoria také dvojice k a l v druhom riadku, pre ktoré je k naľavo od l a platí $k > l$. Napríklad, v permutácii α

$$\alpha = \begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6 \\ 2\ 4\ 6\ 1\ 5\ 3 \end{pmatrix}$$

tvoria inverziu (čítame z druhého riadku) dvojice $(2,1)$, $(4,1)$, $(4,3)$, $(6,1)$, $(6,5)$, $(6,3)$ a $(5,3)$.

Veta 8.7. *Permutácia množiny $X = \{1, 2, \dots, n\}$ je párna práve vtedy, keď obsahuje párny počet inverzií.*

Dôkaz. Aby sme dokázali túto vetu, stačí overiť, že vynásobením ľubovoľnej permutácie α transpozíciou $\tau = (kl)$ sa zmení počet inverzií o nepárne číslo. To preto, lebo identická permutácia sa dá zapísať pomocou 0 transpozícií a neobsahuje žiadnu inverziu, a každú permutáciu $(a_{k_1} a_{k_2})(a_{k_3} a_{k_4}) \dots (a_{k_{t-1}} a_{k_t})$ vieme previesť na identitu vynásobením (sprava) transpozíciami $(a_{k_t} a_{k_{t-1}})(a_{k_{t_2}} a_{k_{t-3}}) \dots (a_{k_2} a_{k_1})$. Uvažujme teda permutácie α a $\alpha \cdot \tau$:

$$\alpha = \begin{pmatrix} 1\ 2 & \dots & n \\ \dots k \dots l \dots & & \end{pmatrix} \qquad \alpha \cdot \tau = \begin{pmatrix} 1\ 2 & \dots & n \\ \dots l \dots k \dots & & \end{pmatrix}$$

Sledujúc druhý riadok maticovej reprezentácie α a $\alpha \cdot \tau$ vidíme, že tieto permutácie majú tie isté inverzie, až na dvojice obsahujúce buď k, alebo l.

Uvažujme prvok m v druhom riadku. Ak sa nachádzal naľavo od k aj l, tak sa počet inverzií nezmenil. Podobne sa počet inverzií nezmenil, ak sa m nachádzal

napravo od k aj l. Iná je situácia, ak m leží medzi k a l. Vtedy v práve jednej z našich dvoch permutácií tvorí (km) inverziu a v práve jednej tvorí inverziu (lm). To znamená, že kvôli m v $\alpha \cdot \tau$ buď pribudnú dve inverzie, alebo žiadna, alebo dve zaniknú. Paritu počtu inverzií to neovplyvní. Avšak ešte je tu (kl). Táto dvojica tvorí inverziu v práve jednej z našich permutácií, a teda vynásobením α transpozíciou (kl) sa počet inverzií zmenil o nepárne číslo. □

Poznámka 1. Veta 8.7 tvrdí, že párnosť permutácie je dobre definovaná. To preto, lebo ľubovoľnej permutácii množiny $\{a_1, a_2, \ldots, a_n\}$ zodpovedá permutácia množiny $\{1, 2, \ldots, n\}$ (stačí uvažovať indexy). Teda každá permutácia je buď párna, alebo nepárna, ale nemôže byť „obojaká“.

Poznámka 2. Poznamenajme, že parita permutácie je dôležitá pri determinantoch. Závisí od nej znamienko príslušného súčinu.

Definícia. Ak $X = \{1, 2, \ldots, n\}$, tak grupu všetkých možných permutácií na X nazývame **symetrická grupa** a označujeme ju S_n. Podgrupu S_n tvorenú párnymi permutáciami nazývame **alternujúca grupa** a označujeme ju A_n.

Poznámka. Všimnime si, že A_n je naozaj podgrupou S_n. (Je uzavretá vzhľadom na skladanie permutácií a na inverzné permutácie.) Dokonca tvorí v S_n normálnu podgrupu. To preto, lebo S_n má $n!$ prvkov a A_n má $n!/2$ prvkov (toto platí pre $n = 2$ a indukciou sa dá platnosť tvrdenia dokázať pre ľubovoľné n), čiže existujú len dve triedy rozkladu S_n podľa A_n. Faktorovou grupou S_n/A_n je C_2.

Maticové grupy

Definícia. Násobenie matíc je asociatívne, a preto grupu tvoria aj množiny matíc, ktoré sú uzavreté vzhľadom na operáciu násobenia a na inverzné matice. Takéto grupy nazývame **maticové**.

Poznámka. Keďže n-prvkovej permutácii α zodpovedá matica $\mathbb{A} = (a_{i,j})$ typu $n \times n$, ktorá je definovaná:

$$a_{i,j} = \begin{cases} 0 & \text{ak } j \neq \alpha(i) \\ 1 & \text{ak } j = \alpha(i) \end{cases}$$

tak podľa Cayleyho vety je každá konečná grupa izomorfná s nejakou maticovou grupou.

Cvičenia

Cvičenie 8.1. Rozhodnite, či sú nasledujúce zobrazenia izomorfizmy grúp
a) $\varphi : (\mathbb{Z}; +) \to (\mathbb{Z}; +)$, kde $\varphi(x) = 3x$ pre každé $x \in \mathbb{Z}$;
b) $\varphi : (\mathbb{R}; +) \to (\mathbb{R}; +)$, kde $\varphi(x) = 3x$ pre každé $x \in \mathbb{R}$;
c) $\varphi : (\mathbb{R}^+; \cdot) \to (\mathbb{R}^+; \cdot)$, kde $\varphi(x) = \frac{1}{\sqrt{x}}$ pre každé $x \in \mathbb{R}^+$.

Cvičenie 8.2. Sú nasledujúce grupy izomorfné?
a) D_3 a S_3;
b) D_4 a S_4;
c) $(\mathbb{Z}_7 - \{0\}; \odot)$ a $(\mathbb{Z}_6; \oplus)$;
d) $(\mathbb{R}^+; \cdot)$ a $(\mathbb{R} - \{0\}; \cdot)$;
e) $(\mathbb{R}; +) \times (\mathbb{R}; +)$ a $(\mathbb{C}; +)$;
f) $(\mathbb{Z}_2; \oplus) \times (\mathbb{Z}_2; \oplus)$ a $(\mathbb{Z}_4; \oplus)$;
g) $(\mathbb{R} - \{0\}; \cdot) \times (\mathbb{R} - \{0\}; \cdot)$ a $(\mathbb{C} - \{0\}; \cdot)$.

Cvičenie 8.3. Nájdite geometrický útvar, ktorého grupa symetrií je izomorfná s grupou
a) $\mathbb{Z}_2 \times \mathbb{Z}_3$;
b) $\mathbb{Z}_2 \times \mathbb{Z}$;
c) $\mathbb{Z} \times \mathbb{Z}$.

Cvičenie 8.4. Ukážte, že grupa $(\mathbb{C}-\{0\}; \cdot)$ obsahuje prvky rádu n pre ľubovoľné kladné celé číslo n a tiež prvky nekonečného rádu. Platí podobné tvrdenie aj pre $(\mathbb{R} - \{0\}; \cdot)$?

Cvičenie 8.5. Ktoré z nasledujúcich grúp sú cyklické?
a) $(\mathbb{Z}_3; \oplus) \times (Z_4; \oplus)$;
b) $(\mathbb{Z}_3; \oplus) \times (Z_3; \oplus)$;
c) $(\mathbb{Z}_2; \oplus) \times (Z_4; \oplus)$;
d) $(\mathbb{Z}_{11} - \{0\}; \odot)$;
e) $(\{3^n;\ n \in \mathbb{Z}\}; \cdot)$;
f) $(\{1, -\frac{1}{2} + i\frac{\sqrt{3}}{2}, -\frac{1}{2} - \frac{\sqrt{3}}{2}\}; \cdot)$.

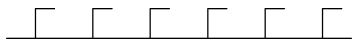
Cvičenie 8.6. Určte počet cyklických podgrúp
a) D_4;
b) S_3;
c) grupy symetrií kocky.

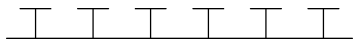
Cvičenie 8.7. Tvoria nasledujúce množiny transformácií spolu s operáciou skladania grupu?
a) $\{f : \mathbb{Z} \to \mathbb{Z};\ f(n) = n + k,\ \text{kde } k \in \mathbb{Z}\}$;
b) $\{f : \mathbb{Z} \to \mathbb{Z};\ f(n) = nk,\ \text{kde } k \in \mathbb{Z}\}$;
c) $\{f : \mathbb{R}^+ \to \mathbb{R}^+;\ f(x) = \sqrt[k]{x^n},\ \text{kde } k, n \in \mathbb{Z}\}$;
d) $\{f : \mathbb{R} \to \mathbb{R};\ f(x) = ax + b,\ \text{kde } a, b \in \mathbb{Q}\}$;
e) $\{f : \mathbb{R} \to \mathbb{R};\ f(x) = ax + b,\ \text{kde } a \in \mathbb{Q} \text{ a } b = 0\}$;
f) $\{f : \mathbb{R} \to \mathbb{R};\ f(x) = ax + b,\ \text{kde } a \in \mathbb{Q} - \{0\} \text{ a } b \in \mathbb{R}\}$;
g) $\{f : \mathbb{R} \to \mathbb{R};\ f(x) = ax + b,\ \text{kde } a \in \mathbb{R} - \{0\} \text{ a } b \text{ je iracionálne}\}$.

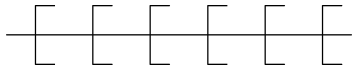
Cvičenie 8.8. Overte, že transformácie f_1, f_2, f_3, f_4, f_5 a f_6 dané vzorcami $f_1(x) = x$, $f_2(x) = \frac{1}{x}$, $f_3(x) = 1 - x$, $f_4(x) = \frac{1}{1-x}$, $f_5(x) = 1 - \frac{1}{x}$, $f_6(x) = \frac{x}{1-x}$ tvoria grupu transformácií množiny $\mathbb{R} - \{0, 1\}$. Je táto grupa komutatívna?

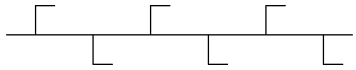
Cvičenie 8.9. Pomocou generátorov opíšte grupu všetkých symetrií Platónskych telies, čiže pravidelného štvorstena, kocky, pravidelného osemstena, pravidelného dvanásťstena a pravidelného dvadsaťstena.

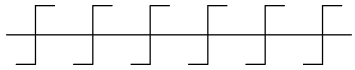
Cvičenie 8.10. Až na izomorfizmus, existuje len 7 rôznych typov symetrií nekonečných pásových ornamentov. Nižšie je uvedený pre každý z týchto typov jeden reprezentant. Pomocou generátorov opíšte grupy symetrií týchto nekonečných ornamentov a pokúste sa určiť, o aké grupy ide.

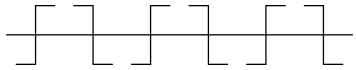
a) 

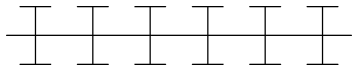
b) 

c) 

d) 

e) 

f) 

g) 

Cvičenie 8.11. Vypočítajte φ^{120} ak

a) $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 8 & 7 & 6 & 2 & 1 & 5 \end{pmatrix}$; b) $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 1 & 7 & 6 & 2 & 3 \end{pmatrix}$.

Cvičenie 8.12. Dokážte, že každá permutácia 6 prvkov má rád najviac 6. Aký najväčší rád môže mať permutácia 8 prvkov?

Cvičenie 8.13. Dokážte, že množina všetkých matíc typu $n \times n$ s reálnymi koeficientami, ktorých determinant sa rovná 1, tvorí s operáciou násobenia matíc grupu.

9 TEÓRIA GRÚP 3

Tri úlohy

Úloha 1 (**Kvadratúra kruhu**). Máme daný kruh. Pomocou pravítka a kružidla zostrojte hranu štvorca, ktorý má rovnaký obsah ako daný kruh.

Úloha 2 (**Zdvojenie kocky**). Daná je hrana kocky. Pomocou pravítka a kružidla zostrojte hranu väčšej kocky, takej, ktorej objem je dvojnásobkom objemu kocky pôvodnej.

Úloha 3 (**Trisekcia uhla**). V rovine je daný uhol. Pomocou pravítka a kružidla rozdeľte tento uhol na tri menšie, rovnako veľké časti.

Tieto úlohy boli známe už v antickom Grécku. Vyše dvetisíc rokov sa ich ľudia snažili vyriešiť, avšak neúspešne. Až moderná algebra ukázala, že tieto úlohy sa vyriešiť nedajú. Kľúčom k dôkazu boli práve rozšírenia polí, ktorým sa budeme venovať v tejto kapitole. Pri prvej úlohe išlo o rozšírenie o transcendentný prvok, zatiaľ čo pri ďalších dvoch o rozšírenia o algebraický prvok.

Okruhy a polia

Definícia. **Okruh** je usporiadaná trojica $(A; +, \cdot)$, kde A je neprázdna množina a $+$ a $\cdot$ sú binárne operácie na A, pričom platí

(a) $(A, +)$ je komutatívna grupa;
(b) A je uzavretá vzhľadom na $\cdot$;
(c) pre každé $a, b, c \in A$ platí $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (asociatívny zákon);
(d) pre každé $a, b, c \in A$ platí $a \cdot (b + c) = a \cdot b + a \cdot c$ (ľavý distributívny zákon) a tiež $(a + b) \cdot c = a \cdot c + b \cdot c$ (pravý distributívny zákon).

Poznámka. Operácie $+$ a $\cdot$ nazývame sčítanie a násobenie, aj keď to nemusí byť klasické sčítanie a násobenie. Kvôli stručnejšiemu zápisu sa znak násobenia často vynecháva a aby sme nemuseli písať priveľa zátvoriek, uzavrieme dohodu, že násobenie má väčšiu prioritu ako sčítavanie.

Lema 9.1. *V ľubovoľnom okruhu* $(A; +, \cdot)$

(1) *pre každé* $a \in A$ *platí* $a0 = 0a = 0$;
(2) *pre každé* $a, b \in A$ *platí* $a(-b) = (-a)b = -ab$.

DÔKAZ. Využijúc 0, čiže neutrálny prvok grupy $(A,+)$, a distributívny zákon, dostávame $aa = a(a+0) = aa + a0$. Teraz keď od obidvoch strán rovnice odčítame aa, získame $a0 = 0$. Podobne zo vzťahu $aa = (a+0)a = aa + 0a$ získame $0a = 0$. Čiže $a0 = 0a = 0$.

K dôkazu druhej časti stačí ukázať, že $a(-b)$ aj $(-a)b$ sú prvky opačné k ab. Keďže $a(-b) + ab = a(-b+b) = a0 = 0$ a $(-a)b + ab = (-a+a)b = 0b = 0$, tvrdenie je dokázané. □

DEFINÍCIA. **Pole** je taký okruh $(A;+,\cdot)$, v ktorom je $(A-\{0\},\cdot)$ komutatívnou grupou.

LEMA 9.2. *V poli $(A;+,\cdot)$ pre každé $a,b \in A$, $a \neq 0$ a $b \neq 0$, platí $ab \neq 0$.*

DÔKAZ. Predpokladajme, že $ab = 0$. Keďže $a \neq 0$, existuje v poli prvok a^{-1} inverzný k a. Potom však vynásobením $ab = 0$ zľava prvkom a^{-1} dostávame $(a^{-1}a)b = a^{-1}0$, čiže $b = 0$ podľa Lemy 9.1. Podľa vety o obrátenej implikácii platí dokazované tvrdenie. □

Lema 9.2 tvrdí, že v poli neexistujú netriviálne delitele nuly.

DEFINÍCIA. Okruh A je **podokruhom** okruhu $(B;+,\cdot)$ ak $A \subseteq B$ a ak sčitovanie a násobenie prvkov z A dáva rovnaký výsledok v A aj B. Podobne pole A je **podpoľom** poľa $(B;+,\cdot)$ ak $A \subseteq B$ a ak sčitovanie a násobenie prvkov z A dáva rovnaký výsledok v A aj B.

VETA 9.3. *Neprázdna podmnožina X okruhu $(A;+,\cdot)$ je podokruhom práve vtedy, keď je uzavretá vzhľadom na rozdiel a súčin. (Teda keď pre každé $a,b \in X$ platí $a-b \in X$ aj $ab \in X$.) Neprázdna podmnožina X poľa $(A;+,\cdot)$ je podpoľom práve vtedy, keď je uzavretá vzhľadom na rozdiel, podiel a obsahuje jednotku. (Teda keď pre každé $a,b \in X$ platí $a-b \in X$, pre každé $a,b \in X$, $b \neq 0$, $a \cdot b^{-1} \in X$ a tiež $e \in X$.*

DÔKAZ. Podmienky vety sú zjavne nutné na to, aby bola množina X okruhom, respektíve poľom. Ukážeme, že sú aj postačujúce. Nato potrebujeme overiť, že je $(X,+)$ komutatívna grupa a vlastnosti (b), (c) (d) z definície okruhu pre prvú časť vety, respektíve vlastnosť (d) z definície okruhu a podmienku že je $(X-\{0\},\cdot)$ komutatívna grupa pre druhú časť vety.

Keďže X je neprázdna, obsahuje prvok a a aj $0 = a-a$. Teda s každým prvkom a obsahuje $0-a = -a$ a s každými dvoma prvkami $a,b \in X$ obsahuje aj $a,-b \in X$ a teda aj $a-(-b) = a+b$. Čiže X je uzavretá vzhľadom na $+$ a opačné prvky, a podľa Vety 7.4 je $(X,+)$ komutatívna grupa.

Podobne sa z existencie $e \in X$ dokáže, že $(X-\{0\},\cdot)$ je komutatívna grupa pre druhú časť vety.

Pre prvú časť vety uzavretosť X vzhľadom na $\cdot$ máme medzi podmienkami a asociativita je splnená pre všetky prvky A, teda aj pre všetky prvky X. Podobne je to aj s distributívnymi zákonmi. □

DEFINÍCIA. Množina $X \subseteq A$ **generuje okruh** $(A;+,\cdot)$, zapisujeme $[X]=A$, ak sa každý podokruh A obsahujúci X rovná A. Podobne, $X \subseteq A$ **generuje pole** $(A;+,\cdot)$, zapisujeme $[[X]]=A$, ak sa každé podpole A obsahujúce X rovná A.

V nasledujúcich vetách opisujeme, ako možno ku komutatívnemu okruhu, teda k okruhu, v ktorom je $\cdot$ komutatívne, respektíve k poľu, pridávať nové prvky u.

VETA 9.4. *Nech je A podokruh komutatívneho okruhu B s jednotkou e a nech $e \in A$. Potom pre ľubovoľný prvok $u \in B - A$ sa $[A \cup \{u\}]$ rovná množine*

$$A[u] = \{a_0 + a_1u + a_2u^2 + \cdots + a_nu^n;\ \textit{kde } n \in \mathbb{N} \textit{ a } a_0, a_1, \ldots, a_n \in A\}.$$

DÔKAZ. Okruh $[A \cup \{u\}]$ je uzavretý na sčitovanie a násobenie, a preto s každými svojimi prvkami obsahuje aj ich súčiny a súčty. Čiže $A[u] \subseteq [A \cup \{u\}]$. Keďže $u = 0 + eu \in A[u]$, zostáva dokázať, že $A[u]$ tvorí okruh.

Nech sú $a = a_0 + a_1u + \cdots + a_nu^n$ a $b = b_0 + b_1u + \cdots + b_mu^m$ dva prvky $A[u]$. Potom $a - b = (a_0 - b_0) + (a_1 - b_1)u + \ldots$, pričom tento výraz má konečnú dĺžku $(\max\{n,m\}+1)$, a teda $a - b \in A[u]$. Podobne, $a \cdot b = a_0b_0 + (a_0b_1 + a_1b_0)u + \ldots$ (tu využívame komutativitu násobenia), pričom aj tento výraz má konečnú dĺžku (nanajvýš $n+m+1$), a teda $a \cdot b \in A[u]$. Keďže operácie používame presne tie isté ako sú operácie B, podľa Vety 9.3 platí $A[u] = [A \cup \{u\}]$. □

VETA 9.5. *Nech je A podpole poľa B. Potom pre ľubovoľný prvok $u \in B - A$ sa $[[A \cup \{u\}]]$ rovná množine*

$$A(u) = \left\{ \frac{a_0 + a_1u + a_2u^2 + \cdots + a_nu^n}{b_0 + b_1u + b_2u^2 + \cdots + b_mu^m};\ \textit{kde } n, m \in \mathbb{N}, \right.$$
$$\left. a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_m \in A \textit{ a } b_0 + b_1u + \cdots + b_mu^m \neq 0 \right\}.$$

DÔKAZ. Pole $[[A \cup \{u\}]]$ je uzavreté na sčitovanie, násobenie a podiel, a preto s každými svojimi prvkami obsahuje aj ich súčiny, súčty a podiely (ak je deliteľ rôzny od 0). Čiže $A(u) \subseteq [[A \cup \{u\}]]$. Keďže $u = \frac{0+eu}{e} \in A(u)$, zostáva dokázať, že $A(u)$ tvorí pole.

Zjavne $e = \frac{e}{e} \in A(u)$. Nech sú $a = \frac{a_0+a_1u+\cdots+a_nu^n}{c_0+c_1u+\cdots+c_ou^o}$ a $b = \frac{b_0+b_1u+\cdots+b_mu^m}{d_0+d_1u+\cdots+d_pu^p}$ dva prvky $A(u)$. Potom $a - b$ má (po úprave na spoločného menovateľa) opäť tvar ako v znení vety, a teda $a - b \in A[u]$. Podobne, $a : b = a \cdot b^{-1}$, pričom aj tento výraz má tvar ako v znení vety. Keďže operácie používame presne tie isté, ako sú operácie B, podľa Vety 9.3 platí $A[u] = [A \cup \{u\}]$. □

Jednoduché rozšírenia polí

DEFINÍCIA. Nech je A podpole poľa $(B; +, \cdot)$. Prvok $u \in B$ je **algebraický** nad A ak existuje nenulový polynóm f nad A (čiže $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ pre vhodné $n \in \mathbb{N}$ a $a_0, a_1, \ldots a_n \in A$) taký, že $f(u) = 0$. Prvok u je **transcendentný** nad A ak $f(u) \neq 0$ pre každý nenulový polynóm f nad A.

PRÍKLAD 1. Prvok $\sqrt{2} + 1$ je algebraický nad $\mathbb{Q}$. To preto, lebo $1 + \sqrt{2} \in \mathbb{R}$, pričom $\mathbb{Q}$ je podpole poľa $\mathbb{R}$ a $1 + \sqrt{2}$ je koreňom polynómu druhého stupňa $f(x) = (x + 1 + \sqrt{2})(x + 1 - \sqrt{2}) = x^2 + 2x + 1 - 2 = (-1) + 2x + 1x^2$.

PRÍKLAD 2. Prvok i je algebraický nad $\mathbb{Q}$. To preto, lebo $i \in \mathbb{C}$, pričom $\mathbb{Q}$ je podpole $\mathbb{C}$ a i je koreňom polynómu $f(x) = 1 + 0x + 1x^2$.

PRÍKLAD 3. Prvky e a π sú transcendentné nad $\mathbb{Q}$. Zjavne $e, \pi \in \mathbb{R}$, pričom $\mathbb{Q}$ je podpole $\mathbb{R}$. Avšak fakt, že ani e ani π nie sú koreňom polynómu nad $\mathbb{Q}$ nateraz ponecháme bez dôkazu.

DEFINÍCIA. Pole B je **jednoduchým algebraickým rozšírením** poľa A ak existuje prvok $u \in B$ algebraický nad A taký, že $B = A(u)$. Pole B je **jednoduchým transcendentným rozšírením** poľa A ak existuje prvok $u \in B$ transcendentný nad A taký, že $B = A(u)$.

VETA 9.6. *Ak sú u a v transcendentné prvky nad poľom $(A; +, \cdot)$, tak rozšírenia $A(u)$ a $A(v)$ sú izomorfné.*

NÁZNAK DÔKAZU. Izomorfizmom $A(u) \to A(v)$ je φ definované

$$\varphi\left(\frac{a_0 + a_1 u + a_2 u^2 + \cdots + a_n u^n}{b_0 + b_1 u + b_2 u^2 + \cdots + b_m u^m}\right) = \frac{a_0 + a_1 v + a_2 v^2 + \cdots + a_n v^n}{b_0 + b_1 v + b_2 v^2 + \cdots + b_m v^m}.$$

Podľa Vety 9.5 je φ všade definovaná a surjektívna relácia $A(u) \to A(v)$. Avšak nato, aby sme ukázali že φ je jednoznačná relácia a že je injektívna, potrebovali by sme trochu lepšie opísať podielové polia. Tým by sa ukázalo, že φ je bijekcia. Že je φ izomorfizmom, to plynie z toho, že nad A sú operácie $+$ a $\cdot$ z $A(u)$ a $A(v)$ totožné, a polynómy stupňa vyššieho ako 0 nie sú z A (keďže rozšírenia sú transcendentné). □

DEFINÍCIA. Polynóm $f(x)$ je **normovaný**, ak je koeficientom pri najvyššej mocnine x v tomto polynóme prvok e (jednotka). **Minimálny polynóm** prvku u algebraického nad poľom $(A; +, \cdot)$ je normovaný polynóm najnižšieho stupňa, pre ktorý platí $f(u) = 0$. Nuž a polynóm $f(x)$ je **ireducibilný**, ak sa nedá napísať ako súčin dvoch polynómov, z ktorých každý má stupeň aspoň 1.

LEMA 9.7. *Ak je m minimálny polynóm prvku u algebraického nad poľom $(A; +, \cdot)$, tak m je ireducibilný nad A.*

DÔKAZ. Nech $m = f \cdot g$, kde f aj g sú polynómy stupňa aspoň 1. Potom platí $m(u) = f(u) \cdot g(u)$, a keďže $(A; +, \cdot)$ je pole, tak podľa Vety 9.2 buď $f(u) = 0$

alebo $g(u) = 0$. Keďže f aj g sú polynómy stupňa aspoň 1, tak obidva tieto polynómy majú stupeň menší ako je stupeň polynómu m. Lenže to protirečí minimalite polynómu m. $\square$

Nasledujúca veta opisuje jednoduché algebraické rozšírenia.

VETA 9.8. *Nech je u algebraický prvok nad poľom $(A; +, \cdot)$ a nech má minimálny polynóm m prvku u stupeň n. Potom každý prvok v jednoduchého algebraického rozšírenia $A(u)$ vieme vyjadriť v tvare*

$$v = a_0 + a_1 u + a_2 u^2 + \cdots + a_{n-1} u^{n-1},$$

kde $a_0, a_1, \ldots, a_{n-1} \in A$.

NÁZNAK DÔKAZU. Podľa Vety 9.5 možno každý prvok v jednoduchého algebraického rozšírenia $A(u)$ vyjadriť v tvare

$$v = \frac{c_0 + c_1 u + c_2 u^2 + \cdots + c_o u^o}{b_0 + b_1 u + b_2 u^2 + \cdots + b_m u^m}, \tag{1}$$

kde $o, m \in \mathbb{N}$ a $c_0, c_1, \ldots, c_o, b_0, b_1, \ldots, b_m \in A$, pričom $b_0 + b_1 u + \cdots + b_m u^m \neq 0$.

Avšak v zlomku (1) stačí uvažovať len také čitatele a menovatele, ktoré sú polynómami stupňa nanajvýš $n - 1$. To preto, lebo ľubovoľný polynóm $p(x)$ vieme zapísať (pomocou delenia polynómom $m(x)$) v tvare $p(x) = m(x) \cdot q(x) + z(x)$, kde z má stupeň menší ako n. A keďže $m(u) = 0$, tak $p(u) = z(u)$.

Zostáva nám opísať, ako odstrániť menovateľa $r(u) = b_0 + b_1 u + b_2 u^2 + \cdots + b_m u^m$ v (1). Keďže m je ireducibilný polynóm (podľa Lemy 9.7) a stupeň r je menší ako stupeň m, tak najväčší spoločný deliteľ týchto dvoch polynómov je jednotka e. Lenže potom existujú polynómy m^* a r^* také, že $m(x) \cdot m^*(x) + r(x) \cdot r^*(x) = 1$ (toto tvrdenie sme nedokázali, preto sa jedná len o náznak dôkazu a nie o dôkaz; tvrdenie sa dá dokázať pomocou takzvaného Euklidovho algoritmu). Po dosadení u získavame $m(u) \cdot m^*(u) + r(u) \cdot r^*(u) = r(u) \cdot r^*(u) = 1$, čiže $r^*(u) = r^{-1}(u)$. Teda $p(u)/r(u) = p(u) \cdot r^*(u)$. $\square$

Z Vety 9.8 plynie nasledujúce tvrdenie.

DÔSLEDOK. *Ak je u algebraický nad poľom $(A; +, \cdot)$ a stupeň minimálneho polynómu prvku u je n, tak $A(u)$ s operáciou $+$ je vektorový priestor dimenzie n nad A s bázou $1, u, u^2, \ldots, u^{n-1}$.*

V ďalšom si ukážeme niekoľko príkladov. Ak je u algebraický nad poľom $(A; +, \cdot)$, tak počítanie v $A(u)$ sme v podstate opísali už v dôkaze Vety 9.8. Poznamenajme, že toto počítanie je dôsledkom skutočnosti, že $A(u)$ je faktorový okruh $A[x]/m$, kde m je minimálny polynóm prvku u a $A[x]$ je okruh všetkých polynómov nad A.

PRÍKLAD 1. Asi najznámejším jednoduchým algebraickým rozšírením je $\mathbb{R}(i)$, kde i je koreňom polynómu $x^2 + 1$. Keďže $i^2 + 1 = 0$, tak $i^2 = -1$, čo sa občas zapisuje ako $i = \sqrt{-1}$. Je zrejmé, že $\mathbb{R}(i) = \mathbb{C}$, čiže sa jedná o pole komplexných čísel. Prvkami $\mathbb{C}$ sú čísla $a + bi$, kde $a, b \in \mathbb{R}$.

Pole $\mathbb{R}$ sa nedá z $\mathbb{Q}$ získať pomocou jednoduchých algebraických rozšírení tak, ako sa dá získať $\mathbb{C}$ z $\mathbb{R}$. (Napríklad preto, lebo π nie je algebraické nad $\mathbb{Q}$, a teda toto číslo nevieme získať ani pomocou viacnásobných algebraických rozšírení poľa $\mathbb{Q}$.) Pomocou jednoduchých algebraických rozšírení však vieme pridať ku $\mathbb{Q}$ zopár reálnych čísel.

PRÍKLAD 2. Pole $\mathbb{Q}(\sqrt{2})$ získame rozšírením $\mathbb{Q}$ o koreň polynómu x^2-2. Prvkami poľa $\mathbb{Q}(\sqrt{2})$ sú čísla $a+b\sqrt{2}$, kde $a,b\in\mathbb{Q}$. V tomto poli je k číslu $a+b\sqrt{2}$ inverzné $\frac{a}{a^2-2b^2}+\frac{-b}{a^2-2b^2}\sqrt{2}$, keďže $(a+b\sqrt{2})(a-b\sqrt{2})=a^2-2b^2$. (Všimnime si, že ak $a+b\sqrt{2}\neq 0$, tak aj $a^2-2b^2\neq 0$.)

PRÍKLAD 3. Pole $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ získame rozšírením poľa $\mathbb{Q}(\sqrt{2})$ o koreň polynómu x^2-3. Prvkami poľa $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ sú čísla $(a+b\sqrt{2})+(c+d\sqrt{2})\sqrt{3}$, čiže prvky $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$, kde $a,b,c,d\in\mathbb{Q}$.

PRÍKLAD 4. Pole $\mathbb{Q}(\sqrt[3]{2})$ získame rozšírením $\mathbb{Q}$ o koreň polynómu x^3-2. Prvkami poľa $\mathbb{Q}(\sqrt[3]{2})$ sú čísla $a+b\sqrt[3]{2}+c\sqrt[3]{4}$, kde $a,b,c,d\in\mathbb{Q}$. V tomto poli je k prvku $1+\sqrt[3]{2}+\sqrt[3]{4}$ inverzný prvok $-1+\sqrt[3]{2}$.

POZNÁMKA. Vráťme sa k trom úlohám zo začiatku kapitoly. Ak máme v rovine danú úsečku, môžeme predpokladať, že jej dĺžka je 1 (ako jedna jednotka). Ak začiatok tejto úsečky prehlásime za počiatok súradnicovej sústavy, čiže bod $(0,0)$, a jej koniec za bod $(1,0)$, tak pomocou pravítka a kružidla ľahko zostrojíme všetky body (a,b), kde $a,b\in\mathbb{Z}$. A pomocou rovnoľahlosti vieme zostrojiť aj body (a,b), kde $a,b\in\mathbb{Q}$. Pomocou kružidla vieme k týmto bodom pridať aj druhé odmocniny, keďže rovnica kruhu je druhého stupňa. Takto postupne vieme rozširovať pole $\mathbb{Q}$ o $\sqrt{2},\sqrt{3},\ldots$. Je však zrejmé, že takto nikdy nedostaneme číslo π, pretože nato by sme potrebovali transcendentné rozšírenie poľa $\mathbb{Q}$. Tým je nahliadnutá nemožnosť kvadratúry kruhu. Nemožnosť zdvojenia kocky plynie z toho, že $\sqrt[3]{2}$ nevieme získať pomocou rozšírení poľa $\mathbb{Q}$ o druhé odmocniny (jedná sa zakaždým o rozšírenia druhého stupňa, pri k-násobných rozšíreniach získame rozšírenie stupňa 2^k, a keďže 3 nedelí 2^k, tak $\sqrt[3]{2}$ sa v týchto rozšíreniach nenachádza – toto je náznak riešenia). A podobne ako sa ukázala nemožnosť zdvojenia kocky sa dá ukázať nemožnosť trisekcie uhla (stačí si zvoliť vhodný uhol, napríklad $30°$).

Cvičenia

CVIČENIE 9.1. Určte, ktoré z nasledujúcich množín tvoria spolu so zvyčajným sčitovaním a násobením pole.

a) $\{a+b\sqrt{5};\ a,b\in\mathbb{Q}\}$
b) $\{a+b\sqrt[3]{3};\ a,b\in\mathbb{Q}\}$
c) $\{a+b\sqrt[3]{3}+c\sqrt[3]{9};\ a,b,c\in\mathbb{Q}\}$
d) $\{a+bi\sqrt{2};\ a,b\in\mathbb{Q}\}$
e) $\{a;\ a\in\mathbb{Q}\ \&\ a>0\}$
f) $\{a;\ a\in\mathbb{Q}\ \&\ a\geq 0\}$

Cvičenie 9.2. Dokážte, že množina $\mathcal{P}(X)$ všetkých podmnožín neprázdnej množiny X pri operáciách $A + B = A \div B$ (symetrická diferencia) a $A \cdot B = A \cap B$ tvorí okruh.

Cvičenie 9.3. Nech sú $(A_1; +_1, \cdot_1)$ a $(A_2; +_2, \cdot_2)$ okruhy, ktoré majú aspoň 2 prvky. Dokážte, že potom v priamom súčine $A_1 \times A_2$ týchto okruhov (operácie sú definované po zložkách tak, ako pri priamom súčine grúp) existujú netriviálne delitele nuly.

Cvičenie 9.4. Určte, ktoré prvky a majú v poli $(\mathbb{Z}_p; +, \cdot)$ druhú odmocninu (čiže existuje b také, že $b \cdot b = a$). Úlohu riešte pre $p \in \{3, 5, 7, 11, 13\}$.

Cvičenie 9.5. Ukážte, že $\mathbb{Z}_2 \times \mathbb{Z}_3$ a $\mathbb{Z}_6$ sú izomorfné okruhy. (Izomorfizmus okruhov a polí sa definuje presne tak, ako izomorfizmus grúp. Je to bijekcia zachovávajúca operácie.)

Cvičenie 9.6. Dokážte, že pole $\mathbb{C}$ je izomorfné s poľom všetkých matíc tvaru $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, kde $a, b \in \mathbb{R}$.

Cvičenie 9.7. V poli $\mathbb{C}$ zostrojte $[\{0, 1\}]$ a $[[\{0, 1\}]]$, čiže najmenší podokruh a podpole obsahujúce nulu a jednotku.

Cvičenie 9.8. Ukážte, že $\mathbb{Q}(\sqrt{2})$ a $\mathbb{Q}(-\sqrt{2})$ sú izomorfné polia.

Cvičenie 9.9. Ukážte, že z predpokladu „minimálne polynómy prvkov u a v nad poľom $(A; +, \cdot)$ sú rôzne“ nevyplýva $A(u) \neq A(v)$. Za pole A stačí zvoliť $\mathbb{Q}$.

Cvičenie 9.10. Dokážte, že ak majú prvky u a v rovnaké minimálne polynómy stupňa n nad poľom $(A; +, \cdot)$, tak zobrazenie $\varphi : A(u) \to A(v)$ definované vzťahom $\varphi(f(u)) = f(v)$, kde $f(x)$ je polynóm stupňa nanajvýš $n - 1$, je izomorfizmus.

10 TEÓRIA GRÚP 4

Štvorprvkové pole

Je zrejmé, že ak je p prvočíslo, tak je $(\mathbb{Z}_p; +, \cdot)$ pole. Je však poľom aj $(A; +, \cdot)$, kde $A = \{0, e, a, b\}$ a tabuľky pre operácie $+$ a $\cdot$ sú nasledovné?

$+$	0	e	a	b
0	0	e	a	b
e	e	0	b	a
a	a	b	0	e
b	b	a	e	0

$\cdot$	0	e	a	b
0	0	0	0	0
e	0	e	a	b
a	0	a	b	e
b	0	b	e	a

Viaceré z viet uvádzaných v tejto kapitole platia pre okruhy, respektíve pre okruhy bez deliteľov nuly, či pre komutatívne okruhy. My ich však budeme formulovať pre polia, lebo našim cieľom je charakterizovať konečné polia, dať návod na ich zostrojenie a na prácu s nimi.

Rád prvku a charakteristika poľa

Definícia. Nech je $(A; +, \cdot)$ pole. **Rádom prvku** $a \in A$ je najmenšie k také, že $\underbrace{a + a + \cdots + a}_{k} = 0$. Ak také k neexistuje, rádom a je ∞.

Všimnime si, že 0 je jediný prvok poľa, ktorého rád je 1.

Poznámka. Výraz $\underbrace{a + a + \cdots + a}_{k}$ budeme zapisovať skrátene $k \times a$. Ak teda píšeme $k \times a$, tak k je prirodzené číslo, a je prvok poľa. Symbol $\cdot$ si rezervujeme na násobenie prvkov poľa.

Lema 10.1. *V poli majú všetky nenulové prvky rovnaký rád.*

Dôkaz. Nech sú a a b nenulové prvky poľa $(A; +, \cdot)$, pričom a má rád k, b má rád l a $k \leq l$. Podľa distributívneho zákona platí $0 = (k \times a) \cdot b = k \times (a \cdot b) = a \cdot (k \times b)$, a podľa Lemy 9.2 $k \times b = 0$. Teda $l = k$. $\square$

DEFINÍCIA. Nech je $(A;+,\cdot)$ pole. **Charakteristika poľa** A je najmenšie prirodzené číslo k také, že $k \times a = 0$ pre každé $a \in A$. Ak také k neexistuje, tak charakteristika poľa je ∞.

POZNÁMKA. Ak je A pole, ktoré má okrem 0 ešte aspoň jeden prvok, tak jeho charakteristika je rádom jednotky e.

VETA 10.2. *Nech je $(A;+,\cdot)$ pole, ktoré má okrem 0 ešte aspoň jeden prvok. Potom jeho charakteristika je buď ∞ alebo prvočíslo.*

DÔKAZ. Stačí ukázať, že charakteristika nemôže byť zložené číslo. Sporom predpokladajme, že $(A;+,\cdot)$ má charakteristiku $k = mn$, kde $1 < m \le n < k$. Použitím distributívneho zákona dostávame

$$(\underbrace{e+e+\cdots+e}_{m})\cdot(\underbrace{e+e+\cdots+e}_{n}) = (\underbrace{e^2+e^2+\cdots+e^2}_{k}) = 0,$$

čo je v spore s Lemou 9.2, ktorá tvrdí, že v poli neexistujú netriviálne delitele nuly. □

VETA 10.3. *Nech je $(A;+,\cdot)$ pole s jednotkou e. Ak je charakteristika tohoto poľa ∞, tak $[[e]]$ je podpole A izomorfné s $(\mathbb{Q};+,\cdot)$; zatiaľ čo ak je charakteristika tohoto poľa p, tak $[[e]]$ je podpole A izomorfné so $(\mathbb{Z}_p;+,\cdot)$.*

DÔKAZ. Je zrejmé, že do $[[e]]$ patria všetky celočíselné násobky $n \times e$ prvku e. Čiže $\{n \times e;\ n \in \mathbb{Z}\} \subseteq [[e]]$. Ak je však charakteristika poľa p, kde p je prvočíslo, tak $\{n \times e;\ n \in \mathbb{Z}\} = \{0,1,\ldots,p{-}1\}$. Ukážeme, že zobrazenie φ poľa $(\mathbb{Z}_p;+,\cdot)$ do podmnožiny $\{0,1,\ldots,p{-}1\}$ poľa $(A;+,\cdot)$, definované $\varphi(n) = n \times e$, je izomorfizmom. A izomorfizmom je toto zobrazenie preto, lebo

$$\varphi(m \oplus n) = (m \oplus n) \times e = (m+n) \times e = (m \times e) + (n \times e) = \varphi(m) + \varphi(n)$$
$$\varphi(m \odot n) = (m \odot n) \times e = (mn) \times e = (m \times e) \cdot (n \times e) = \varphi(m) \cdot \varphi(n).$$

(Kvôli rozlíšeniu operácií v poliach $\mathbb{Z}_p$ a A sme v poli $\mathbb{Z}_p$ použili $\oplus$ a $\odot$ na sčítanie, respektíve násobenie.) Keďže φ je izomorfizmus, $\{0,1,\ldots,p{-}1\}$ je hľadané podpole poľa $(A;+,\cdot)$.

Predpokladajme teraz, že charakteristika poľa $(A;+,\cdot)$ je ∞. V takom prípade $\{n \times e;\ n \in \mathbb{Z}\}$ nie je uzavreté na inverzné prvky vzhľadom na násobenie. Podľa Vety 9.3 $[[e]]$ obsahuje aj všetky prvky tvaru $(m \times e)\cdot(n \times e)^{-1}$, kde $m,n \in \mathbb{Z}$. To však stačí, lebo zobrazenie φ poľa $\mathbb{Q}$ do $\{(m \times e)\cdot(n \times e)^{-1};\ m,n \in \mathbb{Z}\}$ definované $\varphi(m/n) = (m \times e)\cdot(n \times e)^{-1}$ je izomorfizmom. A izomorfizmom je toto zobrazenie preto, lebo (kvôli zjednodušeniu zápisu vynechávame znak násobenia $\cdot$)

$$\begin{aligned}
\varphi(m/n + k/l) &= \varphi\big((ml+kn)/nl\big) = \big((ml+kn)\times e\big)\big((nl)\times e\big)^{-1} = \\
&= \big((ml)\times e + (kn)\times e\big)\big((n\times e)(l\times e)\big)^{-1} = \\
&= \big((m\times e)(l\times e) + (k\times e)(n\times e)\big)\big((n\times e)(l\times e)\big)^{-1} = \\
&= (m\times e)(n\times e)^{-1} + (k\times e)(l\times e)^{-1} = \varphi(m/n) + \varphi(k/l);\\
\varphi\big((m/n)(k/l)\big) &= \varphi\big((mk)/(nl)\big) = (mk\times e)(nl\times e)^{-1} = \\
&= (m\times e)(k\times e)(n\times e)^{-1}(l\times e)^{-1} = \varphi(m/n)\cdot\varphi(k/l). \quad \square
\end{aligned}$$

Pripomeňme si definíciu vektorového priestoru.

DEFINÍCIA. Nech je A pole. Ďalej nech je V množina, na ktorej je daná binárna operácia $+$, a nech je každému $a \in A$ a $\alpha \in V$ priradený prvok $a \cdot \alpha \in V$, pričom platí

(a) $(V; +)$ je komutatívna grupa;
(b) $a \cdot (\alpha + \beta) = a \cdot \alpha + a \cdot \beta$ pre každé $a \in A$ a $\alpha, \beta \in V$;
(c) $(a + b) \cdot \alpha = a \cdot \alpha + b \cdot \alpha$ pre každé $a, b \in A$ a $\alpha \in V$;
(d) $(a \cdot b) \cdot \alpha = a \cdot (b \cdot \alpha)$ pre každé $a, b \in A$ a $\alpha \in V$;
(e) $e \cdot \alpha = \alpha$ pre každé $\alpha \in V$.

Potom V tvorí **vektorový priestor** nad poľom A.

VETA 10.4. *Počet prvkov konečného poľa je mocnina jeho charakteristiky.*

DÔKAZ. Nech charakteristika nášho poľa $(A; +, \cdot)$ je p. Podľa Vety 10.3 (navzájom izomorfné polia môžeme považovať za totožné) je $\mathbb{Z}_p$ podpole poľa A. Avšak potom možno A chápať ako vektorový priestor nad poľom $\mathbb{Z}_p$. Keďže dimenzia tohoto priestoru je konečná, musí v ňom existovať konečná báza, povedzme $u_1, u_2, \ldots, u_t$. Teda každý prvok α vektorového priestoru A sa dá vyjadriť jednoznačne ako lineárna kombinácia $\alpha = a_1 u_1 + a_2 u_2 + \cdots + a_t u_t$, pričom koeficienty a_i sú z poľa $\mathbb{Z}_p$. Keďže existuje práve p^t rôznych t-tic prvkov poľa $\mathbb{Z}_p$, tak počet prvkov vektorového priestoru (poľa) A je p^t. □

Konečné polia

VETA 10.5. *Nech je $(A; +, \cdot)$ konečné pole s q prvkami. Potom pre každý prvok $a \in A$ platí $a^q = a$.*

DÔKAZ. Rovnosť $a^q = a$ je očividne splnená pre $a = 0$, a preto v ďalšom predpokladajme, že $a \neq 0$. Nenulových prvkov poľa A je $q - 1$ a tieto prvky tvoria multiplikatívnu grupu. Podľa Vety 8.3 rád každého prvku delí počet prvkov grupy, čiže $a^{q-1} = e$, z čoho plynie $a^q = a$. □

Pre nasledujúci dôsledok uvádzame len náznak dôkazu, pretože sa v argumentácii budeme často opierať len o intuíciu. Korektný dôkaz by si vyžiadal zavedenie pojmu Euklidovský okruh polynómov a odvodenie základných viet pre tento okruh. Avšak na to nemáme dostatok priestoru.

DÔSLEDOK. *Nech sú $a_1, a_2, \ldots, a_q$ všetky prvky konečného poľa $(A; +, \cdot)$. Potom platí $(x - a_1)(x - a_2) \ldots (x - a_q) = x^q - x$.*

NÁZNAK DÔKAZU. Majme dva polynómy $f(x)$ a $g(x)$. Keď ich vydelíme, dostaneme čiastočný podiel $q(x)$ a zvyšok $r(x)$, čiže $f(x) = g(x) \cdot q(x) + r(x)$, pričom stupeň $r(x)$ je menší ako stupeň $g(x)$. To znamená, že ak je $g(x)$ lineárny polynóm, napríklad $x - a_i$, tak zvyškom je konštanta r. Keďže platí $a_i^q - a_i = 0$ pre každé $i = 1, 2, \ldots, q$, tak $x^q - x = (x - a_i) \cdot q(x) + 0$ (dosaďte a_i za x), kde $q(x)$ je nejaký polynóm. Teda $x - a_i$ delí $x^q - x$ pre každé a_i.

Na druhej strane, polymómy $x - a_i$ a $x - a_j$, $1 \leq i < j \leq q$, sú navzájom nesúdeliteľné. Preto ich súčin $(x-a_1)(x-a_2)\dots(x-a_q)$ delí $x^q - x$. Keďže polynómy $(x-a_1)(x-a_2)\dots(x-a_q)$ a $x^q - x$ majú rovnaký stupeň a vedúcim koeficientom v obidvoch je jednotka e, tieto polynómy sa musia rovnať. □

VETA 10.6. *Multiplikatívna grupa G^* všetkých nenulových prvkov konečného poľa $(A; +, \cdot)$ s q prvkami je cyklická.*

NÁZNAK DÔKAZU. Grupa G^* má $q-1$ prvkov. Rozložme $q-1$ na súčin prvočiniteľov, čiže zapíšme $q - 1 = p_1^{t_1} p_2^{t_2} \dots p_k^{t_k}$ a označme t_i' najväčšiu mocninu p_i, pre ktoré existuje prvok G^* rádu $p_i^{t_i'}$. Podľa Vety 8.3 rád každého prvku grupy delí počet prvkov grupy, a teda $t_i' \leq t_i$ pre všetky $i = 1, 2, \dots, k$. Rozoberme dva prípady:

(1) Pre každé i platí $t_i' = t_i$. Potom G^* obsahuje prvky $a_1, a_2, \dots, a_k$ rádov $p_1^{t_1}, p_2^{t_2}, \dots, p_k^{t_k}$. Keďže tieto prvky komutujú, tak ich súčin má rád $p_1^{t_1} p_2^{t_2} \dots p_k^{t_k}$ (toto tvrdenie sa dá dokázať indukciou vzhľadom na k pri využití skutočnosti, že $p_i^{l_1}$ a $p_j^{l_2}$ sú pre $i \neq j$ a $l_1, l_2 > 0$ nesúdeliteľné). To však znamená, že G^* je cyklická grupa.

(2) Pre niektoré j platí $t_j' < t_j$. Nech je a ľubovoľný prvok grupy G^* a nech je $p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ jeho rád. Označme n súčin všetkých $p_i^{r_i}$ s výnimkou $p_j^{r_j}$. Potom rád prvku a^n je práve $p_j^{r_j}$. Keďže $r_j \leq t_j'$, tak rád každého prvku grupy delí súčin $p_1^{t_1'} p_2^{t_2'} \dots p_k^{t_k'}$, ktorý je vlastným deliteľom $q-1$.

Ak teda grupa G^* nie je cyklická, tak pre $t = p_1^{t_1'} p_2^{t_2'} \dots p_k^{t_k'}$ dostávame, že $x - a$ delí $x^{t-1} - 1$, kde $t - 1 < q - 1$, pre každé $a \in G^*$. To by však znamenalo, že súčin všetkých členov $x-a$, $a \in G^*$, delí polynóm $x^{t-1}-1$, čo je v spore s predchádzajúcim dôsledkom. □

DÔSLEDOK. *Konečné pole s $q = p^t$ prvkami je jednoduchým algebraickým rozšírením poľa $\mathbb{Z}_p$.*

DÔKAZ. Nech je $(A; +, \cdot)$ pole s $q = p^t$ prvkami. Podľa Vety 10.3 je $(\mathbb{Z}_p; +, \cdot)$ podpole A. Nech je c prvok, ktorý generuje multiplikatívnu grupu G^* poľa $(A; +, \cdot)$. Potom $\mathbb{Z}_p(c)$ je podpole A ktoré má aspoň toľko prvkov, ako A. Keďže A má konečne veľa prvkov, $\mathbb{Z}_p(c)$ a A sú izomorfné polia. □

Teraz môžeme sformulovať najpodstatnejšie tvrdenie tejto kapitoly. Uvádzame ho bez dôkazu.

VETA 10.7. *Pre každé číslo tvaru $q = p^t$, kde p je prvočíslo a $t > 0$ je prirodzené číslo, existuje (až na izomorfizmus) práve jedno q-prvkové pole. Toto pole sa nazýva* **Galoisovo** *a označuje sa symbolom $GF(q)$.*

Vytvorenie Galoisovho poľa $GF(p^t)$

Na vytvorenie $GF(p^t)$ nám stačí nájsť vhodný ireducibilný polynóm $m(x)$ stupňa t nad $\mathbb{Z}_p$. Tento polynóm bude podľa Vety 10.5 deliť $x^q - x$ a $GF(p^t)$ bude faktorovým poľom $\mathbb{Z}_p[x]/m(x)$ (kde $\mathbb{Z}_p[x]$ je okruh polynómov nad $\mathbb{Z}_p$). Z tejto poznámky je zrejmé, ako sa bude v $GF(p^t)$ počítať (pozri Vetu 9.8). Problémom je nájsť vhodný ireducibilný polynóm. Tieto sa dajú nájsť v rôznych publikáciách, a ako príklad tu uvádzame jeden takýto polynóm pre každé $t = 1, 2, \ldots, 15$ nad $\mathbb{Z}_2$.

t	polynóm
2	$x^2 + x + 1$
3	$x^3 + x + 1$
4	$x^4 + x + 1$
5	$x^5 + x^2 + 1$
6	$x^6 + x + 1$
7	$x^7 + x^3 + 1$
8	$x^8 + x^4 + x^3 + x^2 + 1$

t	polynóm
9	$x^9 + x^4 + 1$
10	$x^{10} + x^4 + 1$
11	$x^{11} + x^2 + 1$
12	$x^{12} + x^6 + x^4 + x + 1$
13	$x^{13} + x^4 + x^3 + x + 1$
14	$x^{14} + x^{10} + x^6 + x + 1$
15	$x^{15} + x + 1$

PRÍKLAD 1. Zostrojme pole $GF(4)$. Podľa predchádzajúcej tabuľky je vhodným polynómom $m(x) = x^2 + x + 1$. Potom $GF(4)$ bude mať prvky $0, 1, x_0, x_0 + 1$, kde x_0 je koreňom polynómu $m(x)$. Tabuľkami pre sčítanie a násobenie sú

$+$	0	1	x_0	$x_0{+}1$
0	0	1	x_0	$x_0{+}1$
1	1	0	$x_0{+}1$	x_0
x_0	x_0	$x_0{+}1$	0	1
$x_0{+}1$	$x_0{+}1$	x_0	1	0

$\cdot$	0	1	x_0	$x_0{+}1$
0	0	0	0	0
1	0	1	x_0	$x_0{+}1$
x_0	0	x_0	$x_0{+}1$	1
$x_0{+}1$	0	$x_0{+}1$	1	x_0

pričom násobenie je „modulo“ polynóm $m(x)$. Takže pre súčin x_0 a $x_0 + 1$ máme $x_0(x_0{+}1) = x_0^2 + x_0 = x_0^2 + x_0 + 1 + 1 = m(x_0) + 1 = 1$. Podobne vieme vypočítať $(x_0{+}1)(x_0{+}1) = x_0^2 + x_0 + x_0 + 1 = x_0^2 + 1 = m(x_0) + x_0 = x_0$ atď. Všimnime si, že toto pole je izomorfné so štvorprvkovou štruktúrou uvedenou na začiatku kapitoly.

PRÍKLAD 2. Zostrojme pole $GF(16)$. Vhodným ireducibilným polynómom je $m(x) = x^4 + x + 1$ a prvkami sú polymómy v x_0, stupňa nanajvýš 3 nad $\mathbb{Z}_2$. Opäť, x_0 je koreňom $m(x)$. Sčítanie prvkov $GF(16)$ je triviálne, pre násobenie využijeme skutočnosť (zistenú metódou pokusov a omylov), že x_0 je generátor multiplikatívnej grupy G^* poľa $GF(16)$. Dostávame nižšie uvedenú tabuľku. Podľa nej súčinom $x_0^2 + 1$ a $x_0^3 + x_0 + 1$ je $(x_0^2 + 1)(x_0^3 + x_0 + 1) = x_0^8 x_0^7 = x_0^{15} = 1$. Respektíve $(x_0^3 + x_0^2 + x_0 + 1)^2 = x_0^{12} x_0^{12} = x_0^{24} = x_0^{15+9} = 1 \cdot x^9 = x_0^3 + x_0$ atď. V tejto tabuľke vieme veľmi rýchlo hľadať inverzné prvky. To preto, lebo k x_0^i je inverzným x_0^{15-i}.

Všimnime si, že $\{x_0^5, x_0^{10}, x_0^{15}{=}1, 0\}$ je podpole $GF(16)$. Uzavretosť na násobenie je zrejmá z uvedeného zápisu a uzavretosť na sčítanie plynie z toho, že $x_0^5 + 1 = x_0^{10}$.

$$
\begin{array}{lll}
x_0 = x_0 & x_0^6 = x_0^3 + x_0^2 & x_0^{11} = x_0^3 + x_0^2 + x \\
x_0^2 = x_0^2 & x_0^7 = x_0^3 + x_0 + 1 & x_0^{12} = x_0^3 + x_0^2 + x_0 + 1 \\
x_0^3 = x_0^3 & x_0^8 = x_0^2 + 1 & x_0^{13} = x_0^3 + x_0^2 + 1 \\
x_0^4 = x_0 + 1 & x_0^9 = x_0^3 + x_0 & x_0^{14} = x_0^3 + 1 \\
x_0^5 = x_0^2 + x_0 & x_0^{10} = x_0^2 + x_0 + 1 & x_0^{15} = 1
\end{array}
$$

PRÍKLAD 3. Zostrojme pole $GF(27)$. Vhodným ireducibilným polynómom je $m(x) = x^3 + 2x + 1$ a prvkami sú polymómy v koreni x_0 stupňa nanajvýš 2 nad $\mathbb{Z}_3$. Sčítanie týchto polynómov je zrejmé. Napríklad $(x_0^2 + 2x_0 + 2) + (2x_0^2 + 2x_0 + 1) = x_0$. Pre násobenie opäť využijeme, že x_0 generuje multiplikatívnu grupu G^*. Avšak aby sme si zjednodušili zápis, budeme polynómy kódovať pomocou ich koeficientov. Tak napríklad $2x_0^2 + 1$ zapíšeme 201, zatiaľ čo $2x_0$ zapíšeme 020 ap. Dostávame tabuľku

$x_0 = 010$	$x_0^6 = 111$	$x_0^{11} = 112$	$x_0^{16} = 021$	$x_0^{21} = 101$
$x_0^2 = 100$	$x_0^7 = 122$	$x_0^{12} = 102$	$x_0^{17} = 210$	$x_0^{22} = 022$
$x_0^3 = 012$	$x_0^8 = 202$	$x_0^{13} = 002$	$x_0^{18} = 121$	$x_0^{23} = 220$
$x_0^4 = 120$	$x_0^9 = 011$	$x_0^{14} = 020$	$x_0^{19} = 222$	$x_0^{24} = 221$
$x_0^5 = 212$	$x_0^{10} = 110$	$x_0^{15} = 200$	$x_0^{20} = 211$	$x_0^{25} = 201$

pričom $x_0^{26} = 001$, čiže $x_0^{26} = 1$.

Cvičenia

CVIČENIE 10.1. Dokážte že v každom poli tvorí množina všetkých prvkov konečného rádu podpole.

CVIČENIE 10.2. Ukážte, že ak je charakteristika poľa A rôzna od 2, tak v A možno riešiť kvadratické rovnice metódou doplnenia na úplný štvorec. Odvoďte všeobecný vzorec pre riešenie kvadratických rovíc v A.

CVIČENIE 10.3. Dokážte, že ak je v konečnom poli a koreňom rovnice $x^n - 1 = 0$, tak aj každá mocnica a je koreňom tejto rovnice.

CVIČENIE 10.4. Dokážte, že pre každé prvočíslo p a $a \in \mathbb{N}$ platí **malá Fermatova veta**, čiže platí $a^p \equiv a \pmod{p}$

Cvičenie 10.5. Dokážte, že množina $\{0,1\} \times \{0,1\}$ tvorí štvorprvkové pole $GF(4)$, ak na nej definujeme sčítanie modulo 2 po zložkách a násobenie podľa vzťahu $(a,b) \times (u,v) = (au + bv, av + bu)$.

Cvičenie 10.6. Prvok konečného poľa je **primitívny** ak generuje cyklickú grupu G^* nenulových prvkov vzhľadom na násobenie. Dokážte, že ak je a primitívny prvok poľa $GF(q)$, tak a^j je primitívny práve vtedy, keď sú čísla j a $q-1$ nesúdeliteľné. (Dôsledkom tohoto tvrdenia je, že $GF(q)$ má $\varphi(q-1)$ primitívnych prvkov, kde φ je Eulerova funkcia.)

Cvičenie 10.7. Zostrojte tabuľky sčítania a násobenia pre pole $GF(8)$.

Cvičenie 10.8. Zostrojte tabuľky sčítania a násobenia pre pole $GF(9)$.

Cvičenie 10.9. Zostrojte pole $GF(25)$.

Cvičenie 10.10. Dokážte, že $GF(4)$ nie je podpole $GF(8)$.

Cvičenie 10.11. Pre ktoré hodnoty $k \in \mathbb{Z}_7$ je $\mathbb{Z}_7[x]/(x^2 + k)$ poľom?

11 TEÓRIA GRÚP 5

Matematické štruktúry

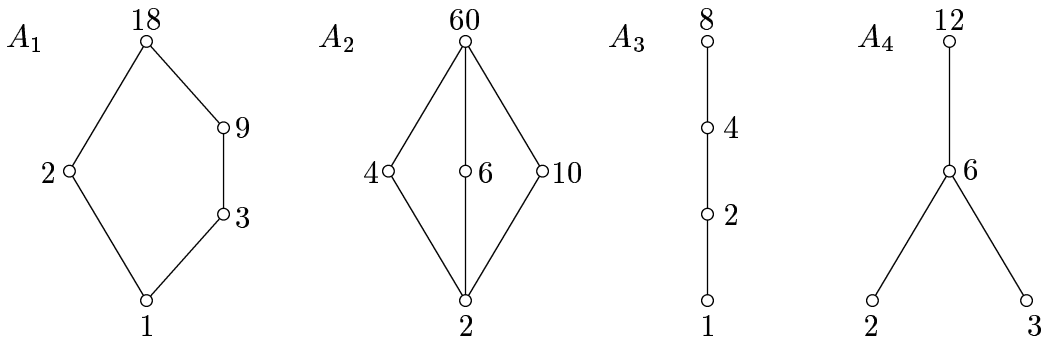
Reálne čísla môžeme sčitovať aj násobiť. Tieto binárne operácie tvorili s množinou $\mathbb{R}$ aditívnu, respektíve multiplikatívnu grupu, a obidve operácie spoločne tvorili na $\mathbb{R}$ pole. Avšak reálne čísla môžeme aj usporiadať. Usporiadanie je tvorené binárnou reláciou $\leq$, ktorá na $\mathbb{R}$ tvorí zväz. Nuž a práve zväzmi sa budeme zaoberať v tejto kapitole.

Zväzy

DEFINÍCIA. Binánu reláciu $\leq$ na neprázdnej množine A nazývame **čiastočné usporiadanie**, ak pre každé $a, b, c \in A$ platí

(a) $(a \leq a)$ (**reflexívnosť**);
(b) $\big((a \leq b)\ \&\ (b \leq c)\big) \Rightarrow (a \leq c)$ (**tranzitívnosť**);
(c) $\big((a \leq b)\ \&\ (b \leq a)\big) \Rightarrow (a = b)$ (**antisymetričnosť**).

PRÍKLAD. Nech je A potenčná množina množiny M (čiže A je množina všetkých podmnožín M). Relácia inklúzie $\subseteq$ je čiastočným usporiadaním A. To preto, lebo pre každé množiny $X, Y, Z \in A$ platí $X \subseteq X$ ($\subseteq$ je reflexívna relácia), ak $X \subseteq Y$ a $Y \subseteq Z$ tak $X \subseteq Z$ ($\subseteq$ je tranzitívna) a ak $X \subseteq Y$ a $Y \subseteq X$ tak $X = Y$ ($\subseteq$ je antisymetrická).



Obrázok 6

Čiastočné usporiadanie na konečnej množine vizualizujeme pomocou **Hasseho diagramu**. Hasseho diagram je graf, v ktorom krúžky predstavujú prvky A. Ak sú dva krúžky a a b spojené úsečkou idúcou „zdola nahor“ od prvku a k b, tak platí $a \leq b$ a zároveň neexistuje prvok x rôzny od a a b, pre ktorý by platilo $a \leq x$ a $x \leq b$.

PRÍKLAD. Relácia „delí bezo zvyšku“ (označujeme $|$) je čiastočným usporiadaním na ľubovoľnej podmnožine množiny kladných celých čísel. Na Obrázku 6 sú Hasseho diagramy tohto čiastočného usporiadania pre množiny $A_1 = \{1, 2, 3, 9, 18\}$, $A_2 = \{2, 4, 6, 10, 60\}$, $A_3 = \{1, 2, 4, 8\}$ a $A_4 = \{2, 3, 6, 12\}$.

DEFINÍCIA. Nech je $\leq$ čiastočné usporiadanie na množine A a nech $a, b \in A$.

(1) Prvok $c \in A$ nazývame **infimum** (**priesek**) prvkov a a b ak platí $c \leq a$, $c \leq b$ a pre každé x pre ktoré platí $x \leq a$ a $x \leq b$ platí aj $x \leq c$.
(2) Prvok $c \in A$ nazývame **suprémum** (**spojenie**) prvkov a a b ak platí $a \leq c$, $b \leq c$ a pre každé x pre ktoré platí $a \leq x$ a $b \leq x$ platí aj $c \leq x$.

Infimum prvkov a a b zaznačujeme $a \wedge b$ a suprémum $a \vee b$.

VETA 11.1. *Nech je $\leq$ čiastočné usporiadanie na množine A. Potom pre každé $a, b, c \in A$ platí*

(A1)	$a \wedge b = b \wedge a$	*(komutatívnosť)*
(A2)	$a \vee b = b \vee a$	*(komutatívnosť)*
(A3)	$a \wedge (b \wedge c) = (a \wedge b) \wedge c$	*(asociatívnosť)*
(A4)	$a \vee (b \vee c) = (a \vee b) \vee c$	*(asociatívnosť)*
(A5)	$a \wedge (b \vee a) = a$	*(zákon absorbcie)*
(A6)	$a \vee (b \wedge a) = a$	*(zákon absorbcie)*

DÔKAZ. Vlastnosti (A1) a (A2) platia triviálne.

Rozpísaním $d = a \wedge (b \wedge c)$ dostávame $d \leq a$, $d \leq b$, $d \leq c$, pričom d je najväčší prvok spĺňajúci tieto nerovnosti. Keďže rozpísaním $(a \wedge b) \wedge c$ dostávame to isté, platí (A3). Podobne sa nahliadne aj (A4).

Ak $u \leq v$ tak $u \wedge v = u$. Keďže $a \leq b \vee a$, platí $a \wedge (b \vee a) = a$. Analogicky ak $u \leq v$ tak $v \vee u = v$. Keďže $b \wedge a \leq a$, platí $a \vee (b \wedge a) = a$. □

DEFINÍCIA. **Zväz** je dvojica $(A; \leq)$, kde $\leq$ je čiastočné usporiadanie na množine A, pričom každé dva prvky majú v A infimum aj suprémum.

PRÍKLAD. Zväzmi sú $(A_1; |)$, $(A_2; |)$ a $(A_3; |)$ z Obrázku 6, zatiaľ čo $(A_4; |)$ zväzom nie je, pretože prvky 2 a 3 nemajú infimum.

DEFINÍCIA. Nech je $(A; \leq)$ zväz. Podzväzom tohoto zväzu je taká neprázdna podmnožina B množiny A (relácie sú identické), pre ktorú platí:

$$(\forall a)(\forall b)\Big((a \in B) \;\&\; (b \in B)\Big) \Rightarrow \Big(\big((a \wedge b) \in B\big) \;\&\; \big((a \vee b) \in B\big)\Big).$$

PRÍKLAD. Zväzy $(A_1; |)$ a $(A_2; |)$ z Obrázku 6 nie sú podzväzmi zväzu $(\mathbb{N}^+; |)$, zatiaľ čo $(A_3; |)$ je podzväzom $(\mathbb{N}^+; |)$.

VETA 11.2. *V každom zväze $(A; \leq)$ pre všetky $a, b, c \in A$ platí:*

(D1') $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$ **zákon polodistributívnosti**
(D2') $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$ **zákon polodistributívnosti**

DÔKAZ. Dokážeme prvé tvrdenie, pretože druhé sa dokazuje analogicky.

Zjavne $(a \wedge b) \leq a$ a $(a \wedge c) \leq a$, a teda $(a \wedge b) \vee (a \wedge c) \leq a$ z definície supréma. Podobne $(a \wedge b) \leq b$ a $(a \wedge c) \leq c$, takže pre suprémum $(b \vee c)$ platí $(a \wedge b) \vee (a \wedge c) \leq (b \vee c)$. Avšak z definície infima pre prvky a a $(b \vee c)$ dostávame $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$. □

DEFINÍCIA. Zväz $(A; \leq)$ je **distributívny** ak pre každé $a, b, c \in A$ platí

(D1) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ **distributívny zákon**
(D2) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ **distributívny zákon**

PRÍKLAD. Zväzy $(\mathbb{R}; \leq)$, $(\mathbb{N}^+; |)$ aj $(\mathcal{P}(M); \subseteq)$, kde M je množina (prázdna, konečná, či nekonečná), sú distributívne.

VETA 11.3. *Zväz $(A; \leq)$ je distributívny práve vtedy, keď neobsahuje podzväz izomorfný so zväzom $(A_1; |)$ či $(A_2; |)$ z Obrázku 6.*

NÁZNAK DÔKAZU. Nech je zväz $(A; \leq)$ distributívny. Potom všetky prvky A spĺňajú identity (D1) a (D2), a teda každý podzväz A musí byť tiež distributívny. Avšak vo zväze $(A_1; |)$ z Obrázku 6 pre $a = 9$, $b = 3$ a $c = 2$ máme

$$a \wedge (b \vee c) = 9 \wedge (3 \vee 2) = 9 \wedge 18 = 9$$
$$(a \wedge b) \vee (a \wedge c) = (9 \wedge 3) \vee (9 \wedge 2) = 3 \vee 1 = 3$$

zatiaľ čo vo zväze $(A_2; |)$ z Obrázku 6 pre $a = 4$, $b = 6$ a $c = 10$ máme

$$a \wedge (b \vee c) = 4 \wedge (6 \vee 10) = 4 \wedge 60 = 4$$
$$(a \wedge b) \vee (a \wedge c) = (4 \wedge 6) \vee (4 \wedge 10) = 2 \vee 2 = 2$$

čiže ani jeden z týchto zväzov nie je distributívny.

Dôkaz skutočnosti, že ak zväz neobsahuje podzväz izomorfný so zväzom $(A_1; |)$ či $(A_2; |)$ z Obrázku 6, tak je distributívny, je zložitejší. Preto ho vynechávame. □

Ďalšie pekné tvrdenie o distributívnych zväzoch uvádzame bez dôkazu.

VETA 11.4. *Každý distributívny zväz je izomorfný s podzväzom zväzu podmnožín nejakej množiny M s inklúziou, $(\mathcal{P}(M); \subseteq)$.*

VETA 11.5. *Nech je $(A;\leq)$ distributívny zväz a $a,b,c \in A$. Potom ak platí $a \wedge b = a \wedge c$ a $a \vee b = a \vee c$, tak nutne $b = c$.*

DÔKAZ. Využitím zákonov absorbcie, komutatívnosti, distributívnych zákonov a s využitím predpokladov, dostávame:

$$b = b \wedge (a \vee b) = b \wedge (a \vee c) = (b \wedge a) \vee (b \wedge c) =$$
$$= ((c \wedge a) \vee (b \wedge c) = c \wedge (a \vee b) = c \wedge (a \vee c) = c \quad \square$$

Booleove algebry

DEFINÍCIA. Nech je $(A;\leq)$ zväz s najmenším prvkom 0 (čiže pre každé $a \in A$ platí $0 \leq a$) a najväčším prvkom 1 (čiže pre každé $a \in A$ platí $a \leq 1$). Nech $a \in A$. Prvok $b \in A$ nazývame **komplementom** prvku a ak platí $a \vee b = 1$ a $a \wedge b = 0$. Komplement prvku a označujeme a'.

LEMA 11.6. *V distributívnom zväze $(A;\leq)$ s najmenším a najväčším prvkom má každý prvok $a \in A$ nanajvýš jeden komplement.*

DÔKAZ. Nech sú b a c komplementy prvku a. Potom platí $a \wedge b = a \wedge c$ a $a \vee b = a \vee c$. Z toho podľa Vety 11.5 dostávame $b = c$. $\square$

DEFINÍCIA. Distributívny zväz $(A;\leq)$ s najmenším prvkom 0 a najväčším prvkom 1, v ktorom ku každému prvku a existuje komplement a', nazývame **Booleovou algebrou**. Túto Booleovu algebru zapisujeme $(A;\wedge,\vee,',0,1)$.

V Booleovej algebre sú relácie $\wedge$ a $\vee$ binárne, relácia komplementu $'$ je unárna, zatiaľ čo relácie 0 a 1 sú nulárne.

POZNÁMKA. Všimnime si, že v zápise Booleovej algebry $(A;\wedge,\vee,',0,1)$ sa nevyskytuje relácia čiastočného usporiadania $\leq$. Avšak môžeme si ju spätne rekonštruovať zavedením $a \leq b$ práve vtedy, keď $a \wedge b = a$ (alebo ekvivalentne $a \vee b = b$).

DEFINÍCIA. Majme Booleovu algebru $(A;\wedge,\vee,',0,1)$. Prvok $a \in A$ je **atóm** ak zo vzťahu $x \leq a$ plynie $x = 0$ alebo $x = a$.

Nasledujúca veta je zosilnením Vety 11.4 pre Booleove algebry.

VETA 11.7. *Nech je $(A;\wedge,\vee,',0,1)$ konečná Booleova algebra (čiže A je konečná množina). Potom je táto algebra izomorfná so zväzom $(\mathcal{P}(M);\subseteq)$ pre nejakú konečnú množinu M.*

NÁZNAK DÔKAZU. Dôkaz nie je ťažký, je však trocha zdĺhavý. Preto uvedieme len hľadaný izomorfizmus.

Nech je M množina všetkých atómov $(A;\wedge,\vee,',0,1)$. Potom $(A;\wedge,\vee,',0,1)$ je izomorfná s $(\mathcal{P}(M);\subseteq)$, pričom pre izomorfizmus φ máme $\varphi(a) = a$ pre každý atóm a. Samozrejme, $\varphi(0) = \emptyset$. A pre každý iný prvok $b \in A$ máme $\varphi(b) = B$, kde B je množina atómov a pre ktoré $a \leq b$. $\square$

DÔSLEDOK. *Konečná Booleova algebra má 2^n prvkov, kde n je počet jej atómov.*

DÔKAZ. Podľa Vety 11.7 je $(A; \wedge, \vee, ', 0, 1)$ izomorfná so zväzom $(\mathcal{P}(M); \subseteq)$ pre nejakú konečnú množinu M. Avšak ak má M práve n prvkov, tak $\mathcal{P}(M)$ má 2^n prvkov, pričom atómami sú práve prvky množiny M. □

Veta 11.7 je veľmi silné tvrdenie. Pomocou nej môžeme pre Booleove algebry dokazovať identity tak, že sa odvoláme na analogické tvrdenia z teórie množín. Tak napríklad platí:

LEMA 11.8. *Nech je $(A; \wedge, \vee, ', 0, 1)$ konečná Booleova algebra. Potom pre každé $x, y \in A$ platí*

(M1) $(x \vee y)' = (x' \wedge y')$ **de Morganov zákon**
(M2) $(x \wedge y)' = (x' \vee y')$ **de Morganov zákon**

DÔKAZ. Tvrdenie je dôsledkom Vety 11.7 a Vety 6.2. □

Ďalšia aplikácia Booleovych algebier je vo výrokovej logike. Keď nahradíme disjunkcie suprémom, konjunkcie infimom a negácie komplementom, tak výroková formula je tautológiou práve vtedy, keď sa jej zápis v Booleovej algebre dá zjednodušiť na 1.

PRÍKLAD. Dokážeme, že $A \Rightarrow (B \Rightarrow A)$ je tautológia. Najprv nahradíme všetky implikácie $C \Rightarrow D$ disjunkciami $\neg C \vee D$, výrok prepíšeme ako tvrdenie v Booleovej algebre, nato využijeme komutatívny zákon, následne asociatívny zákon, definíciu komplementu a supréma. Dostávame

$$A \Rightarrow (B \Rightarrow A) = \neg A \vee (\neg B \vee A) = A' \vee (B' \vee A) =$$
$$= A' \vee (A \vee B') = (A' \vee A) \vee B' = 1 \vee B' = 1$$

čiže daný výrok je tautológia.

Samozrejme, v priebehu výpočtu môžeme využiť aj Vetu 11.7 a prejsť do terminológie teórie množín.

PRÍKLAD. Dokážeme, že $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$ je tautológia. Začneme tak, ako v predchádzajúcom príklade, avšak potom prejdeme do teórie množín, kde využijeme identity $(D \cup E)^c = D^c \cap E^c$, $(D \cap E)^c = D^c \cup E^c$ a $(D^c)^c = D$. Symbolom $\mathcal{U}$ označujeme univerzum, z ktorého sú naše množiny. Na záver prejdeme do Booleovej algebry, kde dôkaz dokončíme. Dostávame

$$(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C)) =$$
$$= \neg(\neg A \vee (\neg B \vee C)) \vee (\neg(\neg A \vee B) \vee (\neg A \vee C)) =$$
$$= (A^c \cup (B^c \cup C))^c \cup ((A^c \cup B)^c \cup (A^c \cup C)) =$$
$$= ((A^c)^c \cap (B^c \cup C)^c) \cup (((A^c)^c \cap B^c) \cup (A^c \cup C)) =$$

$$= (A \cap (B \cap C^c)) \cup ((A \cap B^c) \cup (A^c \cup C)) =$$
$$= (A \cap ((B \cap C^c) \cup B^c)) \cup (A^c \cup C)) = (A \cap (B^c \cup C^c)) \cup (A^c \cup C)) =$$
$$= ((A \cap B^c) \cup (A \cap C^c)) \cup (A^c \cup C) = (A \cap B^c) \cup ((A \cap C^c) \cup (A^c \cup C)) =$$
$$= (A \cap B^c) \cup \mathcal{U} = (A \cap B') \vee 1 = 1$$

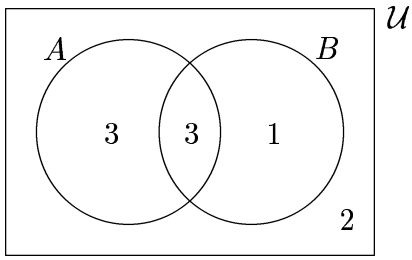
čiže daný výrok je tautológia.

Nuž a keď už prejdeme do terminológie teórie množín, môžeme využiť aj Vennove diagramy.

Príklad. Dokážeme, že $(\neg A \Rightarrow \neg B) \Rightarrow ((\neg A \Rightarrow B) \Rightarrow A)$ je tautológia. Podobne ako v predchádzajúcom príklade dostávame

$$(\neg A \Rightarrow \neg B) \Rightarrow ((\neg A \Rightarrow B) \Rightarrow A) = \neg(\neg(\neg A) \vee \neg B) \vee (\neg(\neg(\neg A) \vee B) \vee A) =$$
$$= ((A^c)^c \cup B^c)^c \cup (((A^c)^c \cup B)^c \cup A) = (A \cup B^c)^c \cup (A \cup B)^c \cup A$$

Získali sme zjednotenie troch množín. Na Obrázku 7 je číslom 1 vyznačená plocha zodpovedajúca prvej množine, číslom 2 plocha zodpovedajúca druhej a číslom 3 plocha tretej. Keďže zjednotením týchto množín je celé univerzum, daný výrok je tautológia.



Obrázok 7

Cvičenia

Cvičenie 11.1. Zostrojte všetky možné Hasseho diagramy zväzov s nanajvýš 6 prvkami.

Cvičenie 11.2. Nech sú $(A_1; \leq_1)$ a $(A_2; \leq_2)$ zväzy. Potom $(A_1 \times A_2; \leq)$, kde $(a_1, a_2) \leq (b_1, b_2)$ práve vtedy, keď $a_1 \leq_1 b_1$ a $a_2 \leq_2 b_2$, je zväz. Dokážte.

Cvičenie 11.3. Zostrojte všetky možné Hasseho diagramy distributívnych zväzov s nanajvýš 6 prvkami.

Cvičenie 11.4. Nech je $(A; |)$ zväz na množine $A = \{1, 2, 3, 5, 6, 15, 30\}$ usporiadaný reláciou deliteľnosti. Je tento zväz distributívny?

Cvičenie 11.5. Dokážte, že zväz $(M; \leq)$, v ktorom pre každé $x, y \in M$ platí buď $x \leq y$ alebo $y \leq x$, je distributívny.

Cvičenie 11.6. Dokážte, že v distributívnom zväze platí nasledujúci vzťah: $(x \wedge y) \vee (y \wedge z) \vee (z \wedge x) = (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$.

Cvičenie 11.7. Ukážte, že vo zväze možno z každého z distributívnych zákonov odvodiť druhý.

Cvičenie 11.8. Nech je $(L; \subseteq)$ zväz všetkých takých podmnožín množiny $\mathbb{N}$, ktorých doplnok (v $\mathbb{N}$) je konečný. Dokážte, že v tomto zväze neexistujú atómy.

Cvičenie 11.9. Pomocou definície komplementu s využitím distributívnych zákonov dokážte, že v Booleovej algebre platí $(x \vee y)' = x' \wedge y'$ a $(x \wedge y)' = x' \vee y'$.

Cvičenie 11.10. Nech sú x, y a z prvky Booleovej algebry. S pomocou definície komplementu a distributívnych zákonov zjednodušte výraz $((x \wedge y) \vee x) \wedge (z' \vee (z \wedge x))$.

Index

Literatúra

[1] Birkhoff, G. – Bartee, T.O.: *Aplikovaná algebra.* Alfa, Bratislava 1981.

[2] Birkhoff, G. – MacLane, S.: *Prehľad modernej algebry.* Alfa, Bratislava 1979.

[3] Katriňák, T. a kol.: *Algebra a teoretická artimetika I.* Alfa, Bratislava 1985.

[4] Kolář, J. – Štěpánková, O. – Chytil, M.: *Logika, algebry a grafy.* SNTL, Praha 1989.

[5] MacLane, S. – Birkhoff, G.: *Algebra.* Alfa, Bratislava 1974.

[6] Olejár, D. – Škoviera, M.: *Úvod do diskrétnej matematiky I.* MFF UK, Bratislava 1992.

[7] Šalát, T. a kol.: *Algebra a teoretická artimetika II.* Alfa, Bratislava 1986.

[8] Winkler, P.: *Random structures and zero-one laws.* Finite and Infinite Combinatorics of Sets and Logic (N. Sauer, R. Woodrow and B. Sands, eds.), NATO Advanced Science Institutes Series, Kluwer Academic Publishers, Kluwer Academic, Dordrecht 1993, pp. 339-420.

Obsah