Verzia: 20. februára 2004

Tento text nie je zamýšľaný ako jediný materiál, ktorý by sám stačil na prípravu na štátnice. Skôr by mal pomôcť pri opakovaní otázok.

Keď je nejaká časť zadania otázky uvedená v zátvorkách, znamená to, že hoci sa pôvodne v otázkach vyskytla, no v poslednej verzii štátnicových otázok už nebola. Do hranatých zátvoriek som naopak dával tie podotázky, ktoré pribudli oproti pôvodnej verzii. V prípade, že niektorú vynechanú časť som už mal napísanú v čase aktualizácie otázok (nové znenie otázok sme dostali na obhajobách), nechal som ju v texte, hoci sa ju netreba učiť. V novej verzii otázok je vynechaná celá 8. a 10. otázka a tiež veľká časť 9.otázky.

Jedinú výnimku predstavuje časť 14., 15. a 18. (a ...) otázky, ktorá bola v zadaní uvedená v zátvorkách. Teda niektoré zátvorky znamenajú skutočné zátvorky.

Určite je tu ešte stále veľa chýb, takže ak sa niekto naučí z týchto otázok tvrdenia, ktoré v skutočnosti neplatia, vopred sa mu ospravedlňujem.

Chcel by som poďakovať Marekovi Hyčkovi a Ondrovi Vacekovi, ktorý opravením mnohých chýb prispeli k výslednej podobe týchto otázok (či skôr odpovedí?).

Poznámky sa momentálne nachádzajú na `thales.doa.fmph.uniba.sk/sleziak/texty`. Sú tam uverejnené aj zdrojáky - takže v prípade, že sa sylaby zmenia máte možnosť si ich upraviť, nejaké časti vynechať alebo naopak pridať. Ak by ste našli v texte chyby, budem rád, keď mi o nich dáte vedieť na `sleziak@fmph.uniba.sk` a pri najbližšej aktualizácii tam už bude opravená verzia.

1 Teória čísel

Základná veta aritmetiky, vlastnosti prvočísel, základné vlastnosti kongruencií. Diofantické rovnice, pytagorovské trojuholníky.

Pri písaní tejto otázky som používal [ATA2] a [KOL].

1.1 Deliteľnosť

Definícia 1. $a \mid b$, $(a \neq 0)$ ak existuje q také, že $b = aq$.

Definícia 2. Prirodzené číslo $p > 1$ sa nazýva *prvočíslom*, ak jedinými jeho kladnými deliteľmi sú čísla 1 a p. Prirodzené číslo $n > 1$ sa nazýva *zložené číslo*, ak n nie je prvočíslo.

Veta 1. *Každé číslo $n > 1$ je súčin prvočísel.*

Lema 1. *Nech b je celé a a prirodzené číslo. Potom existuje jediná taká dvojica čísel q, r, že $b = a.q + r$, $0 \leq r < a$.*

Definícia 3. Číslo d sa nazýva *spoločným deliteľom* čísel a, b, ak $d \mid a$, $d \mid b$. Najväčší prvok množiny spoločných deliteľov čísel a a b je *najväčší spoločný deliteľ a, b*, značíme (a, b). Ak $(a, b) = 1$, tak čísla a, b nazývame *nesúdeliteľnými*.

Lema 2. *Ak sa čísla a, b nerovnajú súčasne nule, tak existujú také čísla x_0, y_0, že $(a, b) = ax_0 + by_0$.*

O nasledujúcej leme prof. Šalát hovoril, že sa tiež zvykne volať základná veta aritmetiky.

Lema 3. *Ak $a \mid b.c$, $(a, b) = 1$, tak $a \mid c$.*

Lema 4. *Nech p je prvočíslo a $p \mid a.b$. Potom buď $p \mid a$, alebo $p \mid b$.*

Veta 2. *Každé číslo $n > 1$ má práve jeden kanonický rozklad.*

Definícia 4. *Najmenší spoločný násobok* $[a, b]$

Veta 3. *Pre ľubovoľné dve prirodzené čísla* a, b *platí* $[a, b] = \frac{a.b}{(a,b)}$.

1.2 Vlastnosti prvočísel

Veta 4 (Euklides). *Všetkých prvočísel je nekonečne mnoho.*

Definícia 5. $\pi(x)$ je počet prvočísel p, ktoré spĺňajú $p \leq x$ (nepresahujú x). Funkciu π nazývame *prvočíselná funkcia.*

Tvrdenie 1. $\pi(x) \geq \frac{\log x}{2 \log 2}$

Veta 5 (Prvočíselná veta).

$$\lim_{x \to \infty} \frac{\pi(x)}{\left(\frac{x}{\ln x}\right)} = 1$$

Dôkaz prvočíselnej vety je veľmi ťažký, táto veta patrí medzi najvýznamnejšie výsledky teórie čísel.

Veta 6. *Nekonečný rad* $\sum_{k=1}^{\infty} \frac{1}{p_k}$ *prevrátených hodnôt všetkých prvočísel diverguje.*

Definícia 6. Nech $A \subseteq \mathbb{N}$, $x \in \mathbb{N}$. Označme znakom $A(x)$ počet všetkých tých $a \in A$, pre ktoré $a \leq x$. Ak existuje $\lim_{x \to \infty} \frac{A(x)}{x}$, nazývame toto číslo *asymptotickou hustotou* množiny A a označujeme ho $h(A)$.

Veta 7. $h(P) = 0$

Dôsledok 1. $h(\mathbb{N} \setminus P) = 1$

1.3 Kongruencie

Definícia 7. $a \equiv b \,(mod\ m) \Leftrightarrow m \mid (a - b)$
Hovoríme, že a a b sú kongruentné a zápis $a \equiv b \,(mod\ m)$ nazývame *kongruenciou.*

Relácia $\equiv$ je očividne reláciou ekvivalencie.

Veta 8.

(i) Ak $a \equiv b \,(mod\ m)$ *a* $c \equiv d \,(mod\ m)$, *tak*

- *(a)* $a + c \equiv b + d \,(mod\ m)$,
- *(b)* $a - c \equiv b - d \,(mod\ m)$,
- *(c)* $ac \equiv bc \,(mod\ m)$.

(ii) Ak $ac \equiv bc \,(mod\ m)$ *a* $(c, m) = 1$, *tak* $a \equiv b \,(mod\ m)$.

Veta 9. *Množina všetkých zvyškových tried pri definovanom sčítaní tvorí Abelovu grupu. Jednotkou operácie sčítania je trieda* $\overline{0} \,(mod\ m)$.

Lema 5. *Nech* $(a, m) = 1$, c *je ľubovoľné číslo. Potom existuje jediná zvyšková trieda* $(mod\ m)$, *že pre každý jej prvok* x *platí* $ax \equiv c \,(mod\ m)$.

Definícia 8. Nech $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ je polynóm n-tého rádu s celočíselnými koeficientami. Výrokovú funkciu $f(x) \equiv 0\,(mod\ m)$ nazývame *kongruenciou n-tého stupňa* s celočíselnými koeficientmi.

Lema 6. *Nech* $x_1 \equiv x_0\,(mod\ m)$. *Potom platí* $f(x_1) \equiv f(x_0)\,(mod\ m)$.

Definícia 9. Zvyškovú triedu $(mod\ m)$ nazveme *redukovanou zvyškovou triedou* $(mod\ m)$, ak každý jej prvok je nesúdeliteľný s číslom m.

Veta 10. *Množina všetkých redukovaných zvyškových tried* $(mod\ m)$ *pri zavedenom násobení tvorí grupu. Jednotka operácie je trieda* $\overline{1}$.

Definícia 10. Pre $m \geq 1$ nech $\varphi(m)$ označuje počet čísel postupnosti $1, 2, \ldots, m-1, m$ nesúdeliteľných s m. Funkcia φ sa nazýva *Eulerova funkcia*.

Tvrdenie 2. $\varphi(1) = 1$, $\varphi(p) = p - 1$

Lema 7. *Nech* $(a, m) = 1$, $k = \varphi(m)$. *Ak* $\{r_1, r_2, \ldots, r_k\}$ *je redukovaný zvyškový systém* $(mod\ m)$, *tak aj* $\{ar_1, ar_2, \ldots, ar_k\}$ *je redukovaný zvyškový systém* $(mod\ m)$. *(redukovaný zvyškový systém = z každej redukovanej zvyškovej triedy vezmeme jedného reprezentanta)*

Veta 11 (Eulerova). *Nech* $(a, m) = 1$. *Potom platí* $a^{\varphi(m)} \equiv 1\,(mod\ m)$

Pre $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ platí

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\ldots\left(1 - \frac{1}{p_k}\right)$$

1.4 Lineárne diofantické rovnice

Všeobecný tvar lineárnej diofantickej rovnice je

$$a_1x_1 + a_2x_2 + \ldots + a_kx_k = c \tag{1.1}$$

kde a_j a c sú dané celé čísla, neznáme sú x_i.

Označme $d = (a_1, a_2, \ldots, a_k)$.

Veta 12. *Rovnica* (1.1) *má riešenie v celých číslach vtedy a len vtedy, keď* $d \mid c$.

Uvažujme rovnicu s dvoma neznámymi:

$$ax + by = c \tag{1.2}$$

Veta 13. *Ak* $d \mid c$, *tak existujú také* $x_0, y_0 \in \mathbb{Z}$, *že* $ax_0 + by_0 = c$ *a všetky riešenia rovnice* (1.2) *v celých číslach sú dané parametrickými rovnosťami*

$$x = x_0 + \frac{b}{d}t, \qquad y = y_0 - \frac{a}{d}t \qquad (t \in \mathbb{Z}).$$

1.5 Pytagorovské trojuholníky

Pytagorovské trojuholníky sú pravouhlé trojuholníky s celočíselnými dĺžkami strán.

$PT(x, y, z) \Leftrightarrow x^2 + y^2 = z^2$.

Všetky pytagorovské trojuholníky možno rozdeliť do tried na základe podobnosti. Primitívny pytagorovský trojuholník je taký, ktorý má spomedzi podobných pytagorovských trojuholníkov najmenší obsah. Pytagorovský trojuholník x, y, z je primitívny $\Leftrightarrow (x, y) = 1$ $\Leftrightarrow (x, z) = 1 \Leftrightarrow (y, z) = 1$.

Lema 8. *Ak x, y, z je primitívny pytagorovský trojuholník, tak jedno z čísel x, y je párne a druhé nepárne.*

Veta 14. *Ak $PT(x, y, z)$ je primitívny pytagorovský trojuholník, tak existujú $m, n \in \mathbb{N}$, $m > n$, $(m, n) = 1$ opačnej parity také, že $x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$. Platí to aj obrátene.*

Veta 15. *Ak $PT(x, y, z)$ je primitívny pytagorovský trojuholník existujú také $k, l \in \mathbb{N}$, $k > l$, $(k, l) = 1$, obe nepárne, že $x = kl$, $y = \frac{k^2 - l^2}{2}$, $z = \frac{k^2 + l^2}{2}$. Platí to aj obrátene.*

Veta 16. *Existuje nekonečne veľa primitívnych pytagorovských trojuholníkov, ktorých prepona je kvadrátom prirodzeného čísla.*

Veta 17. *Existuje nekonečne veľa primitívnych pytagorovských trojuholníkov, v ktorých jedna odvesna je kvadrátom prirodzeného čísla.*

Veta 18 (Fermat). *Neexistuje pytagorovský trojuholník, ktorého dĺžky dvoch strán by boli kvadráty.*

Veta 19. *$x^n + y^n = z^{n-1}$ má nekonečne veľa riešení.*

1.6 Multiplikatívne funkcie

Definícia 11. Funkcia $f : \mathbb{N} \to \mathbb{C}$ sa nazýva *aritmetická funkcia.* Aritmetická funkcia f sa nazýva *multiplikatívna,* ak sa nerovná identicky nule, a ak z podmienky $a, b \in \mathbb{N}$, $(a, b) = 1$ vyplýva

$$f(a.b) = f(a).f(b)$$

Aritmetická funkcia f sa nazýva *úplne multiplikatívna*, ak táto rovnosť platí pre ľubovoľné $a, b \in \mathbb{N}$.

Tvrdenie 3. *Ak f je multiplikatívna funkcia, tak $f(1) = 1$.*
Ak f a g sú multiplikatívne funkcie, tak aj $f.g$ je multiplikatívna funkcia.

Veta 20. *Nech $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ je kanonický rozklad čísla $a \in \mathbb{N}$ a nech f je multiplikatívna funkcia. Potom platí*

$$\sum_{d|a} f(d) = (1 + f(p_1) + \dots + f(p_1^{\alpha_1})) \dots (1 + f(p_k) + \dots + f(p_k^{\alpha_k}))$$

$\tau(n)$=počet deliteľov čísla n
$\sigma(n)$=súčet deliteľov čísla n
Funkcie τ, σ a φ sú multiplikatívne.
Funkcia n^s je úplne multiplikatívna funkcia.

$$\sigma(a) = \frac{p_1^{\alpha_1+1}}{p_1 - 1} \dots \frac{p_k^{\alpha_k+1}}{p_k - 1}$$
$$\tau(a) = (\alpha_1 + 1) \dots (\alpha_k + 1)$$

Tvrdenie 4. *Pre každé $n > 1$ platí $\sigma(n) \geq n + 1$.*

Dôsledok 2. $\lim_{n \to \infty} \sigma(n) = +\infty$

Tvrdenie 5. $\liminf_{n\to\infty} \tau(n) = 2$ *a* $\limsup_{n\to\infty} \tau(n) = +\infty$

Každé prirodzené číslo $k \geq 2$ je hromadnou hodnotou postupnosti $(\tau(n))_{n=1}^{\infty}$. ($\tau(p^k) = k+1$)

Tvrdenie 6. *Pre každé* $\eta > 0$ *je* $\lim_{n\to\infty} \frac{\tau(n)}{n^\eta} = 0$.

Tvrdenie 7. $\sum_{d|n} \varphi(d) = n$

Tvrdenie 8. $\lim_{n\to\infty} \varphi(n) = +\infty$

Definícia 12. *Möbiusova funkcia* $\mu(1) = 1$, $\mu(a) = 0$, ak existuje prvočíslo p také, že $p^2 \mid a$ a $\mu(a) = (-1)^k$, ak $a = p_1 \dots p_k$ (prvočísla p_i sú navzájom rôzne).

Veta 21. *Nech* f *je multiplikatívna funkcia a nech* $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ *je kanonický rozklad čísla* $a \in \mathbb{N}$. *Potom platí*

$$\sum_{d|a} \mu(d) f(d) = (1 - f(p_1)) \dots (1 - f(p_k))$$

Pri voľbe $f(n) = 1$, resp. $f(n) = \frac{1}{n}$ dostaneme z predchádzajúcej vety:

Dôsledok 3.

$$\sum_{d|1} \mu(d) = 1, \ \sum_{d|a} \mu(d) = 0 \ (a > 1)$$

$$\sum_{d|1} \frac{\mu(d)}{d} = 1, \ \sum_{d|a} \frac{\mu(d)}{d} = \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right)$$

$$\varphi(a) = a \sum_{d|a} \frac{\mu(d)}{d}$$

Definícia 13. Číslo $n \in \mathbb{N}$ sa nazýva *dokonalé,* ak $\sigma(n) = 2n$. (Ekvivalentne: n sa rovná súčtu svojich vlastných deliteľov.)

Veta 22. *Párne číslo* $n \in \mathbb{N}$ *je dokonalé práve vtedy, keď má tvar* $a = 2^{p-1}(2^p - 1)$, *kde* p *je prvočíslo a* $M_p = 2^p - 1$ *je tiež prvočíslo.*

Nie je známe, či existuje dokonalé nepárne číslo, ani či je dokonalých čísel nekonečne veľa.

1.7 Cantorove rozvoje reálnych čísel

Veta 23. *Nech* $(q_k)_{k=1}^{\infty}$ *je postupnosť prirodzených čísel väčších ako 1. Potom každé reálne číslo* x *možno jednoznačne vyjadriť v tvare*

$$x = c_0 + \sum_{k=1}^{\infty} \frac{c_k}{q_1 . q_2 \dots q_k}, \tag{1.3}$$

kde c_k $(k = 0, 1, \dots)$ *sú celé čísla,* $0 \leq c_k < q_k$ $(k = 1, 2, \dots)$ *a pre nekonečne mnoho* k *platí* $c_k < q_k - 1$.

Tento rozvoj voláme *Cantorovým rozvojom* čísla x. Špeciálnymi prípadmi sú g-adické a faktoriálové rozvoje.

Veta 24. *Nech $(q_k)_{k=1}^{\infty}$ má rovnaký význam ako v predchádzajúcej vete. Nech ku každému prvočíslu p existuje nekonečne veľa takých k, že $p \mid q_k$. Potom číslo x vyjadrené Cantorovým rozvojom (1.3) je iracionálne vtedy a len vtedy, keď pre nekonečne mnoho k platí $c_k \neq 0$.*

To znamená, že ak základná postupnosť $(q_k)_{k=1}^{\infty}$ spĺňa predpoklady tejto vety, tak x je racionálne práve vtedy, keď Cantorov rozvoj je konečný.

Veta 25. *Čísla $x_1 = \sum_{n=1}^{\infty} \frac{\tau(n)}{n!}$ a $x_2 = \sum_{n=1}^{\infty} \frac{\varphi(n)}{n!}$ sú iracionálne.*

Veta 26. *Číslo x vyjadrené g-adickým rozvojom je racionálne vtedy a len vtedy, keď je tento rozvoj periodický.*

Veta 27. *Nech $n \in \mathbb{N}$, $n \geq 2$. Nech a je prirodzené číslo a $a \neq k^n$ pre žiadne prirodzené číslo k. Potom $\sqrt[n]{a}$ je iracionálne číslo.*

Veta 28. *Nech r je kladné racionálne číslo a $r \neq 10^n$ pre žiadne $n \in \mathbb{Z}$. Potom číslo $\log_{10} r$ je iracionálne.*

Teória čísel je užitočná na to, aby sa pomocou nej dalo promovať.
Landau

2 Moduly

Pojem modulu a základné vlastnosti. Voľné moduly, základná veta o tvare konečne generovaného modulu. Kanonické tvary matíc, podobné matice. Charakteristický a minimálny polynóm matice, elementárne delitele a invariantné faktory matíc.

2.1 Okruhy, ideály, okruhy s jednoznačným rozkladom

Nejaké úvodné veci, z [ATA].

Faktorové okruhy a ideály

Definícia 1. Neprázdnu podmnožinu I okruhu A nazývame *ideálom* okruhu A, ak

(i) $x, y \in I \Rightarrow x - y \in I$,

(ii) $x \in I, a \in A \Rightarrow ax \in I, xa \in I$.

I je *vlastný ideál,* ak $I \neq A$.

Veta 1. *Ak I je ideál okruhu A, tak množina A/I všetkých tried aditívnej grupy A podľa podgrupy I s operáciami*

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

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

tvorí okruh. Tento okruh nazývame faktorový okruh *A podľa I. Ak A je komutatívny, resp. obsahuje jednotku, tak aj A/I je komutatívny, resp. obsahuje jednotku.*

Definícia 2. Ideál I okruhu A nazývame *prvoideál*, ak

$$\forall a, b \in A : ab \in I \Rightarrow a \in I \vee b \in I.$$

Ideál I okruhu A nazývame *maximálny*, ak $I \neq A$ a ak pre každý ideál J $I \subset J \subset A$ implikuje $J = I$ alebo $J = A$.

Každý maximálny ideál je prvoideál.

Veta 2. *Faktorový okruh A/I komutatívneho okruhu A s jednotkou je poľom práve vtedy, keď I je maximálny ideál.*

Faktorový okruh A/I komutatívneho okruhu A s jednotkou je oborom integrity práve vtedy, keď I je vlastný prvoideál.

Definícia 3. Hovoríme, že prvok $x \in A$ generuje ideál I komutatívneho okruhu A s jednotkou, ak $I = xA = \{xa; a \in A\}$.

Ideál I okruhu A nazývame *hlavným ideálom,* ak je generovaný niektorým prvkom $x \in A$.

Komutatívny okruh A nazývame *okruh hlavných ideálov*, ak každý ideál okruhu A je hlavný.

Veta 3. *V okruhu hlavných ideálov je každý prvoideál maximálny.*

Okruhy s jednoznačným rozkladom

Obor integrity (OI) = komutatívny okruh s jednotkou bez deliteľov nuly.

Euklidovský okruh = taký obor integrity A, v ktorom existuje zobrazenie $\delta\colon A \setminus \{0\} \to \mathbb{Z}$ také, že platí:
a) $\delta(a) \geq 0$ pre každé $a \in A$.
b) Pre každé $a, b \in A$, $b \neq 0$ existujú prvky $q, r \in A$ tak, že $a = bq + r$, pričom alebo $r = 0$, alebo $r \neq 0$ a $\delta(r) < \delta(b)$.

Okruh s jednoznačným rozkladom (Gaussov okruh), je obor integrity, v ktorom sa každý prvok dá zapísať v tvare $a = up_1p_2 \dots p_n$, kde $a \in U(A)$ (delitele jednotky v OI A) a p_i sú ireducibilné prvky v A, pričom tento zápis je jednoznačný až na poradie a asociovanosť.

Euklidovské okruhy

V euklidovskom okruhu existuje najväčší spoločný deliteľ dvoch prvkov.

Euklidovský okruh je okruhom hlavných ideálov.

Okruhy hlavných ideálov

V okruhu hlavných ideálov platí
a) $a \mid b \Leftrightarrow (a) \supset (b)$
b) $a \sim b \Leftrightarrow (a) = (b)$
Ak $a, b \in A$, A je OHI, tak
a) $(a) + (b) = \{x \in A; x = au + bx, u, v \in A\}$ je ideálom v okruhu A,
b) existuje $d \in A$ s vlastnosťou $(d) = (a) + (b)$ a platí $d = (a, b)$.

Veta 4. *Nech A je OHI. Potom A je okruhom s jednoznačným rozkladom práve vtedy, keď A je obor integrity.*

Vo zvyšku otázky budeme pod OHI rozumieť OI, ktorý je OHI. (Takto to používal Guričan. V [ATA] je to definované tak, ako som to dal sem.)

Gaussove okruhy

Nech A je okruh s jednoznačným rozkladom. Nech $a = up_1p_2 \dots p_n$, $b = vq_1q_2 \dots q_r$ sú dva kanonické rozklady prvkov $a, b \in A$. Potom $a \mid b$ práve vtedy, keď existuje injektívne zobrazenie $\varphi\colon \{1 \dots k\} \to \{1 \dots k\}$ tak, že $p_i \sim q_{i\varphi}$ pre všetky $i = 1, \dots, k$.

2.2 Smithov kanonický tvar

Matice nad euklidovským okruhom nazývame riadkovo ekvivalentné/ stĺpcovo ekvivalentné/ ekvivalentné, ak sa jedna dá upraviť na druhú konečnou postupnosťou riadkových/ stĺpcových/ ľubovoľných úprav.

Veta 5. *Nech A je matica typu $m \times n$ nad euklidovským okruhom R. Potom existuje diagonálna matica $D = \operatorname{diag}(d_1, d_2, \dots)$ ekvivalentná s A a taká, že platí:*

$$d_i \mid d_j \text{ pre prípustné } i, j \text{ také, že } i \leq j.$$

Matica D je jednoznačne určená až na asociovanosť.

Determinanty podmatíc matice A typu $r \times r$ nazývame *minory* A rádu r. Najväčší spoločný deliteľ minorov A rádu r označíme $\eta_r(A)$. Potom platí $d_1 \dots d_r \doteq \eta_r(A)$. Prvky na diagonále Smithovho kanonického tvaru matice A nazývame *invariantnými faktormi* matice A.

Veta o Smithovom kanonickom tvare platí aj ak R je obor integrity a okruh hlavných ideálov. (Vo zvyšku otázky vždy budeme pod okruhom hlavných ideálov rozumieť obor integrity.) Potrebujeme však všeobecnejšiu definíciu ekvivalencie matíc. Matice A a B typu $m \times n$ nazveme ekvivalentnými, ak existujú štvorcové matice P a Q, ktoré sú delitele jednotky v príslušných okruhoch matíc a platí $A = PBQ$.

2.3 Pojem modulu a základné vlastnosti

Definícia 4. Nech R je okruh a $(M, +)$ je komutatívna grupa. Potom dvojicu (R, M) spolu s „binárnym párovaním“ $\odot\colon R \times M \to M$ nazývame *ľavostranným modulom* nad okruhom R, ak

(i) pre $a \in R$ a $x, y \in M$ platí $a \odot (x + y) = (a \odot x) + (a \odot y)$

(ii) pre $a, b \in R$ a $x \in M$ platí $(a + b) \odot x = (a \odot x) + (b \odot x)$

(iii) pre $a \in R$ a $x, y \in M$ platí $a \odot (b \odot x) = (ab) \odot x$

$\odot$ sa zvyčajne nazýva *skalárny súčin (skalárne násobenie).*

Ak navyše R je komutatívny okruh s jednotkou a platí

$$\text{pre } x \in M \ 1 \odot x = x,$$

tak ide o *unitárny* modul. My sa zaoberáme len unitárnymi modulmi.

Príkladmi modulov sú vektorové priestory, každá grupa je $\mathbb{Z}$-modul, ak I je ideál okruhu R, tak (R, I) je R-modul. Ak $V(F)$ je konečnorozmerný vektorový priestor nad poľom F a A je jeho lineárna transformácia, tak definujeme unitárny modul $(F[\gamma], V(F), A)$, kde $f(\gamma) \odot x = xf(A)$.

Definícia 5. Nech (R, M) je modul. Nech K je podgrupa grupy $(M, +)$. Potom (R, K) nazývame podmodulom modulu (R, M), ak pre $a \in R$ a $x \in K$ je vždy $ax \in K$.

Nech (R, M), (R, K) sú dva moduly nad R. Nech $\varphi\colon M \to K$ je grupový homomorfizmus. Potom hovoríme, že φ je *modulový homomorfizmus*, ak naviac pre každé $a \in R$ a $x \in M$ platí $(ax)\varphi = a(x\varphi)$.

Definícia 6. Nech $\emptyset \neq X \subseteq M$, kde (R, M) je modul. Nech $[X]$ značí množinový prienik všetkých podmodulov modulu (R, M) obsahujúcich množinu X. $[X]$ je tiež podmodul modulu (R, M). Nazývame ho podmodul *generovaný* množinou X. Prvky z množiny X sa nazývajú *generátormi* (pod)modulu $[X]$. Ak pre nejakú konečnú podmnožinu $X \subseteq M$ je $[X] = M$, hovoríme, že (R, M) je *konečne generovaný* modul.

Tvrdenie 1. *Nech (R, M) je unitárny modul. Potom (R, K) je podmodul modulu (R, M) práve vtedy, keď $a, b \in R$ a $x, y \in K$ implikuje $ax + by \in K$.*

Tvrdenie 2. *Nech (R, K) je modul nad komutatívnym okruhom R. Potom*

$$\begin{aligned}[X] =&\{z \in K; z = n_1x_1 + \ldots + n_rx_r + a_1y_1 + \ldots + a_sy_s \wedge r, s \in \mathbb{N} \wedge \\ &\wedge n_1, \ldots, n_r \in \mathbb{Z} \wedge a_1, \ldots, a_s \in R \wedge x_1, \ldots, x_r, y_1, \ldots, y_s \in X\}.\end{aligned}$$

Ak (R, K) je unitárny modul, tak

$$[X] = \{z \in K; z = a_1y_1 + \ldots + a_sy_s \wedge s \in \mathbb{N} \ \wedge a_1, \ldots, a_s \in R \wedge y_1, \ldots, y_s \in X\}.$$

Relácia ekvivalencie Θ na M sa nazýva *kongruenciou* modulu (R, M), ak Θ je kongruenciou na grupe M a $x \cong y(\Theta)$ implikuje $ax \cong ay(\Theta)$. Podobne ako pri grupách sa dá definovať faktorový modul podľa danej kongruencie.

2.4 Voľné moduly

Definícia 7. Unitárny modul (R, M) nazývame *voľným modulom* nad množinou voľných generátorov S, ak

(i) $[S] = (R, M)$ a

(ii) ak $a_1x_1 + \ldots a_nx_n = 0$ pre $a_i \in R$ a po dvoch rôzne $x_1, \ldots, x_n \in S$, tak $a_1 = a_2 = \ldots = a_n = 0$.

V takomto prípade budeme pre (R, M) používať tiež označenie $F_R(S)$. Množinu voľných generátorov S tiež nazývame bázou voľného modulu $F_R(S)$. $F_R(n)$ znamená voľný modul s n-prvkovou bázou.

Veta 6. *Nech (R, M) je unitárny modul. Potom (R, M) je voľný modul práve vtedy, ak*

(i) $[S] = (R, M)$,

(ii) každé zobrazenie $f\colon S \to K$ do (ľubovoľného) unitárneho modulu (R, K) sa dá jediným spôsobom rozšíriť na homomorfizmus $\varphi\colon M \to K$, t.j. $\varphi|S = f$.

Definícia 8. Nech $\{(R, M_i); i \in I\}$ je množina modulov. Potom

$$\prod(M_i : i \in I) = \{f\colon I \to \bigcup(M_i : i \in I); f(i) \in M_i, i \in I\}$$

je tzv. *karteziánsky súčin* množín M_i, $i \in I$. Na tejto množine definujeme operácie $\oplus$ a $\odot$ po zložkách. Dostaneme tak modul - *priamy súčin* modulov M_i.

Veta 7. *Modul (R, M) je izomorfný s priamym súčinom n modulov nad R práve vtedy, keď existujú podmoduly P_i modulu (R, M) tak, že platí:*

(i) $M = [P_1 \cup \ldots \cup P_n]$ *a*

(ii) $\{0\} = P_i \cap [P_1 \cup \ldots \cup P_{i-1}]$ *pre všetky* $i = 2, \ldots n$.

Ak sú splnené uvedené dve podmienky, tak $(R, M) \cong (R, P_1 \times P_2 \times \ldots \times P_n)$

Priamy súčin modulov $(R, M_1 \times \ldots \times M_n)$ značíme tiež $M_1 \oplus \ldots \oplus M_n$.

Veta 8. *Nech R je okruh, (R, M) je unitárny modul a $M = [e_1, \ldots, e_n]$. Potom $M = [e_1] \oplus \ldots \oplus [e_n]$ práve vtedy, keď z rovnice $a_1e_1 + \ldots + a_ne_n = 0$ vyplýva, že $a_1e_1 = \ldots = a_ne_n = 0$.*

Veta 9. *Nech R je okruh s 1. Potom unitárny modul $(R, R_1 \times \ldots \times R_n)$, $n \geq 1$ kde $R_1 = \ldots = R_n = R$ je voľný modul nad n-prvkovou množinou voľných generátorov $S = \{e_1, \ldots, e_n\}$, kde $e_1 = (1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1)$.*

Veta 10. *Nech R je OHI. Potom každý podmodul voľného modulu $F_R(n)$ je voľný modul s konečnou bázou o $m \leq n$ prvkoch (t.j. existuje báza, ktorá má najviac n prvkov).*

Veta 11. *Nech R je obor integrity s 1, nech (R, M) je konečnogenerovaný voľný modul, nech $\alpha_1, \ldots, \alpha_n$ a $\beta_1, \ldots, \beta_m$ sú dve bázy tohoto modulu. Potom $m = n$.*

Definícia 9. Nech (R, M_i), $i \in I$ sú unitárne moduly. Potom priamy súčin týchto modulov $K = \prod(M_i; i \in I)$ je tiež unitárny modul. Podmnožina $L = \{f \in K; f(i) = 0$ pre skoro všetky (t.j. všetky až na konečný počet) $i \in I\}$ tvorí podmodul modulu (R, K). Modul L nazývame *priamy súčet* modulov (R, M_i), $i \in I$ a značíme ho $\sum(M_i; i \in I)$.

2.5 Veta o rozklade modulov

Definícia 10. Nech (R, M) je modul, R je okruh hlavných ideálov. Ak $a \in M$, tak generátor (hlavného) ideálu $\{r \in R; ra = 0\}$ sa nazýva *rád prvku* a, značíme $\mathrm{rad}(a)$.

Veta 12. *Nech (R, M) je konečne generovaný unitárny modul nad okruhom hlavných ideálov R. Potom existuje rozklad na cyklické podmoduly $M = [f_1] \oplus [f_2] \oplus \ldots \oplus [f_k]$, kde* $\mathrm{rad}(f_i) \mid \mathrm{rad}(f_j)$ *pre* $1 \leq i \leq j \leq k$. *Ďalej ak* $\mathrm{rad}(f_1) \nmid 1$, *tak tento rozklad je jednoznačný, presnejšie povedané, ak $M = [f'_1] \oplus [f'_2] \oplus \ldots \oplus [f'_s]$ a je splnené, že* $\mathrm{rad}(f'_1) \nmid 1$ *a tiež* $\mathrm{rad}(f'_i) \mid \mathrm{rad}(f'_j)$ *pre* $1 \leq i \leq j \leq k$, *tak $k = s$ a* $\mathrm{rad}(f_i) \doteq \mathrm{rad}(f'_i)$.

Dôsledok 1. *Nech (R, M) je konečne generovaný unitárny modul nad okruhom hlavných ideálov. Potom $M = M_1 \oplus F$, kde M_1 je podmodul prvkov konečného rádu a F je voľný modul nad R.*

Dimenzia voľného modulu F je určená jednoznačne a nazýva sa Bettiho číslo *modulu (R, M).*

Dôsledok 2. *Konečne generovaná komutatívna grupa je priamy súčin komutatívnej periodickej a voľnej komutatívnej grupy.*

Dôsledok 3. *Konečne generovaná komutatívna grupa je priamy súčin cyklických grúp.*

2.6 Jordanov kanonický tvar

Dve matice A, B typu $n \times n$ nad poľom F sú *podobné,* ak existuje regulárna matica P taká, že $B = PAP^{-1}$, alebo, ekvivalentne, ak sú matice A, B maticami toho istého lineárneho zobrazenia daného vektorového priestoru pri dvoch bázach.

Modul prislúchajúci matici A možno podľa vety o rozklade modulov rozložiť na cyklické podmoduly. O nich platí:

Lema 1. *Každý cyklický podmodul M_i je podpriestor vektorového priestoru $V(F)$, ktorý je invariantný vzhľadom na lineárne zobrazenie A.*

Z toho vyplýva, že matica A je podobná blokovo diagonálnej matici, kde bloky zodpovedajú podpriestorom M_i.

Definícia 11. *Minimálny polynóm* $m_{A,\alpha}(\gamma)$ transformácie (matice) A v bode α je normovaný polynóm, ktorý generuje ideál $M_{A,\alpha} = \{f \in F[\gamma]; \alpha f(A) = 0\}$. ($m_{A,\alpha}(\gamma) \doteq \mathrm{rad}(\alpha)$)

Minimálny polynóm $m_{A,S}(\gamma)$ transformácie (matice) A na podpriestore S je normovaný polynóm, ktorý generuje ideál $M_{A,S} = \{f \in F[\gamma]; (\forall \alpha \in S)\alpha f(A) = 0\} = \bigcap\limits_{\alpha \in S} M_{A,\alpha}$.

Minimálny polynóm $m_{A,V_n}(\gamma)$ transformácie (matice) A (na priestore $V_n(F)$) je normovaný polynóm, ktorý generuje ideál $M_{A,V_n} = \{f \in F[\gamma]; (\forall \alpha \in V_n)\alpha f(A) = 0\} = \bigcap\limits_{\alpha \in V_n} M_{A,\alpha}$.

$M_i = [g_i]$ má bázu $g_i, g_i A, \ldots g_i A^{st(d_i)-1}$, kde $d_i = \mathrm{rad}(g_i) = M_{A,g_i}(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0$. Transformácia A zúžená na podpriestor M_i má pri tejto báze maticu

$$\begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \ldots & 1 \\ -a_0 & -a_1 & & \ldots & -a_{m-1} \end{pmatrix}$$

Maticu, ktorá pozostáva z takýchto blokov na diagonále je *Jordanov kanonický tvar matice A prvého druhu.*

Ak $(F[\gamma], V(F), A) = [g_1] \oplus \ldots \oplus [g_k]$, tak polynómy $\mathrm{rad}(g_1), \ldots, \mathrm{rad}(g_k)$ ($= m_{A,g_1}(\gamma), \ldots, m_{A,g_k}(\gamma)$) nazývame *invariantné faktory* matice A. Sú to diagonálne prvky Smithovho kanonického tvaru matice $\gamma I - A$.

Nech $M = (F[\gamma], V(F), A) = [g]$ a nech $\mathrm{rad}(g) = m_1(\gamma)m_2(\gamma)\ldots m_n(\gamma)$, pričom m_i sú po dvoch nesúdeliteľné. Položme $\hat{m}_i(\gamma) = \frac{\mathrm{rad}(g)}{m_i(\gamma)}$. Platí

Veta 13. *Existujú $e_1 \ldots e_l$ také, že $M = [g] = [e_1] \oplus \ldots \oplus [e_l]$ a $\mathrm{rad}(e_i) = m_i$.*

(Prvky e_i sa nájdu ako $e_i = \hat{m}_i(\gamma)g$)

Táto veta umožňuje rozložiť jednotlivé bloky Jordanovej kanonickej matice prvého druhu nasledovným spôsobom: Nech blok C_i je pridružený ku polynómu (invariantnému faktoru matice A) $d_i(\gamma) = p_{i1}^{k_{i1}} \ldots p_{is_i}^{k_{is_i}}$, kde jednotlivé polynómy sú ireducibilné normované a po dvoch nesúdeliteľné. Potom na základe predošlej vety vieme ešte blok C_i rozložiť na blokovo diagonálnu maticu $diag(B_{i1}, \ldots, B_{is_i})$, kde každé B_{ij} je matica pridružená k polynómu $P_{ij}^{k_{ij}}(\gamma)$. Tieto polynómy sa nazývajú *elementárne delitele* matice A.

Ak uvažujeme o module $M = (F[\gamma], [g], A)$, pričom $\mathrm{rad}(g) = p^k(\gamma)$, kde $p(\gamma)$ je ireducibilný polynóm. Potom vektory

$$\begin{vmatrix} g_1 = g & g_2 = gA & \dots & g_p = gA^{q-1} \\ g_{q+1} = gp(A) & g_{q+2} = gp(A)A & \dots & g_{q+p} = gp(A)A^{q-1} \\ g_{2q+1} = gp^2(A) & g_{2q+2} = gp^2(A)A & \dots & g_{2q+p} = gp^2(A)A^{q-1} \\ \vdots & \vdots & & \vdots \\ g_{(k-1)q+1} = gp^{k-1}(A) & g_{(k-1)q+2} = gp^{k-1}(A)A & \dots & g_{(k-1)q+q} = gp^{k-1}(A)A^{q-1} \end{vmatrix}$$

tvoria bázu. Vzhľadom na túto bázu dostaneme vyjadrenie A v tvare

$$B = \begin{pmatrix} P & N & 0 & \dots & 0 & 0 \\ 0 & P & N & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & P & N \\ 0 & 0 & 0 & \dots & 0 & P \end{pmatrix}$$

kde

$$P = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ -c_0 & -c_1 & -c_2 & \dots & -c_{q-2} & -c_{q-1} \end{pmatrix}$$

a

$$N = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 \end{pmatrix}$$

Dostali sme *Jordanov kanonický tvar matice A druhého druhu.*

Nad algebraicky uzavretým poľom F sú ireducibilné normované polynómy v tvare $x - a$. V tom prípade dostaneme

$$J_{(x-a)^k} = \begin{pmatrix} a & 1 & 0 & \dots & 0 & 0 \\ 0 & a & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a & 1 \\ 0 & 0 & 0 & \dots & 0 & a \end{pmatrix}$$

Veta 14. *Nech A, B sú matice $n \times n$ nad poľom F. Nasledujúce podmienky sú ekvivalentné:*

(i) A a B sú podobné,

(ii) $\gamma I - A$ a $\gamma I - B$ sú ekvivalentné nad $F[\gamma]$ (t.j. majú „rovnaký“ Smithov kanonický tvar),

(iii) A a B majú rovnaké invariantné faktory,

(iv) A a B majú rovnaké systémy elementárnych deliteľov.

Veta 15. *Nech A je matica nad poľom F. Nasledujúce podmienky sú ekvivalentné:*

(i) A je podobná diagonálnej matici,

(ii) elementárne delitele matice A sú polynómy prvého stupňa,

(iii) posledný invariantný faktor má samé jednoduché korene a tie ležia všetky v poli F.

Definícia 12. *Charakteristický polynóm* matice A je polynóm $\det(xI - A)$. *Minimálny polynóm* matice A je nenulový polynóm p najnižšieho možného stupňa taký, že $p(A) = 0$.

Veta 16. *Charakteristický polynóm matice A je súčin jej invariantných faktorov (a teda aj všetkých elementárnych deliteľov).*

Veta 17. *Minimálny polynóm matice A je jej posledný invariantný faktor.*

Dôsledok 4. *Matica A je podobná diagonálnej matici práve vtedy, keď jej minimálny polynóm má len jednoduché korene a tie všetky patria do poľa F.*

Veta 18 (Cayley-Hamilton). *Nech $ch_A(\gamma) \in F[\gamma]$ je charakteristický polynóm matice A. Potom $ch_A(A) = 0$.*

Neistota duše je zlá vlastnosť, ale istota je smiešna.
Voltaire

3 Grupy

Sylowove vety z teórie konečných grúp. Voľná grupa a jej podgrupy. Voľný súčin grúp. Radikály ideálu, prvoideál a maximálny ideál okruhu. Polopriamy súčin okruhov. (Okruhy zlomkov, primárny rozklad ideálu.)

3.1 Normálne podgrupy a grupy permutácií

Zdalo sa mi, že aj toto by som mal niekde dať. Ak sa vám bude zdať, že sú to príliš ľahké veci, ktoré dokonale ovládate, stačí to jednoducho preskočiť.

Grupy permutácií

Cyklickou permutáciou (cyklom) dĺžky k prvkov $a_1, a_2, \ldots, a_k$ množiny X nazývame permutáciu γ, takú, že $a_i\gamma = a_{i+1}$ $(i = 1, \ldots, k-1)$ a $a_k\gamma = a_1$. Označujeme $\gamma = (a_1 a_2 \ldots a_k)$.

Súčin disjunktných cyklov nezávisí od poradia. Každá permutácia je súčin disjunktných cyklov. Tento rozklad je jednoznačný až na poradie a cykly dĺžky 1. Rád permutácie je najmenší spoločný násobok dĺžok cyklov vystupujúcich v rozklade.

Transpozícia = cyklus dĺžky 2. Každá permutácia sa dá zapísať ako súčin transpozícií.
Parita permutácie = parita počtu transpozícií = parita počtu inverzií ($i < j$, $i\varphi > j\varphi$).
S_n = symetrická grupa rádu n = permutácie množiny $\{1, \ldots, n\}$
A_n = alternujúca grupa = grupa všetkých párnych permutácií množiny $\{1, \ldots, n\}$
Grupa A_n je generovaná cyklami dĺžky 3.
Pre $n \geq 5$ jediné normálne podgrupy grupy S_n sú 1, A_n, S_n. (A_n je jadro homomorfizmu, ktorý každej permutácii priraďuje jej paritu, teda je to normálna podgrupa.)

Ak $\varphi \in S_n$, tak $\varphi^{-1}(a_1 \ldots a_k)\varphi = (a_1\varphi a_2\varphi \ldots a_k\varphi)$. K ľubovoľným dvom cyklom $\alpha, \beta \in S_n$ rovnakej dĺžky existuje permutácia $\varphi \in S_n$ taká, že $\beta = \varphi^{-1}\alpha\varphi$. Obe tieto vlastnosti sa prenesú aj na súčin disjunktných cyklov. Teda φ_1, φ_2 sú konjugované, ak sú rovnaké dĺžky cyklov v ich rozkladoch.

Normálne podgrupy

Definícia 1. Podgrupa H grupy G sa nazýva *normálna* (alebo invariantná) v G, ak pre každý prvok $a \in G$ platí implikácia: $h \in H \Rightarrow a^{-1}ha \in H$.

Ak H je normálna, tak definujeme faktorovú grupu G/H. Existuje jednojednoznačný vzťah: normálne podgrupy $\leftrightarrow$ kongruencie $\leftrightarrow$ jadrá homomorfizmov.

$gNg^{-1} = N \Leftrightarrow gN = Ng$.

Ak $H \subseteq K$ sú normálne podgrupy grupy G, tak H je normálna podgrupa grupy K a K/H je normálna podgrupa grupy G/H.

Vnútorné automorfizmy: $f_a : x \mapsto a^{-1}xa$.
$a \mapsto f_a$ je homomorfizmus, jeho jadro je $Z(G)$.

Tvrdenie 1. *Ak H, N sú podgrupy G a N je normálna, tak HN je podgrupa G. Ak navyše H je normálna, tak aj HN je normálna.*

Prienik normálnych podgrúp je normálna podgrupa. To znamená, že existuje najmenšia normálna podgrupa G obsahujúca danú podmnožinu G.

3.2 Sylowove vety

Tvrdenie 2. *Nech G je cyklická grupa, $|G| = n$, $d \mid n$. Potom existuje podgrupa H grupy G taká, že $|H| = d$.*

Nech G je komutatívna grupa, $|G| = n$, $d \mid n$. Potom existuje podgrupa H grupy G taká, že $|H| = d$.

Akcia grupy na množine

Definícia 2. Nech $M \neq \emptyset$ je množina, $(G, \circ)$ je grupa. *Akciou grupy G na množine M* nazveme zobrazenie $\alpha\colon M \times G \to M$ také, že
a) (typ 1) 1. $(\forall m \in M)\alpha(m, e) = m$
2. $(\forall m \in M)(\forall g_1, g_2 \in G)\alpha(\alpha(m, g_1), g_2) = \alpha(m, g_1 \circ g_2)$
b) (typ 2) 1. $(\forall m \in M)\alpha(m, e) = m$
2. $(\forall m \in M)(\forall g_1, g_2 \in G)\alpha(\alpha(m, g_1), g_2) = \alpha(m, g_2 \circ g_1)$

Stručnejší zápis: $me = m$, $(mg_1)g_2 = m(g_1g_2)$; $(mg_1)g_2 = m(g_2g_1)$.
Príklady: $\alpha_1(a, g) = gag^{-1}$ pre $M = G$ (konjugácia, akcia konjugáciou)
Ak H je podgrupa G, tak $\alpha_H(X, h) = \{hxh^{-1}; x \in X\}$ pre $h \in H$ je akcia grupy H na množine $M = \mathcal{P}(G) \setminus \{\emptyset\}$.

Definícia 3. Nech $M \neq \emptyset$ je množina, G je grupa, α je akcia G na M. Hovoríme, že $S_\alpha(m) = \{g \in G; \alpha(m, g) = m\}$ je *stabilizátor* prvku $m \in M$ v akcii α.

Tvrdenie 3. *$S_\alpha(m)$ je podgrupa G.*

Definícia 4. Nech $M \neq \emptyset$ je množina, G je grupa, α je akcia G na M. Hovoríme, že $O_\alpha(m) = \{n \in M; (\exists g \in G)\alpha(m, g) = n\}$ je *orbita* prvku $m \in M$ v akcii α.

Veta 1. $|O_\alpha(m)| = |G : S_\alpha(m)|$

Lema 1. *Systém $\{O_\alpha(m) : m \in M\}$ je rozklad M.*

Definícia 5. Nech G je grupa, $\emptyset \neq X \subset G$. Potom množinu $C_G(X) = \{z \in G; (\forall x \in X)zx = xz\}$ nazývame *centralizátor* množiny X v grupe G. Špeciálne $C_G(G) =: Z(G)$ nazývame *centrum* grupy G.

Definícia 6. Nech G je grupa a H je podgrupa G. Hovoríme, že H je *charakteristická,* ak pre každý homomorfizmus $\varphi\colon G \to G$ platí $\varphi(H) = H$.

Každá charakteristická podgrupa je normálna. $Z(G)$ je charakteristická podgrupa.
Označme $gxg^{-1} =: x^g$, $\{x^h; x \in X\} =: X^h$.

Definícia 7. Nech H je podgrupa G. Množina $N_{G,H}(X) = \{h \in H : X^h = X\}$ sa nazýva *normalizátor* množiny X v grupe H.
$N_{G,G}(X) =: N_G(X)$ je normalizátor X v G.
$N_{G,H}(X) = S_{\alpha_H}(X)$ a $C_G(\{x\}) = S_{\alpha_1}(x) = N_{G,G}(\{x\})$, preto $N_{G,H}(X)$ a $C_G(\{x\})$ sú podgrupy G. $C_G(X) = \bigcap\limits_{x\in X} C_G(\{x\})$, teda aj $C_G(X)$ je podgrupa G. (Nemusí byť normálna.)

Definícia 8. Nech G je grupa, $a, b \in G$. Hovoríme, že a a b sú *konjugované*, ak existuje $g \in G$ také, že $b = a^g = gag^{-1}$ (t.j. $b \in O_{\alpha_1}(a)$). Je to relácia ekvivalencie.

$\varphi_g : a \mapsto a^g = gag^{-1}$ je *vnútorný automorfizmus.*
$g \mapsto \varphi_g$ je tzv. antihomomorfizmus (obracia operácie).

Sylowove vety

Lema 2. *Nech G je grupa, K, H sú podgrupy G. Triedou rozkladu G podľa dvojného modulu K, H nazývame množinu $KgH = \{kgh; k \in K, h \in H\}$ (pre $g \in G$).*
Triedy KgH, $g \in G$ tvoria rozklad grupy G.

Veta 2. *Nech K, H sú podgrupy G. Počet ľavých tried rozkladu podľa podgrupy H v množine KgH je $[K : K \cap gHg^{-1}] = [g^{-1}Kg : g^{-1}Kg \cap H]$. Počet pravých tried rozkladu podľa podgrupy K v množine KgH je $[gHg^{-1} : K \cap gHg^{-1}] = [H : g^{-1}Kg \cap H]$.*

Lema 3. $|O_{\alpha_1}(g)| = 1 \Leftrightarrow g \in Z(G)$

Veta 3 (Cauchy). *Nech G je konečná grupa, p je prvočíslo a $p \mid |G|$. Potom existuje podgrupa H grupy G taká, že $|H| = p$.*

Dôsledok 1. *Nech G je konečná grupa taká, že existuje prvočíslo p s vlastnosťou $p \mid |G|$ a pre každú vlastnú podgrupu H platí $p \mid |[G : H]|$. Potom G má netriviálne centrum, t.j. $Z(G) \neq \{e\}$.*

Dôsledok 2. *Nech G je grupa s p^2 prvkami, pričom p je prvočíslo. Potom G je komutatívna.*

Veta 4 (1. Sylowova). *Nech G je grupa, p je prvočíslo, $|G| = p^m.s$, $p \nmid s$. Potom*

(i) v G existujú podgrupy $H_1, \ldots, H_m$ také, že $|H_i| = p^i$,

(ii) ak $i < m$ a H je p^i-prvková podgrupa G, tak existuje p^{i+1}-prvková podgrupa G taká, že H je jej invariantná podgrupa.

Definícia 9. Grupa G sa nazýva *p-grupa*, ak každý jej prvok má rád tvaru p^m. (p-prvočíslo)

Tvrdenie 4. *Konečná p-grupa G má p^m prvkov pre vhodné m.*

Definícia 10. Nech G je konečná grupa, p je prvočíslo, $|G| = p^m.s$, $p \nmid s$. Podgrupa S grupy G sa nazýva *Sylowova p-podgrupa G*, ak $|S| = p^m$. Podgrupa S grupy G sa nazýva *Sylowova podgrupa G*, ak existuje prvočíslo p také, že S je Sylowova p-podgrupa G.

Dôsledok 3. *Ak p je prvočíslo a $p \mid |G|$, tak existuje Sylowova p-podgrupa grupy G. Ak S je podgrupa G, $|S| = p^k$, tak existuje Sylowova p-podgrupa H grupy G taká, že $S \subseteq H$.*

Dôsledok 4. *Ak G je konečná p-grupa, $|G| = p^m$, tak každá podgrupa S taká, že $|S| = p^{m-1}$ je invariantná v G.*

Veta 5 (2. Sylowova veta). *Nech P_1, P_2 sú dve Sylowove p-podgrupy G. Potom $(\exists g \in G)P_1 = gP_2g^{-1}$, t.j. P_1 a P_2 sú konjugované.*

Dôsledok 5. *Nech G je konečná grupa, S je Sylowova p-podgrupa. Potom S je jediná Sylowova p-podgrupa grupy $N_G(S)$.*

Veta 6 (3. Sylowova). *Nech G je konečná grupa, $p \mid |G|$, p je prvočíslo. Potom pre počet k Sylowových p-podgrúp platí*

(i) $k \mid |G|$

(ii) $k = 1 + lp$, $l \in \mathbb{N}_0$

Veta 7. *Nech $P \subseteq K \subseteq H \subseteq G$ sú podgrupy grupy G. Nech P je Sylowova p-podgrupa, $K = N_G(P)$. Potom $N_G(H) = H$.*

Veta 8. *Nech A, B sú invariantné podgrupy G také, že $A \cap B = \{e\}$ a $A.B = [A \cup B] = G$. Potom $G \cong A \times B$.*

Veta 9. *Nech G je grupa, $x \in G$ je taký, že $rad(x) = mn$, $(m, n) = 1$. Potom existuje jediná dvojica prvkov $y, z \in G$ taká, že $x = yz = zy$, pričom $rad(y) = m$, $rad(z) = n$.*

Tvrdenie 5. *Konečná p-grupa má netriviálne centrum.*

Veta 10. *Nech G je konečná grupa. Nasledujúce podmienky sú ekvivalentné:*

(i) Ak pre prvočíslo p platí $p \mid |G|$, tak v G existuje práve jedna Sylowova p-podgrupa (t.j. pre každé prípustné p má len jednu Sylowovu p-podgrupu).

(ii) G sa dá napísať ako priamy súčin svojich Sylowových p-podgrúp.

(iii) Žiadna vlastná podgrupa grupy G nie je totožná sa svojím normalizátorom.

Veta 11. *Nech G je p-grupa a $H \subseteq G$ je invariantná p-prvková podgrupa. Potom $H \subseteq Z(G)$.*

Definícia 11. $[a, b] = aba^{-1}b^{-1} =$ *komutant* prvkov a, b
$[G, G] = [\{[a, b]; a, b \in G\}] =$ *komutátor* grupy G

$[G, G]$ je charakteristická podgrupa (teda je normálna).
G/N je komutatívna $\Leftrightarrow G \supseteq N \supseteq [G, G]$
Označme $Z_1(G) = Z(G)$ a $Z_{k+1}(G) = \psi^{-1}(Z(G/Z_k(G)))$ (ψ je prirodzený homomorfizmus).
$1 \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \ldots$

Definícia 12. Grupa G je *nilpotentná,* ak existuje také k, že $Z_k(G) = G$. Najmenšie také k nazveme *stupeň nilpotentnosti* grupy G.

Tvrdenie 6. *Každá konečná p-grupa je nilpotentná.*

3.3 Voľné grupy a voľné súčiny

Voľná grupa a jej podgrupy

Nech $X' = \{a, a^{-1}, b, b^{-1}, \ldots\}$ pre $X = \{a, b, \ldots\}$. Nech W' je množina všetkých slov nad abecedou X'. Slovo $w \in W'$ je v *redukovanom tvare* ak neobsahuje podslovo tvaru xx^{-1} alebo $x^{-1}x$. Dá sa ukázať, že pre každé slovo existuje jediný redukovaný tvar, bez ohľadu na to, v akom poradí vykonávame redukcie. Ak vytvoríme reláciu ekvivalenciu na W' takú, že 2 slová budú ekvivalentné ak majú rovnaký redukovaný tvar a definujeme násobenie, dostaneme grupu FX. FX je *voľná grupa* na X.

Tvrdenie 7. *Pre ľubovoľné zobrazenie $f\colon X \to G$, kde G je grupa, existuje jediný homomorfizmus $\varphi\colon FX \to G$ taký, že $\varphi|_X = f$.*

Veta 12 (Nielsen-Schreier). *Podgrupa voľnej grupy je voľná.*

TODO Možno by sa patrilo stratiť aj pár slov a dôkaze.

Veta 13. *Ak U je podgrupa grupy F_r indexu n, tak U má $n(r-1)+1$ generátorov.*

$$U \cong F_{n(r-1)+1}$$

Voľný súčin grúp

Voľný súčin grúp možno reprezentovať ako postupnosti, v ktorých sa striedajú prvky jednotlivých grúp, ktoré vystupujú v súčine. Opäť sa dá zaviesť ekvivalencia, redukciu bude teraz predstavovať vynechanie jednotky niektorej grupy z postupnosti a nahradenie dvoch po sebe idúcich prvkov tej istej grupy ich súčinom.

Písať sem aj voľný súčin s amalgamáciou???

Veta 14 (Kuroš). *Nech $G = \prod_{i\in I} G_i$ je voľný súčin grúp. Nech $H \neq 1$ je podgrupa grupy G. Potom H je tiež voľný súčin grúp v tvare*

$$H = F \prod \alpha_j^{-1} B_j \alpha_j,$$

kde F je voľná grupa a každá s podgrúp $\alpha_j^{-1} B_j \alpha_j$ je podgrupa konjugovaná s podgrupou B_j niektorej z grúp G_i, $i \in I$.

3.4 Okruhy, radikály, prvoideály

Prvoideály v komutatívnych okruhoch

V tejto časti R bude znamenať komutatívny okruh s jednotkou.

Lema 4. *$a \in R$ nie je invertibilný $\Leftrightarrow$ existuje maximálny ideál I okruhu R taký, že $a \in I$.*

Lema 5. *Nech I je ideál okruhu R a $x \in R$. Potom najmenší ideál okruhu R, ktorý obsahuje I aj x je $I + (x) = \{a + bx; a \in I, b \in R\}$.*

Lema 6. *I je maximálny ideál $R \Leftrightarrow (\forall r \notin I)(\exists x \in R)(1 - rx \in I)$.*

Veta 15. *Ak A je ideál v R, $A \subseteq B$, B je prvoideál, potom množina $\{P; A \subseteq P$ a P je prvoideál$\}$ má minimálny prvok.*

Definícia 13. Nech R je komutatívny okruh. *Radikál* R je $rad(R) = \bigcap\{I; I \text{ je prvoideál}\}$.

Ak R je obor integrity, tak $rad(R) = 0$.
Radikál je ideál.

Definícia 14. Prvok a okruhu R sa nazýva *nilpotentný,* ak existuje $n \in \mathbb{N}$ také, že $a^n = 0$.

Lema 7. *Nech $T \subset R$ a existuje ideál I taký, že $I \cap T = \emptyset$. Potom existuje maximálny (v zmysle inklúzie - nie maximálny ideál okruhu) ideál I_0 taký, že $I_0 \cap T = \emptyset$.*

Definícia 15. $T \subseteq R$ je uzavretá na konečné súčiny, ak $1 \in T$, $0 \notin T$ a pre $a, b \in T$ aj $ab \in T$.

Lema 8. *Nech $T \subseteq R$ je uzavretá na konečné súčiny, P je maximálny ideál (maximálny vzhľadom na inklúziu) taký, že $P \cap T = \emptyset$. Potom P je prvoideál.*

Tvrdenie 8. $rad(R) = \{a \in R; a \text{ je nilpotentný}\}$

Definícia 16. *Jacobsonov radikál* $Rad(R) = \bigcap(I; I \text{ je maximálny ideál})$

Lema 9. $r \in Rad(R) \Leftrightarrow (\forall x) 1 - rx$ *je invertibilný v* R

Definícia 17. Okruh R je *polojednoduchý*, ak $Rad(R) = \{0\}$. *R má triviálny radikál*, ak $rad(R) = \{0\}$.

Veta 16. *(i) $R/Rad(R)$ je polojednoduchý okruh.*

(ii) $R/rad(R)$ má triviálny radikál.

Polopriamy súčin

Definícia 18. Okruh R nazývame *polopriamy súčin* okruhov S_i, $i \in I$ ak $\kappa\colon R \hookrightarrow \prod S_i$ a každé $\pi_i \circ \kappa$ je surjektívne.

Veta 17. *Okruh R je polopriamy súčin okruhov S_i $i \in I \Leftrightarrow S_i \cong R/K_i$, K_i je ideál R a $\bigcap K_i = \{0\}$.*

Dôsledok 6. *Komutatívny okruh R je polojednoduchý práve vtedy, keď je polopriamy súčin polí. Komutatívny okruh má triviálny radikál práve vtedy, keď je polopriamy súčin oborov integrity.*

Dôsledok 7. *Komutatívny okruh R má triviálny radikál práve vtedy, keď R je izomorfný podokruhu súčinu oborov integrity.*

Dôsledok 8. *Komutatívny okruh R má triviálny radikál práve vtedy, keď R je izomorfný podokruhu súčinu polí. (Pri dôkaze sa využije, že každý obor integrity vieme vložiť do podielového poľa.)*

Definícia 19. Hovoríme, že okruh R je *polopriamo nerozložiteľný* ak prienik všetkých jeho nenulových ideálov je nenulový ideál.

Tvrdenie 9. *Ak R je polopriamo nerozložiteľný a R je polopriamy súčin S_i, tak $R = S_i$ pre niektoré i a pre $j \neq i$ je $S_j \cong \{0\}$.*

Veta 18 (Birkhoff). *Každý okruh je polopriamy súčin polopriamo nerozložiteľných okruhov.*

3.5 Okruhy zlomkov

Najprv by som aspoň veľmi stručne spomenul, čo je podielové pole. Jednak preto, že tieto dve konštrukcie sú podobné a dvak preto, že podielové pole asi patrí k veciam, ktoré by mal človek končiaci štruktúry vedieť.

Zlomkom nad oborom integrity D nazývame usporiadanú dvojicu (a, b), kde $a, b \in D$, $b \neq 0$. Na množine všetkých zlomkov definujeme reláciu ekvivalencie $(a, b) \equiv (a', b')$ práve vtedy, keď $ab' = a'b$. Ďalej definujeme súčet a súčin ako $(a, b) + (c, d) = (ad + bc, bd)$, $(a, b)(c, d) = (ac, bd)$. Triedy ekvivalencie zlomkov s takto definovanými operáciami tvoria pole, ktoré sa nazýva *podielové pole* a označuje $Q(D)$. Je to najmenšie pole obsahujúce obor integrity D v tom zmysle, že ak je D vnorené do nejakého poľa, tak toto vnorenie možno rozšíriť na celé $Q(D)$.

Toto som odpísal z [ASH].

Okruh zlomkov je podobná konštrukcia ako podielové pole. Pretože nepracujeme s oborom integrity, ale s ľubovoľným okruhom, treba obmedziť množinu prípustných menovateľov, aby sme nedostali v menovateli nulu. Ďalej budeme predpokladať, že R je komutatívny okruh.

Definícia 20. Nech S je podmnožina okruhu R. Hovoríme, že S je *multiplikatívna,* ak $0 \notin S$, $1 \in S$ a $a, b \in S \Rightarrow ab \in S$.

Typické príklady:
$S =$ množina všetkých nenulových prvkov oboru integrity,
$S =$ množina všetkých prvkov komutatívneho okruhu, ktoré nie sú deliteľmi nuly,
$S = R \setminus P$, kde P je prvoideál komutatívneho okruhu R.

Ak S je multiplikatívna podmnožina okruhu R, tak definujeme na $R \times S$ reláciu ekvivalencie

$$(a, b) \sim (c, d) \text{ práve vtedy, keď pre nejaké } s \in S \text{ je } s(ad - bc) = 0.$$

(Ľahko sa overí, že je to relácia ekvivalencie, keď využijeme komutatívnosť R. Vraj sa okruhy zlomkov zavádzajú aj v nekomutatívnom prípade, ale je to o dosť obtiažnejšie.)

Zlomok $\frac{a}{b}$ potom definujeme ako triedu ekvivalencie dvojice (a, b). Množinu zlomkov označíme $S^{-1}R$. $S^{-1}R$ s prirodzene definovaným sčitovaním a násobením tvorí komutatívny okruh. Ak R je obor integrity, tak takýmto spôsobom dostaneme podielové pole.

Tvrdenie 10. *Nech $f\colon R \to S^{-1}R$, $f(a) = a/1$. Potom f je okruhový homomorfizmus. Ak S neobsahuje delitele nuly, tak f je prosté, čiže R možno vložiť do $S^{-1}R$.*

Lámme si hlavu!
Šalát

4 Polynómy

Rezultant. Vlastnosti polynómov nad poľom reálnych a komplexných čísel. Separácia koreňov, ohraničenie koreňov, Sturmov systém. Numerický výpočet koreňov.

4.1 Rezultant

Definícia 1. Nech $f, g \in F[x]$, $f = a_0x^n + a_1x^{n-1} + \ldots + a_n$, $g = b_0x^m + \ldots + b_m$. Potom *rezultant* polynómov f a g je

$$R(f,g) = \begin{vmatrix} a_0 & a_1 & \ldots & a_n & 0 & \ldots & 0 \\ 0 & a_0 & a_1 & \ldots & a_n & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & a_0 & a_1 & \ldots & a_n \\ b_0 & b_1 & \ldots & b_m & 0 & \ldots & 0 \\ 0 & b_0 & b_1 & \ldots & b_m & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & b_0 & b_1 & \ldots & b_m \end{vmatrix}$$

(pomocou polynómu f je vytvorených prvých m riadkov a pomocou g zvyšných n riadkov)

Tvrdenie 1.

$$R(f,g) = a_0^m \prod_{i=1}^{n} g(\alpha_i),$$

kde korene f sú po rade $\alpha_1, \ldots, \alpha_n$.

Dôsledok 1. *$R(f,g) = 0$ práve vtedy, keď f a g majú spoločný koreň.*

$R(f, f')$ sa nazýva *diskriminant* f. Diskriminant je nulový práve vtedy, keď f má násobný koreň.

4.2 Vlastnosti polynómov nad poľom reálnych a komplexných čísel

Veta 1 (Gaussova, Základná veta algebry). *Pole $\mathbb{C}$ je algebraicky uzavreté.*

Tvrdenie 2. *Polynóm $f(x)$ s reálnymi koeficientmi je ireducibilný nad $\mathbb{R}$ práve vtedy, keď $\operatorname{st} f(x) = 1$ alebo $\operatorname{st} f(x) = 2$ a $f(x)$ nemá reálne korene, t.j. má dva združené imaginárne korene.*

Tvrdenie 3. *Majme $f(x) = a_0 + a_1x + \ldots + a_nx^n \in Z[x]$ stupňa $n \geq 1$. Nech $\frac{p}{q} \in \mathbb{Q}$, pričom $(p,q) = 1$. Ak $\frac{p}{q}$ je koreňom $f(x)$, tak $p \mid a_0$ a $q \mid a_n$ v okruhu Z.*

4.3 Ohraničenie a separácia koreňov

Budeme sa zaoberať rovnicou

$$f(x) = x^n + a_1x^{n-1} + \ldots + a_n = 0 \tag{1}$$

Veta 2. *Všetky reálne korene rovnice (1) s reálnymi koeficientmi ležia v intervale $\langle -1 - A, 1 + A\rangle$, kde $A = \max\{|a_1|, \ldots, |a_n|\}$.*

Veta 3. *Nech (1) je rovnica s reálnymi koeficientmi, pričom aspoň jeden z koeficientov je záporný. Predpokladajme, že a_k je v poradí prvý záporný koeficient. Nech B je najväčšia z absolútnych hodnôt záporných koeficientov rovnice (1). Potom každý reálny koreň rovnice (1) je menší ako číslo $1 + \sqrt[k]{B}$.*

Ak použijeme predchádzajúcu vetu na polynóm $f(-x)$, tak dostaneme ohraničenie zdola.

4.4 Sturmov systém

Majme rovnicu (1) s reálnymi koeficientmi. Predpokladajme, že polynóm $f(x)$ má len jednoduché korene. *Sturmov reťazec polynómov* $f_0(x), f_1(x), \ldots, f_m(x)$ patriacich k polynómu $f(x)$ sa zostrojí takto: Položme $f_0(x) = f(x)$ a $f_1(x) = Df(x) = f'(x)$. Ostatné polynómy Sturmovho reťazca získame zo vzťahu $f_i(x) = f_{i+1}(x)q_{i+1}(x) - f_{i+2}(x)$. (Tento vzťah určuje až na znamienko polynómy vystupujúce v Euklidovom algoritme. Teda stupne postupne klesajú.)

Pod *znamienkovou zmenou* v postupnosti $f_0(c), f_1(c), \ldots, f_m(c)$ rozumieme prípad, keď $f_i(c).f_{i+1}(c) < 0$ alebo $f_i(c) = 0$ a $f_{i-1}(c).f_{i+1}(c) < 0$. (Viackrát za sebou tam 0 byť nemôže.)

Veta 4 (Sturmova). *Majme polynóm $f(x)$ s reálnymi koeficientmi a reálne čísla $a < b$. Nech $f(a) \neq f(b)$. Potom počet reálnych koreňov rovnice (1) ležiacich v otvorenom intervale (a, b) sa rovná číslo $Zn(a) - Zn(b)$. ($Zn(c)$ znamená počet znamienkových zmien v postupnosti $f_0(c), \ldots, f_m(c)$.)*

4.5 Numerické riešenie

Newtonova metóda (metóda dotyčníc) a metóda tetív (regula falsi).

Pri Newtonovej metóde sa v [ATA] spomína táto veta (je tam bez dôkazu).

Veta 5. *Majme rovnice (1) s reálnymi koeficientmi a jednoduchými koreňmi. Nech rovnica (1) má jediný koreň vnútri intervalu $\langle a, b\rangle$. Ďalej predpokladáme, že $f'(x) \neq 0$ a $f''(x) \neq 0$ na celom intervale $\langle a, b\rangle$. Označme znakom c_1 to z čísel a, b, v ktorom $f(c_1).f''(c_1) > 0$. Znakom d_1 označme druhé číslo z čísel a, b, t.j. číslo v ktorom $f(d_1).f''(d_1) < 0$. Utvorme postupnosti*

$$c_1,\ c_2 = c_1 - \frac{f(c_1)}{f'(c_1)},\ c_3 = c_2 - \frac{f(c_2)}{f'(c_2)}, \ldots$$
$$d_1,\ d_2 = d_1 - \frac{f(d_1)}{f'(c_1)},\ d_3 = d_2 - \frac{f(d_2)}{f'(c_2)}, \ldots$$

Potom jedna z postupností je klesajúca, druhá rastúca a obe postupnosti konvergujú ku koreňu α.

Nikto nekričí: „Už spíme!“
Valková

5 Konečné polia a kódovanie

Polynómy nad konečným poľom, ich rozklad na súčin ireducibilných polynómov. Rozkladové pole polynómu. Bezpečnostné kódy. Lineárne kódy, Hammingove kódy. Generujúce polynómy a cyklické kódy.

5.1 Rozklad na súčin ireducibilných polynómov

V tejto a v nasledujúcej časti sú odpísané nejaké veci z [ATA].

Okruhy polynómov - koreň, deliteľnosť, NSD, Euklid, OHI

Veta 1. *Majme polynóm $f(x) = a_0 + \ldots + a_n x^n$ v neurčitej x nad poľom F. Nech $a_n \neq 0$ a $n \geq 1$. Potom existujú polynómy $p_1(x), \ldots, p_m(x)$ normované a ireducibilné nad F a platí*

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

Tento rozklad je jednoznačne určený až na poradie činiteľov.

Veta 2 (Eisensteinovo kritérium). *Nech p je prvočíslo a $a(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ je polynóm s celočíselnými koeficientami taký, že $a_n \not\equiv 0\,(mod\ p)$ a $a_{n-1} \equiv a_{n-2} \equiv \ldots a_0 \equiv 0\,(mod\ p)$, $a_0 \not\equiv 0\,(mod\ p^2)$. Potom $a(x)$ je ireducibilný nad poľom racionálnych čísel.*

5.2 Rozkladové pole polynómu

Algebraické a transcendentné rozšírenia

Definícia 1. Nech F, L sú polia, $F \subseteq L$. Prvok $u \in L$ sa nazýva *algebraický* nad F, ak je koreňom nejakého polynómu z $F[x]$. Prvok $u \in L$ sa nazýva *transcendentný* nad F, ak nie je koreňom žiadneho polynómu z $F[x]$.

Definícia 2. Pole L nazývame *jednoduchým algebraickým rozšírením* poľa $F \subseteq L$, ak existuje prvok $u \in L$, algebraický nad F taký, že pole $L = F(u)$ je generované množinou $F \cup \{u\}$ (hovoríme, že L je generované prvkom u nad F.) Ak u je transcendentný nad F, tak $L = F(u)$ nazývame *jednoduché transcendentné rozšírenie* poľa F.

Pole $F(u)$ generované prvkom u má tvar

$$F(u) = \left\{ \frac{f(u)}{g(u)}; g(u) \neq 0 \right\}.$$

Z toho vyplýva nasledujúca úplná charakterizácia jednoduchých transcendentných rozšírení.

Veta 3. *Jednoduché transcendentné rozšírenie $F(u)$ poľa F je izomorfné s podielovým poľom $Q(F[x])$ okruhu $F[x]$ polynómov jednej neurčitej nad F.*

Rozkladové polia

Definícia 3. Rozšírenie L poľa F nazývame *rozkladovým poľom polynómu* f nad F, $\mathrm{st}\, f = n > 0$, ak existujú prvky $c \in F$, $u_1, u_2 \ldots u_n \in L$ také, že $L = F(u_1, \ldots, u_n)$ a f sa dá nad L rozložiť na súčin lineárnych činiteľov

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

Veta 4. *Ak p je ireducibilný polynóm nad poľom F, tak existuje jednoduché algebraické rozšírenie $F(u)$ generované koreňom u polynómu p. (Je izomorfné s $F/(p)$.)*

Veta 5. *Pre každý polynóm f nad poľom F, $\mathrm{st}\, f = n > 0$ existuje rozkladové pole f nad F. Je určené jednoznačne až na izomorfizmus.*

Veta 6. *Pre každé číslo tvaru $q = p^n$, kde p je prvočíslo, $n > 0$ prirodzené číslo, existuje (okrem izomorfizmu) práve jedno q-prvkové pole – je to rozkladové pole polynómu $x^q - x$ nad Z_p.*

Multiplikatívnu grupu poľa F budeme značiť F^*.

Veta 7. *Nech F je pole. Potom každá podgrupa grupy F^* s konečným počtom prvkov je cyklická.*

Veta 8. *Nech F_r je konečné rozšírenie konečného poľa F_q. Potom F_r je jednoduché algebraické rozšírenie a každý primitívny prvok z F_r (generátor F_r^*) je generátorom rozšírenia F_r t.j. $F_r \cong F_q(\xi)$. (ξ je primitívny prvok.)*

Dôsledok 1. *Pre každé $n > 0$ existuje ireducibilný polynóm nad Z_p stupňa n. (Je to minimálny polynóm primitívneho prvku z F_q^*, $q = p^n$.)*

5.3 Kódovanie

Literatúra ku kódovaniu: hlavne [AD], čosi je aj v [JAB].

Definícia 4. Nech A, B sú konečné množiny, B^* je množina všetkých slov nad B, t.j. $B^* = \{u = e_1 \dots e_k; k \in \mathbb{N}_0, e_i \in B\}$. Potom injektívne zobrazenie $k\colon A \to B^*$ sa nazýva *kód.* Prvky z $k(A)$ sa nazývajú kódové slová.

Kód k možno rozšíriť na zobrazenie $k^*\colon A^* \to B^*$. Ak k^* je prosté zobrazenie, hovoríme o *jednoznačne dekódovateľnom* kódovaní.

Označme B^n množinu všetkých slov nad B dĺžky n. Kód $k\colon A \to B^n$ sa nazýva *blokový kód dĺžky n.*

Veta 9. *Nech $n = |B| \geq 2$, nech $A = \{a_1, \dots, a_r\}$. Nech $d_1, \dots, d_r$ sú po rade predpísané dĺžky kódových slov pre $a_1, \dots, a_r$. Nech $d_1 \leq \dots \leq d_r$. Potom sa dá zostrojiť prefixový kód práve vtedy, keď platí Kraftova nerovnosť $n^{-d_1} + \dots + n^{-d_r} \leq 1$.*

Veta 10 (McMilan). *Každý jednoznačne dekódovateľný kód spĺňa Kraftovu nerovnosť*

$$n^{-d_1} + \dots + n^{-d_r} \leq 1,$$

kde d_i sú dĺžky všetkých kódových slov a $n = |B|$.

Bezpečnostné kódy

Definícia 5. Hovoríme, že v slove došlo ku *t-násobnej chybe*, ak prijaté slovo sa líši od vyslaného slova na nanajvýš t miestach. Hovoríme, že kód *objavuje t-násobné chyby,* ak pri vyslaní kódového slova došlo ku t-násobnej chybe, tak prijmeme nekódové slovo.

Definícia 6. Nech T je abeceda a $u, v \in T^n$. $d(u, v) = \|u - v\| = |\{i : u_i \neq v_i\}|$ sa nazýva *Hammingova vzdialenosť* u a v.

Hammingova vzdialenosť je metrika.

$\min\{d(u, v); u \neq v; u, v \in k(A)\}$ sa nazýva *minimálna vzdialenosť kódu.*

Veta 11. *Nech $k\colon A \to T^n$ je blokový kód minimálnej vzdialenosti d. Potom k objavuje t-násobné chyby pre $t < d$, k nie je schopný objaviť d-násobné chyby.*

Definícia 7. Hovoríme, že kód *opravuje t-násobné chyby,* ak po vyslaní $v \in k(A)$ a prijatí $w \in T^n$ s vlastnosťou $d(v, w) \leq t$ platí $d(v, w) < d(x, w)$ pre všetky $x \in k(A)$, $x \neq v$.

Veta 12. *Blokový kód minimálnej vzdialenosti d opravuje chyby pre $t < \frac{d}{2}$.*

Definícia 8. Nech $k\colon A \to T^n$ je blokový kód. Ak existuje $l < n$ a bijekcia $\varphi\colon T^l \to k(A)$, hovoríme, že k má l *informačných* a $n - l$ *kontrolných* znakov. φ sa nazýva kódovanie informačných symbolov.

Blokový kód $k(A) \subseteq T^n$ je *systematický*, ak existuje číslo $l < n$, že každé slovo $v_1 \dots v_l \in T^l$ možno jednoznačne predĺžiť na nejaké kódové slovo.

Veta 13. *Nech $k\colon A \to T^n$ je systematický, pričom má l informačných symbolov. Potom $d \leq n - l + 1$.*

Lineárne kódy

Definícia 9. *Lineárny kód* je podpriestor vektorového priestoru (F, F^n), kde F je konečné pole. (tzv. lineárny (n, r)-kód, kde $r = \dim(k(A))$).

Generujúca matica lineárneho kódu je matica G, ktorej riadky tvoria bázu podpriestoru $k(A)$.

Lineárny kód $k(A)$ je systematický, ak má generujúcu maticu $G = (I_k G')_{k\times n}$. Aby sme zistili, či kód s danou generujúcou maticou je systematický, upravíme ju na redukovaný trojuholníkový tvar. (Pomocou elementárnych riadkových operácií z generujúcej matice dostaneme generujúcu maticu toho istého kódu.)

Definícia 10. Kódy $k_1, k_2 \subseteq F^n$ sú ekvivalentné, ak existuje permutácia stĺpcov G_1, ktorou dostaneme generujúcu maticu G_2.

Definícia 11. Nech K je lineárny (n, k)-kód. Matica B nad poľom F sa nazýva *kontrolná matica* kódu K, ak

$$v_1 \dots v_n \in K \Leftrightarrow B\underline{v}^T = \underline{0}^T.$$

$BG^T = 0$, $GB^T = 0$
Pre $u, v \in F^n$ definujme

$$u * v := u_1 v_1 + \dots + u_n v_n.$$

Veta 14. *Nech K je lineárny (n, k)-kód nad konečným poľom F. Potom $K^\perp = \{v \in F^n : u * v = 0\ \forall u \in K\}$ je podpriestor F^n a $\dim(K^\perp) = n - k$, t.j. $K^\perp$ je lineárny $(n, n-k)$-kód. $K^\perp$ voláme duálny podpriestor/duálny kód ku K.*

Generujúca matica kódu K je kontrolnou maticou kódu $K^\perp$ a obrátene.

Definícia 12. *Hammingova váha* slova $v = v_1 \dots v_n \in F^n$ je počet nenulových zložiek slova v. $\|v\| = |\{i : v_i \neq 0\}|$

Lema 1. *Nech $K \subseteq F^n$ je lineárny kód a d je jeho minimálna vzdialenosť. Potom $d = \min\{\|w\| : w \in K - \{0\}\}$.*

Veta 15. *Lineárny kód objavuje t-násobné chyby práve vtedy, keď každých t stĺpcov jeho kontrolnej matice je lineárne nezávislých.*

Veta 16 (o štandardnom dekódovaní). *Nech K je $(n, k)-$lineárny kód nad poľom F. Nech $e' \in e + K$ je slovo s najmenšou váhou v triede ekvivalencie $e + K$. e' budeme volať reprezentantom triedy $e + K$. Potom zobrazenie $\delta\colon F^n \to K$ definované vzťahom $\delta(w) = w-$reprezentant triedy $(w + K)$, t.j. $\delta(w) = w - e'$ je dekódovanie. Voláme ho* štandardné dekódovanie.

Štandardné dekódovanie opravuje práve tie chybové slová, ktoré sme zvolili za reprezentantov. Navyše žiadne dekódovanie neopravuje väčšiu množinu slov ako δ.

Veta 17. *Nech $\mathbb{H}$ je kontrolná matica lineárneho $(n, k)-$kódu K nad F. Potom $e+K = e'+K$ $\Leftrightarrow \mathbb{H}e^T = \mathbb{H}e'^T$.*

Definícia 13. Nech $\mathbb{H}$ je kontrolná matica lineárneho kódu $K \subseteq F^n$. Nech

$$\mathbb{H}\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix}.$$

Potom slovo $\underline{s} = s_1 \dots s_n$ sa volá *syndróm* slova $v = v_1 \dots v_n$.

Štandardné dekódovanie možno urýchliť pomocou syndrómov, ak vopred vypočítame tabuľku popisujúcu, ktorý reprezentant zodpovedá ktorému syndrómu.

5.4 Hammingove kódy

$F = \mathbb{Z}_2$ - ide o binárny kód.
(7,4)-lineárny kód

$$\mathbb{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Reprezentanti sú e_1 až e_7, syndróm pre e_i je zápis i v dvojkovej sústave. Pre Hammingove kódy je jednoduchý výpočet syndrómu aj výber reprezentanta.

Veta 18. *Binárny lineárny kód opravuje jednoduché chyby práve vtedy, keď stĺpce jeho kontrolnej matice sú nenulové a navzájom rôzne.*

Definícia 14. Binárny kód sa nazýva *Hammingov,* ak jeho kontrolná matica má k riadkov, $2^k - 1$ nenulových stĺpcov a žiadne 2 stĺpce nie sú rovnaké. Je to $(2^k - 1, 2^k - k - 1)$-kód.

Rozšírený Hammingov kód vznikne ak pridáme navyše kontrolu parity, t.j. $v_1 + \ldots + v_{2^m-1} + v_{2^m} = 0$. (Zodpovedá doplneniu riadku pozostávajúceho zo samých jednotiek do kontrolnej matice.)

5.5 Perfektné kódy

Definícia 15. Lineárny kód sa nazýva *perfektný* pre t-násobné opravy, ak jeho reprezentantmi sú všetky slová váhy menšej alebo rovnej t.

Veta 19. *Hammingove kódy sú perfektné pre jednoduché opravy.*
Ak nejaký kód je perfektný binárny lineárny kód na opravu jednoduchých chýb, tak je to Hammingov kód.

Veta 20 (Jietävaismen, Van Lint). *Jediné netriviálne perfektné kódy (až na ekvivalenciu) sú tieto:*

(i) Hammingove kódy pre jednoduché chyby,

(ii) Golayov kód pre trojnásobné chyby

(iii) opakovacie kódy dĺžky $2t + 1$ pre t-násobné chyby.

5.6 Cyklické kódy

Definícia 16. Lineárny kód $K \subseteq F^n$ je *cyklický*, ak $v_0 \ldots v_{n-1} \in K \Rightarrow v_{n-1}v_0 \ldots v_{n-2} \in K$.

$v = v_0 \ldots v_{n-1} \leftrightarrow f(x) = v_0 + v_1 x + \ldots + v_{n-1}x^{n-1}$

Veta 21. *Nech F je konečné pole. Potom lineárny kód $K \subseteq F^n$ je cyklický práve vtedy, keď K je ideálom okruhu $(F^n, +, *) \cong F[x]/(x^n - 1)$. ($*$ je násobenie modulo $x^n - 1$, t.j. $x * f(x)$ predstavuje posun doľava)*

Veta 22. *Každý netriviálny cyklický (n, k)-kód obsahuje polynóm $g(x)$ stupňa $n - k$ a platí:*

(i) K je hlavný ideál v F^n generovaný polynómom $g(x)$.

$$K = \{f \in F^n : f = g * h, h \in F^n\} = (g)$$

(ii) Polynómy $g(x), x * g(x), \dots x^{k-1} * g(x)$ *tvoria bázu* K.

(iii) $g(x) \mid x^n - 1$ *v okruhu* $F[x]$.

Takýto polynóm $g(x)$ *voláme* generujúcim polynómom *cyklického kódu.*

$$\mathbb{G} = \begin{pmatrix} g_0 & g_1 & \dots & g_{n-k} & 0 & \dots & 0 \\ 0 & \ddots & \ddots & & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \ddots & 0 \\ 0 & \dots & 0 & g_0 & g_1 & \dots & g_{n-k} \end{pmatrix}$$

Definícia 17. Nech $x^n - 1 = g(x).h(x)$ v $F[x]$ a nech $K \subseteq F^n$ je cyklický kód s generujúcim polynómom $g(x)$. Potom $h(x)$ voláme kontrolným polynómom kódu K.

$$\mathbb{H} = \begin{pmatrix} 0 & \dots & \dots & 0 & h_k & \dots & h_1 & h_0 \\ 0 & \dots & 0 & h_k & \dots & h_1 & h_0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & h_k & \dots & h_1 & h_0 & 0 & \dots & 0 \\ h_k & \dots & h_1 & h_0 & 0 & \dots & \dots & 0 \end{pmatrix}$$

Bez toho, aby sme veľa museli rozmýšľať. Lebo tam jedná sa o toto.
Katriňák

6 Grafy a ich základné vlastnosti

Grafy a ich základné vlastnosti. Minimálna cesta v grafe, algoritmus na minimálnu kostru. Fordov-Fulkersonov algoritmus, Hallova veta. Lineárny faktor, zložitosť algoritmov. Problém obchodného cestujúceho. Problém čínskeho poštára.

Pri príprave tejto otázky sa okrem poznámok z predmetov Teória grafov a Lineárne programovanie a grafové algoritmy použila aj kniha [PL].

6.1 Grafy a ich základné vlastnosti

Graf - (V, E)
Kyšova terminológia: Graf = neorientovaný, pseudograf = pripúšťajú sa slučky, multigraf = aj paralelné hrany.
Digraf = aj orientácia hrán (E je množina usporiadaných dvojíc)
orientovaný graf = taký, ktorý získame z obyčajného grafu doplnením orientácie hrán
U Plesníka bola terminológia podobná, ibaže multigraf nemal slučky a v pseudografe boli povolené. Migraf bol graf, ktorý mal orientované aj neorientované hrany.
izomorfizmus grafov, stupeň vrchola
Podgraf, indukovaný podgraf (indukovaný množinou vrcholov), faktor (podgraf s rovnakou množinou vrcholov ako má celý graf)
kompletný graf
turnaj = kompletný asymetrický digraf
regulárny graf stupňa k, regulárny digraf stupňa k = vchádzajúci aj vychádzajúci stupeň každého vrchola je k
sled, ťah (neopakujú sa hrany), cesta (neopakujú sa vrcholy)

uzavretý sled, uzavretý ťah, kružnica (cyklus)
súvislý graf, komponenty
excentricita, polomer, priemer, centrum
bipartitný graf

Nevedel som, kde dať Mengerovu vetu, ale zdalo sa mi, že je dosť dôležitá, takže niekde by byť mala. Zatiaľ som ju dal sem. (Separátor som nedefinoval, to sa snáď dá domyslieť z kontextu.)

Veta 1 (Menger–hranová verzia pre digrafy). *Ak u, v sú 2 rôzne vrcholy digrafu D, tak maximálny počet hranovo disjunktných u–v ciest v D sa rovná počtu hrán minimového u–v hranového separátora.*

Veta 2 (Menger–hranová verzia pre grafy). *Ak u, v sú 2 rôzne vrcholy grafu G, tak maximálny počet hranovo disjunktných u–v ciest v G sa rovná počtu hrán minimového u–v hranového separátora.*

Veta 3 (Menger–vrcholová verzia pre digrafy). *Ak u, v sú 2 rôzne vrcholy digrafu D, $uv \notin E(D)$, tak maximálny počet vrcholovo disjunktných u–v ciest v D sa rovná počtu vrcholov minimového u–v vrcholového separátora.*

Podobne vyzerá vrcholová verzia pre grafy.

6.2 Hľadanie najkratšej cesty

Úloha: Nájsť cestu z s do t s minimálnym súčtom ohodnotení.

Moorov algoritmus

Moorov algoritmus rieši túto úlohu v prípade, že každá hrana má ohodnotenie $c_{ij} = 1$. Vždy pridávame vrcholy, do ktorých sa dá dostať z tých, ktoré sme pridávali v poslednom kroku. Každý vrchol dostane značku len raz, čiže stačí $O(m + n)$ operácií. (tzv. postup do šírky)

Dijkstrov algoritmus

Dijkstrov algoritmus predpokladá, že $c_{ij} \geq 0$.
S = vrcholy s trvalou značkou
$\overline{S}$ = vrcholy s dočasnou značkou
Na začiatku $S = \{s\}$, vždy pre vrchol $v \in \overline{S}$ udržiavame v jeho značke dĺžku minimálnej cesty do v cez vrcholy patriace do S a posledný vrchol tejto cesty. (Na začiatku sa značky inicializujú tak, že s má značku 0 a ostatné vrcholy ∞.) V každom kroku pridávame vrchol z $\overline{S}$, ktorý má najmenšiu značku.

Zložitosť: $O(n^2)$. (Dá sa použitím haldy zmodifikovať na $O(m \lg n)$.)

6.3 Algoritmus na minimálnu kostru

Strom = súvislý acyklický graf.

Faktor súvislého grafu, ktorý je stromom, nazveme *kostrou*.

Ak $V_1 \subseteq V$, tak množinu všetkých hrán, ktorých jeden koncový vrchol patrí do V_1 a druhý do $V \setminus V_1$ nazveme *hranový rez*.

Veta 4. *Hrana e patrí do minimálnej kostry práve vtedy, keď e je najlacnejšou hranou nejakého rezu.*

Všeobecný spájací algoritmus (Tarjanov)

Vždy máme zostrojený les (na začiatku sú všetky stromy jednobodové). Vyberieme niektorý z doteraz vytvorených stromov a pridáme najlacnejšiu hranu idúcu z tohto stromu do iného stromu.

Primov algoritmus

Vždy vyberieme najväčší strom (teda vlastne budeme mať len jeden strom) a pridáme najlacnejšiu hranu, ktorá z neho vychádza. Zložitosť: $O(n^3)$. Ak si pre vytvorený strom pamätáme najlacnejšiu hranu, ktorú môžeme pridať a po každom kroku túto informáciu aktualizujeme, môžeme získať $O(n^2)$ algoritmus.

Kruskalov algoritmus

Usporiadame hrany vzostupne podľa ceny a potom ich v takom poradí postupne pridávame, pri každom pridávaní hrany testujeme, či nevznikne cyklus. Usporiadanie trvá $O(m \lg m)$ a detekcia sa dá robiť v čase $O(m \lg n)$ (spolu cez všetky hrany).

6.4 Siete a toky

Sieť = digraf, v ktorom sú vyznačené zdroj s, ústie t a každej hrane je priradené celé číslo - kapacita hrany.

Tok je funkcia $f\colon E \to \mathbb{R}$ taká, že

(i) $0 \leq f(a) \leq c(a)$,

(ii) $\sum_{y \in N^+(x)} f(x,y) = \sum_{y \in N^-(x)} f(y,x)$ pre $x \neq s,t$.

s-t rez je taký rozklad vrcholovej množiny na dve množiny S a T, že $s \in S$, $t \in T$. *Kapacita rezu* $b(S,T)$ = súčet kapacít všetkých hrán, ktoré majú počiatočný vrchol v S a konečný v T.

Veta 5. *Nasledujúce výroky sú ekvivalentné:*

(i) *f je maximálny $s-t$ tok.*

(ii) *Neexistuje zväčšujúca $s-t$ polocesta.*

(iii) *Existuje $s-t$ rez (S,T) taký, že $v(f) = b(S,T)$, kde $v(f)$ označuje veľkosť toku f, t.j. $v(f) = \sum_{y \in N^+(s)} f(s,y) - \sum_{y \in N^-(s)} f(y,s)$.*

Dôsledok 1. *Nech N je sieť definovaná na digrafe D s ústím t a zdrojom s. Potom veľkosť maximálneho $s-t$ toku sa rovná kapacite minimálneho $s-t$ rezu.*

Nasledujúce vety sa dajú dokazovať aj pomocou tokov.

Veta 6 (Hall). *Systém rozličných reprezentantov množín $S_1, \ldots, S_n$ existuje práve vtedy, keď zjednotenie ľubovoľných k množín má aspoň k prvkov.*

Veta 7 (König, Egerváry). *Maximálny počet nezávislých hrán párneho grafu sa rovná minimálnemu počtu vrcholov, ktoré pokryjú všetky hrany grafu.*

Fordov-Fulkersonov algoritmus

Vlastne len označujeme vrcholy, do ktorých sa dá dostať po rezervných (zväčšujúcich) polocestách. Ak sa podarí označkovať vrchol t, zväčšíme tok pomocou rezervnej polocesty a postup opakujeme. V prípade celočíselných kapacít algoritmus musí skončiť. Fordov-Fulkersonov algoritmus nie je polynomiálny, hoci sa v praxi ukazuje pomerne rýchly.

6.5 Lineárny faktor

Definícia 1. *Faktor grafu* = podgraf, ktorý obsahuje všetky vrcholy.
r-faktor = faktor, ktorý je regulárny stupňa r.
Nepárny komponent grafu = komponent, ktorý má nepárny počet vrcholov.

Veta 8 (Tutte). *Graf $G(V, E)$ má 1–faktor $\Leftrightarrow$ ak pre každú podmnožinu S množiny $V(G)$ je počet nepárnych komponentov grafu $G - S$ najviac $|S|$.*

Párenie

Dve hrany sú *nezávislé,* ak nemajú spoločný vrchol. *Párenie* je množina nezávislých hrán grafu G.
maximálne párenie, najpočetnejšie párenie
kompletné párenie = perfektné párenie – obsahuje všetky vrcholy
Voľný vrchol= nie je koncový vrchol žiadnej hrany párenia.
Alternujúca cesta je cesta, ktorej hrany striedavo patria a nepatria do párenia. Alternujúca cesta sa nazýva *zväčšujúcou cestou,* ak koncové vrcholy sú voľné vzhľadom na dané párenie.

Veta 9 (Berge). *Párenie M v grafe G je najpočetnejšie $\Leftrightarrow$ ak v G nie je zväčšujúca polocesta vzhľadom na M.*

6.6 Zložitosť algoritmov

$g = O(f(n))$, ak existujú n_0 a c také, že pre $n > n_0$ je $g(n) \leq cf(n)$.
$O(n)$ = lineárna zložitosť
$O(\lg n)$ = logaritmická zložitosť
$O(n^k)$ = polynomiálna zložitosť
$O(a^n)$ = exponenciálna zložitosť

6.7 Úloha čínskeho poštára a úloha obchodného cestujúceho

Úloha čínskeho poštára

eulerovský sled = uzavretý sled obsahujúci všetky hrany a vrcholy
Úloha: V danom silne súvislom grafe G, kde každá hrana má reálnu dĺžku $c_{ij} \geq 0$, treba nájsť najkratší eulerovský sled. (Poštár má prejsť všetky ulice mesta.)

V eulerovskom grafe je riešením ľubovoľný eulerovský ťah. Inak treba násjť popárovanie všetkých vrcholov nepárneho stupňa pomocou ciest, tak aby súčet ohodnotení týchto ciest bol minimálny. (Nech V_1 je množina vrcholov nepárneho stupňa. Pre $u, v \in V_1$ nájdeme najkratšiu cestu. Na V_1 vytvoríme kompletný graf s ohodnotením d_{uv}= minimálna dĺžka $u - v$ cesty. V takomto grafe sa vytvorí najlacnejšie párovanie - na to existuje algoritmus. Hrany z tohoto párenia pridáme k pôvodnému grafu. Eulerovský ťah v takto získanom grafe zodpovedá najlacnejšiemu eulerovskému sledu v pôvodnom grafe.)

Úloha obchodného cestujúceho

V grafe s nezápornými reálnymi ohodnoteniami hrán nájsť najkratší hamiltonovský cyklus. Je to NP-ťažký problém.

No tak nebudeme si to písať..., ale napíšeme si to.
Gliviak

7 Rovinné a hamiltonovské grafy

Rovinné grafy, Eulerova rovnosť. Farbenie grafov, veta o piatich farbách. (Kružnice v grafoch, hamiltonovské ideály, Chvátalova veta. Stabilita a uzáver grafov. Hamiltonovské kružnice a zakázané podgrafy. Hamiltonovské kružnice a hranové grafy eulerovských grafov.) [Ramseyho problém, Hamiltonovské problémy. Oreho veta.]

Po aktualizácii štátnicových otázok bola vynechaná časť v zátvorke a pribudli Ramseyho problém, Hamiltonovské problémy a Oreho veta. Hamiltonovské problémy a Oreho veta sú v tejto otázke. Ramseyho som nechal v 9. otázke, kde bol pôvodne.

7.1 Planárne (rovinné) grafy

Definícia 1. *Planárne (rovinné) grafy* sú grafy, ktoré sa dajú vnoriť do roviny. (Ekvivalentná podmienka je, že graf možno vnoriť do gule.)

Stena planárneho vnorenia obsahujúca bod x disjunktný s G je množina všetkých bodov roviny, ktorú je možné spojiť s x krivkou pozostávajúcou len z bodov disjunktných s G. *Hranica steny* je množina všetkých bodov x grafu, ktoré je možné spojiť s ľubovoľným bodom steny krivkou, ktorej všetky body okrem x sú disjunktné s grafom. *Dĺžka hranice* je počet hrán hranice danej steny, pričom ak je hrana mostom, tak sa počíta dvakrát.

Veta 1 (Euler). *Pre súvislý planárny graf platí*

$$p - q + r = 2,$$

kde p je počet vrcholov, q je počet hrán a r je počet stien. (Alebo, ak sa vám to tak lepšie pamätá, $v - h + s = 2$.)

Ak je planárny graf G nesúvislý a má $k(G)$ komponentov, tak $p - q + r = 1 + k(G)$.

Eulerova veta sa dokáže indukciou vzhľadom na počet hrán grafu na n vrcholoch.

Existuje práve 5 typov pravidelných mnohostenov (štvorsten, kocka, 8-, 12- a 20-sten.)

Pre počet hrán planárneho grafu platí $q \leq 3p - 6$. Ak neobsahuje trojuholník, tak $q \leq 2p - 4$. (Pomocou týchto nerovností môžeme overiť, že $K_{3,3}$ a K_5 nie sú planárne. Tiež z nich vyplýva, že každý rovinný graf musí obsahovať vrchol stupňa nanajvýš 5.)

Definícia 2. G_1 a G_2 sú *homeomorfné*, ak sú izomorfné alebo obidva grafy možno dostať z toho istého grafu G postupným opakovaním operácie delenia hrán.

Ekvivalentná definícia: Sú izomorfné alebo jeden možno dostať z druhého opakovaním operácií delenia hrany alebo odstránenia vrchola stupňa 2.

Veta 2 (Kuratowského). *Graf je planárny práve vtedy, keď neobsahuje podgraf homeomorfný s K_5 alebo $K_{3,3}$.*

Veta 3 (Wagner, Tutte, Harary - duálna Kuratowského). *Graf je planárny práve vtedy, keď nemá podgraf, ktorý sa dá stiahnuť elementárnou redukciou (t.j. spájaním susedných vrcholov) na K_5 alebo $K_{3,3}$.*

7.2 Farbenie grafu

$\chi(G)$ = *chromatické číslo* = minimálny počet farieb, ktorými sa dá ofarbiť G tak, aby každé dva susedné vrcholy mali rôznu farbu.
$\chi(G) \geq \omega(G)$ ($\omega(G)$ =klikové číslo = veľkosť najväčšieho kompletného podgrafu)
$\chi(G) \leq 1 + \Delta(G)$

Tvrdenie 1 (Szekeres, Will). *Pre ľubovoľný graf G platí*

$$\chi(G) \leq 1 + \max_{G' \subseteq G} \delta(G'),$$

kde maximum sa berie cez všetky indukované podgrafy G' grafu G.

Veta 4 (Brooks). *Nech G je súvislý graf s maximálnym stupňom Δ. Nech G nie je kompletný ani nepárny cyklus (alebo: G nie je kompletný a $\Delta \geq 3$). Potom $\chi(G) \leq \Delta$.*

Veta 5 (Gallai). *$\chi(G) \leq 1 + m(G)$, kde $m(G)$ je dĺžka najdlhšej cesty v G.*

Veta 6 (Kelly, Zykov). *$\frac{p}{\beta} \leq \chi(G) \leq p - \beta + 1$, kde β je mohutnosť najväčšej nezávislej množiny vrcholov.*

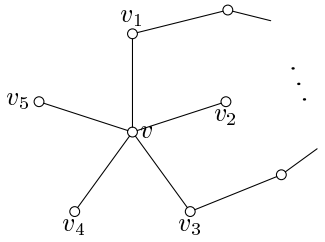
Tvrdenie 2. *Ak G neobsahuje P_4 ako indukovaný podgraf, tak $\chi(G) = \omega(G)$.*

Veta 7. *Pre ľubovoľné kladné celé n existuje n-chromatický graf bez trojuholníkov.*

Veta 8 (4CT). *Každý planárny graf možno ofarbiť 4 farbami.*

Veta 9 (5CT). *Každý rovinný graf je 5-farbiteľný.*

Dôkaz. Nech p je najmenšie také, že to neplatí a nech G je rovinný graf na p vrcholoch, ktorý nie je 5-farbiteľný. V G existuje vrchol stupňa najviac 5 (to vyplýva z odhadu pre počet hrán rovinného grafu $q \leq 3p - 6$). Po vynechaní tohto vrchola v dostaneme 5-farbiteľný graf. $H_{1,3}$ označíme podgraf indukovaný vrcholmi farieb 1 a 3. Ak v_1 a v_3 nie sú spojené v $H_{1,3}$ cestou, tak môžeme zameniť farby 1 a 3 v komponente obsahujúcom v_1. V opačnom prípade nebudú spojené cestou v_2 a v_4 v $H_{2,4}$. □



Farbenie hrán

$\chi_1(G)$ - *chromatický index* = najmenší počet farieb, ktorými je možné ofarbiť hrany G tak, aby susedné hrany nemali rovnakú farbu.

Veta 10 (Vizing). *Ak G je neprázdny, tak $\Delta(G) \leq \chi_1(G) \leq \Delta(G) + 1$.*

Grafy môžeme rozdeliť do 2 tried: $\chi_1(G) = \Delta(G)$ (trieda 1) a $\chi_1(G) = \Delta(G) + 1$ (trieda 2). Erdös a Wilson ukázali, že $P(G \in \text{Trieda 1}) \to 1$, t.j. skoro každý graf je z triedy 1.

Tvrdenie 3. $\chi_1(K_{m,n}) = \Delta = \max(m, n)$.

Veta 11 (König). *Ak G je párny, tak $\chi_1(G) = \Delta$.*

Veta 12. *Každá kubická mapa (t.j. planárny graf s $\deg v = 3$ pre všetky $v \in G$) sa dá hranovo ofarbiť 3 farbami $\Leftrightarrow$ platí 4CT.*

7.3 Eulerovské a hamiltonovské grafy

Eulerovské grafy

Veta 13. *Pre súvislý graf sú nasledovné tvrdenia ekvivalentné:*

(i) G je eulerovský (má eulerovský cyklus).

(ii) Každý vrchol G je párneho stupňa.

(iii) G je zjednotením hranovo disjunktných kružníc.

Hamiltonovské grafy

Graf voláme hamiltonovský, ak obsahuje hamiltonovskú kružnicu. Problém nájsť v grafe hamiltonovskú kružnicu, resp. zistiť, či je daný graf hamiltonovský, je NP-úplný.

Nutná podmienka, aby bol graf hamiltonovský: Pre každú podmnožinu $S \subset V(G)$ je počet komponent $G \setminus S$ $c(G \setminus S) \leq |S|$. (Ako dôsledok dostaneme, že každý hamiltonovský graf je 2-súvislý.)

Veta 14 (Dirac). *Ak minimálny stupeň grafu je $\frac{p}{2}$ (p je počet vrcholov), tak je to hamiltonovský graf.*

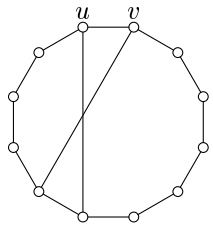
Veta 15 (Ore). *Ak G je graf s p vrcholmi ($p \geq 3$) taký, že pre každú dvojicu nesusedných vrcholov u, v platí*

$$\deg u + \deg v \geq p,$$

tak G je hamiltonovský.

Veta 16 (Bondy-Chvátal). *Nech u, v sú dva rôzne nesusedné vrcholy grafu G s p vrcholmi také, že $\deg u + \deg v \geq p$. Potom $G + uv$ je hamiltonovský $\Leftrightarrow$ G je hamiltonovský.*

Pri dôkaze Bondy-Chvátalovej vety si stačí uvedomiť, že musí existovať modifikujúca dvojica hrán



Uzáver grafu: Ak súčet stupňov dvoch nesusedných vrcholov je väčší alebo rovný p, tak pridám medzi nimi hranu. G je hamiltonovský $\Leftrightarrow$ jeho uzáver $c(G)$ je hamiltonovský.

7.4 Hamiltonovské ideály

Definícia 3. Nech $S = (d_1, \ldots, d_n)$ je postupnosť celých nezáporných čísel. Postupnosť S nazveme *grafovou,* ak existuje graf G taký, že $V(G) = \{v_1, \ldots, v_n\}$, $d_i = \deg v_i$ pre každé i.

Uvažujme o grafe G, kde $|V(G)| = n$, $S = (d_1, \ldots, d_n)$, $d_1 \leq \ldots \leq d_n$.

Definícia 4. Grafovú postupnosť S nazveme *silne hamiltonovskou*, ak každý graf s touto postupnosťou je hamiltonovský.

$$\deg v \geq \frac{n}{2} \qquad \forall v \in V(G) \tag{D}$$

$$|\{v; \deg v \leq j\}| < j \text{ pre } j < \frac{n-1}{2}, \text{ ak } n \text{ je nepárne } |\{v; \deg v \leq \frac{n-1}{2}\}| \leq \frac{n-1}{2} \tag{P}$$

$$(j \leq k, d_j \leq j, d_k \leq k-1) \Rightarrow d_j + d_k \geq n \tag{B}$$

$$d_j \leq j < \frac{n}{2} \Rightarrow d_{n-j} \geq n - j \tag{CH}$$

(D) = Diracova podmienka, (P) = Pósova, (B) = Bondyho, (CH) = Chvátalova
(D) $\Rightarrow$ (P) $\Rightarrow$ (B) $\Rightarrow$ (CH)

Označme S_n = neklesajúce grafové postupnosti dĺžky n, H_n = hamiltonovské postupnosti dĺžky n.

Definícia 5. Nech S, S^* sú prvky S_n. Hovoríme, že S^* *dominuje* S (označujeme $S^* \geq S$) ak pre každé i je $d_i \leq d_i^*$. $(S_n, \leq)$ je čiastočne usporiadaná množina.

$P \subseteq S_n$ nazveme *ideálom*, ak platí $(x \in P, x \leq y) \Rightarrow y \in P$.

H_n netvoria ideál v S_n.

Veta 17. *Ak S nevyhovuje podmienke (CH), tak existuje S^* taká, že $S^* \geq S$ a S^* nie je hamiltonovská.*

Dôsledok 1. *Najväčší ideál P^* v množine silne hamiltonovských postupností obsahuje len také postupnosti, ktoré vyhovujú (CH).*

Postupnosti spĺňajúce Oreho podmienku netvoria ideál. Ak graf spĺňa Oreho podmienku, tak spĺňa aj Chvátalovu.

Veta 18 (Chvátal). *Nech G je graf rádu n s postupnosťou stupňov vrcholov $d_1 \leq \ldots \leq d_n$ spĺňajúcou (CH). Potom G je hamiltonovský.*

7.5 Hamiltonovské kružnice a zakázané podgrafy

Veta 19 (Tutte). *Každý 4-súvislý planárny graf je hamiltonovský.*

Definícia 6. Graf nazveme *H-voľný*, ak neobsahuje indukovaný podgraf izomorfný s H. Graf G nazveme *lokálne súvislý,* ak okolie každého vrchola $v \in V(G)$ indukuje súvislý graf.

Veta 20 (Oberty, Summer). *Nech G je graf rádu $n \geq 3$, súvislý a lokálne súvislý, $K_{1,3}$-voľný. Potom G je hamiltonovský.*

7.6 Hranové grafy a hamiltonovské kružnice

Definícia 7. Graf G nazveme *hranovým grafom* grafu H, ak platí $V(G) = E(H)$, $E(G) = \{(e, f), e \cap f \neq \emptyset$ v grafe $H, e \neq f\}$. Označujeme $G = L(H)$.

Tvrdenie 4. *$G \cong L(G)$, G je súvislý $\Leftrightarrow G = C_n$.*

Nech G, G' sú súvislé grafy, $L(G) \cong L(G')$. Potom $G \cong G'$ okrem prípadu $G = C_3$, $G' = K_{1,3}$.

Veta 21 (Beineke). *Graf G je hranovým grafom práve vtedy, keď neobsahuje indukovaný podgraf izomorfný s $K_{1,3}, F_2, \ldots, F_9$. (Teda každý hranový graf je $K_{1,3}$-voľný.)*

Veta 22. *Graf G je hranovým grafom práve vtedy, keď existuje rozklad $E(G)$ na kompletné podgrafy tak, že každý $v \in V(G)$ patrí do najviac dvoch.*

Veta 23. *Nech G je súvislý graf. Potom G je hranový graf eulerovského grafu práve vtedy, keď existuje rozklad $E(G)$ na kompletné podgrafy párneho rádu (každý kompletný podgraf má párny počet vrcholov) tak, že každý vrchol $v \in V(G)$ patrí do práve dvoch.*

Tvrdenie 5. *Hranový graf eulerovského grafu je hamiltonovský.*

Dôsledok 2. *Ak súvislý graf má rozklad s vlastnosťami uvedenými vo vete 23, potom G je hamiltonovský.*

A na tom dôkaze uvidíte, čo dokážeme.
Šalát

8 Grupy automorfizmov grafu

(Grupy automorfizmov grafu, vrcholovo a hranovo tranzitívne grafy. Fruchtova veta. Charakterizácia vrcholovo tranzitívnych grafov. Cayleyho grafy. Konštrukcia vrcholovo tranzitívnych grafov, ktoré nie sú Cayleyho grafmi. Cirkulantné grafy a hamiltonovské kružnice.)

Definícia 1. Nech $G = (V, E)$ je graf. Automorfizmom grafu G rozumieme každú bijekciu $\varphi\colon V \to V$ s vlastnosťou $(u, v) \in E$ práve vtedy, keď $(\varphi(u), \varphi(v)) \in E$ (t.j. izomorfizmus grafu na seba).

Veta 1. *Všetky automorfizmy grafu G tvoria grupu vzhľadom na operáciu skladania zobrazení, označujeme ju $Aut(G)$.*

Platí $Aut(G) = Aut(\overline{G})$. Pre Petersenov graf je $Aut(P) \cong S_5$.

Definícia 2. Na množine vrcholov V definujeme reláciu ekvivalencie $\sim$ tak, že $u \sim v \Leftrightarrow \varphi(u) = v$ pre nejaké $\varphi \in Aut(G)$. Triedy rozkladu $\theta(u) = \{\varphi(u); \varphi \in Aut(G)\}$ sa nazývajú *orbity* grupy $Aut(G)$.

Ak $Aut(G) = \{id\}$, čiže každá orbita je jednoprvková, hovoríme, že G je *vrcholovo antisymetrický*. Ak existuje jediná orbita, hovoríme, že G je *vrcholovo symetrický (vrcholovo tranzitívny)*.

Definícia 3. Každý automorfizmus $\varphi \in Aut(G)$ indukuje bijektívne zobrazenie $\varphi'\colon E \to E$. $\Gamma_1 = \{\varphi'; \varphi'$ je indukované automorfizmom $\varphi\}$ je *hranová grupa automorfizmov G*.

Veta 2. *$Aut(G) \cong \Gamma_1(G)$ práve vtedy, keď G neobsahuje K_2 ako komponentu súvislosti a má najviac jeden izolovaný vrchol.*

Definícia 4. Graf G nazveme *hranovo tranzitívny*, ak pre každé dve hrany $e, f \in E$ existuje $\varphi' \in \Gamma_1(G)$ tak, že $\varphi'(e) = f$.

Veta 3. *Nech G je hranovo tranzitívny graf bez izolovaných vrcholov. Potom G je vrcholovo tranzitívny alebo G je bipartitný a jeho bipartícia je tvorená dvoma vrcholovými orbitami.*

Dôsledok 1. *Nech G je hranovo tranzitívny graf, nepárneho rádu, regulárny stupňa $d \geq 1$. Potom G je vrcholovo tranzitívny.*

Dôsledok 2. *Nech G je hranovo tranzitívny graf, regulárny stupňa $d \geq \frac{|G|}{2}$. Potom G je vrcholovo tranzitívny.*

Veta 4 (Frucht). *Pre každú konečnú grupu Γ existuje graf G taký, že $\Gamma \cong Aut(G)$.*

8.1 Cayleyho grafy

Definícia 5. Nech Γ je grupa, $S \subseteq \Gamma$, $1 \notin S$, $S = S^{-1}$ (S je uzavretá vzhľadom na inverzné prvky). $G = C(\Gamma, S)$ je graf s $V(G) = \Gamma$ a $E(G) = \{(u, v) : u^{-1}v \in S\}$. Graf G nazývame *Cayleyho graf* grupy Γ vzhľadom na S.

Veta 5. *Cayleyho graf $C(\Gamma, S)$ je*

(i) kompletný graf $\Leftrightarrow$ $S = \Gamma \setminus \{1\}$,

(ii) súvislý graf $\Leftrightarrow$ S generuje Γ.

Veta 6. *Cayleyho graf $C(\Gamma, S)$ je vrcholovo tranzitívny.*

Petersenov graf nie je Cayleyho graf, ale je vrcholovo tranzitívny.

Sedím, sedím, až vysedím.
Tomanová

9 Extremálne úlohy

(Turánova veta, konečný prípad Ramseyovej vety. Grafové Ramseyove čísla, Chvátalova veta, $R(K_m, T_n) = (m-1)(n-1)+1$.)

9.1 Turánov problém

$\alpha(G)$ - číslo nezávislosti grafu G - je počet hrán najväčšej nezávislej množiny vrcholov G.
$E(n, k)$ - minimálny počet hrán grafu na n vrcholoch s $\alpha(G(n, k)) < k$.

Veta 1. *Grafy $G(n, k)$ s minimálnym počtom hrán $E(n, k)$, kde $3 \leq k \leq n$ sú tvaru $G(n, k) = G_1 \cup G_2 \cup \ldots \cup G_{k-1}$. Ak $n = t(k-1) + r$, $0 \leq r < k-1$, tak r z grafov G_i sú K_{t+1} a zvyšné sú K_t.*

Veta 2 (Turán). *Existuje jediný graf rádu $n \geq 3$, ktorý neobsahuje podgraf K_k, $3 \leq k \leq n$ a má maximálny počet hrán.*

9.2 Ramseyove čísla

Nech $p, q \geq 2$ sú celé čísla. Číslo $N > 0$ nazveme (p, q)-ramseyovské, ak pre ľubovoľný rozklad množiny všetkých dvojprvkových podmnožín množiny S (S je N-prvková) na dve časti X, Y existuje p-prvková podmnožina množiny S taká, že všetky jej dvojprvkové podmnožiny patria do X alebo existuje q-prvková podmnožina S taká, že všetky jej dvojprvkové podmnožiny patria do Y.

Veta 3 (Ramsey). *Nech $p, q \geq 2$ sú celé čísla. Potom existuje celé číslo $N > 0$, ktoré je (p, q)-ramseyovské.*

Najmenšie (p, q)-ramseyovské číslo nazývame *Ramseyove číslo* $R(p, q)$.

Tvrdenie 1. *Číslo N je (p, q)-ramseyovské práve vtedy, keď pre každý graf G rádu N platí, že G obsahuje K_p alebo G obsahuje $\overline{K_q}$. (Ekvivalentne: Pri ľubovoľnom ofarbení hrán grafu K_N modrou a červenou farbou nájdeme modré K_p alebo červené K_q.)*

Tvrdenie 2. $R(p, 2) = p$
$R(3, 3) = 6$
$R(p, q) = R(q, p)$

Veta 4 (Erdös, Szekeres). *Nech $p, q \geq 3$ sú celé čísla. $R(p, q) \leq R(p-1, q) + R(p, q-1)$.*

Dôsledok 1. *Nech $p, q \geq 2$ sú celé. $R(p, q) \leq \binom{p+q-2}{p-1}$.*

Tvrdenie 3. *Nech $R(p, q-1)$ a $R(p-1, q)$ sú párne čísla. Potom $R(p, q) \leq R(p-1, q) + R(p, q-1) - 1$.*

Tvrdenie 4 (Erdös). $R(k, k) \geq 2^{\frac{k}{2}}$

Dôsledok 2. *Nech $m = \min\{p, q\}$. Potom $R(p, q) \geq 2^{\frac{m}{2}}$.*

9.3 Grafové Ramseyove čísla

Definícia 1. Nech G_1, G_2 sú grafy, $|G_1|, |G_1| \geq 2$. Celé číslo $N \geq 0$ nazveme (G_1, G_2)-ramseyovské, ak pri ľubovoľnom rozklade množiny všetkých dvojprvkových podmnožín N-množiny na dve časti X_1, X_2 platí $G_1 \subseteq X_1$ alebo $G_2 \subseteq X_2$.

Najmenšie (G_1, G_2)-ramseyovské číslo označujeme $R(G_1, G_2)$.

Ekvivalentné formulácie: cez ofarbenia (modrý G_1 alebo červený G_2); každý graf rádu N obsahuje ako svoj podgraf G_1 alebo $\overline{G_2}$.

Veta 5 (Chvátal). *Nech T_m je strom rádu $m \geq 2$, nech $m \geq 2$ je celé číslo. Potom $R(T_m, K_n) = (m-1)(n-1) + 1$.*

Tvrdenie 5. *Nech G je graf rádu p, s chromatickým číslom $\chi(G)$ číslom nezávislosti $\alpha(G)$. Potom $\chi(G).\alpha(G) \geq p$. (Pozri vetu 6 z otázky 7.)*

Tvrdenie 6. *Nech T_m je ľubovoľný strom rádu $m \geq 1$, G je ľubovoľný graf s $\delta(G) \geq m - 1$ ($\delta(G)$ je minimálny stupeň G). Potom G obsahuje T_m ako svoj podgraf.*

Definícia 2. Graf G nazveme *kritický n-chromatický* ($n \geq 2$), ak $\chi(G) = n$ a $\chi(G - v) = n - 1$ pre každé $v \in G$.

Tvrdenie 7. *Ak G je kritický n-chromatický graf, tak $\delta(G) \geq n - 1$.*

Tvrdenie 8. *Ak $\chi(G) = n \geq 2$, potom G obsahuje kritický n-chromatický podgraf. (Stačí zobrať podgraf najmenšieho rádu s chromatickým číslom n.)*

Dôkaz vety 5. Nech G je ľubovoľný pevne zvolený graf rádu $(m-1)(n-1)+1$. Ukážeme, že obsahuje T_m alebo $\overline{K_n}$.

Nech G neobsahuje $\overline{K_n}$. Potom $\alpha(G) \leq n-1$.

$$\begin{aligned}\chi(G)\alpha(G) &\geq (m-1)(n-1)+1\\ \chi(G) &\geq \frac{(m-1)(n-1)+1}{\alpha(G)} \geq \frac{(m-1)(n-1)+1}{n-1} > m-1\\ k :=& \chi(G) \geq m\end{aligned}$$

Potom G obsahuje kritický k-chromatický podgraf $F \Rightarrow \delta(F) \geq k-1 \geq m-1$. Preto $\delta(G) \geq m-1$ a G obsahuje T_m ako svoj podgraf.

Ešte treba ukázať, že existuje graf na $(m-1)(n-1)$ vrcholoch, ktorý neobsahuje T_m ani $\overline{K_n}$. Je to graf, ktorý má $n-1$ komponent súvislosti tvaru K_{m-1}. □

Túto vetu vie skoro každý.
Skoro každý znamená každý až na množinu miery 0.
Do množiny miery 0 sa zmestí každá spočítateľná množina.
Šalát

10 Kombinatorika

(Enumeračné úlohy.) Vytvárajúce funkcie a ich použitie. Stirlingove čísla, rekurentné vzťahy. (Princíp zapojenia a vypojenia a jeho zovšeobecnenia. Spernerova veta. Chromatický polynóm grafu. Cyklový index grupy, Pólyova veta. Cayleyho veta. Hallova veta, Königova veta. Algoritmus na nájdenie systému rozličných reprezentantov.)

10.1 Vytvárajúce funkcie a ich použitie

$\sum a_n p_n(x)$ nazveme *vytvárajúcou funkciou* pre postupnosť a_n, ak $\operatorname{st} p_n(x) = n$, $p_n(x) \in R[x]$.
Používa sa: $p_n(x) = x^n$, $p_n(x) = \frac{x^n}{n!}$ (–tzv. exponenciálna vytvárajúca funkcia)
$(1+x)^n = \sum \binom{n}{k} x^k$ je vytvárajúca funkcia pre kombinácie
$(1 + x + x^2 + \ldots)^n$ - k-kombinácie s opakovaním z n-množiny
$(1+x)^n = \sum a_k \frac{x^k}{k!}$ - k-variácie bez opakovania z n-množiny
$1 + nx + n^2x^2 + \ldots = \frac{1}{1-nx}$ - k-variácie s opakovaním z n-množiny
Vytvárajúce funkcie sa používajú pri riešení rekurentných rovníc.

Rekurentné rovnice určené konvolúciou

Cauchyho súčin radov: $\sum a_n x^n . \sum b_n x^n = \sum c_n x^n$, $c_n = \sum_{i=0}^{n} a_i b_{n-i}$

Túto metódu sme použili na riešenie rekurencie $u_{n+1} = \sum_{k=0}^{n} u_k u_{n-k}$, $u_0 = 1$, ktorá udáva počet binárnych stromov na n vrcholoch. Výsledkom sú Catalanove čísla: $u_n = \frac{1}{n+1}\binom{2n}{n}$.

10.2 Stirlingove čísla

Nech $c(n,k)$ označuje počet permutácií $\pi \in S_n$, ktoré majú práve k cyklov (počítajú sa aj cykly dĺžky 1). Ďalej definujeme $c(0,0) = 1$ a $c(n,k) = 0$ ak $n \leq 0$ alebo $k \leq 0$, $(n,k) \neq (0,0)$.

Stirlingove čísla prvého druhu sú definované ako

$$s(n,k) = (-1)^{n-k} c(n,k)$$

Pre $n \geq 0$ platí:

$$c(n,k) = (n-1)c(n-1,k) + c(n-1,k-1)$$

$$\sum_{k=0}^{n} c(n,k)x^k = (x)^n = x(x+1)\dots(x+n-1)$$

$$\sum_{k=0}^{n} s(n,k)x^k = (x)_n = x(x-1)\dots(x-n+1)$$

Stirlingove čísla 2.druhu $S(n,k)$ = počet rozkladov n-prvkovej množiny na k častí.

Tvrdenie 1. *S(n,k)=kS(n-1,k)+S(n-1,k-1)*

$$x^n = \sum_{k=0}^{n} S(n,k)(x)_k \qquad (n \geq 0)$$

Bellove čísla $B(n)$ =počet všetkých rozkladov (ekvivalencií) n-prvkovej množiny

$B(n) = \sum_{k=0}^{n} S(n,k)$

$B(n+1) = \sum_{k=0}^{n} \binom{n}{k} B(k)$

V [LW] sú uvedené aj vytvárajúce funkcie pre Stirlingove čísla oboch druhov.

10.3 Rekurentné vzťahy

Lineárna homogénna rekurentná rovnica s konštantnými koeficientami:

$$a_n = c_1 a_{n-1} + \ldots + c_p a_{n-p}, \tag{10.1}$$

$c_1, \ldots, c_p$ sú konštanty, $p \leq n$. Ďalej sú dané $a_0, \ldots, a_{p-1}$ – počiatočné podmienky.

Rovnica $x^p - c_1 x^{p-1} - \ldots - c_p = 0$ je *charakteristická rovnica* pre (10.1), jej korene $\alpha_1, \ldots, \alpha_p$ sú *charakteristické korene.*

Ak máme dve riešenia rovnice (10.1), tak ich lineárna kombinácia je tiež riešenie.

Ku koreňu α násobnosti k prislúchajú riešenia $\alpha^n, n\alpha^n, \ldots, n^{k-1}\alpha^n$.

10.4 Princíp zapojenia a vypojenia

Tvrdenie 2. *Nech S je N-množina a $E_1, \ldots, E_r$ podmnožiny S. Pre každú podmnožinu M množiny $\{1, \ldots, r\}$ definujeme $N(M)$ ako počet prvkov S v $\bigcap_{i \in M} E_i$ a pre $0 \leq j \leq r$ definujeme $N_j := \sum_{|M|=j} N(M)$. Potom počet prvkov S, ktoré nie sú v žiadnej z podmnožín E_i je $N - N_1 + N_2 - N_3 + \ldots + (-1)^r N_r$.*

TODO ?Zovšeobecnenia

10.5 Spernerova veta

Tvrdenie 3. *Maximálna veľkosť antireťazca v $\mathcal{P}(N)$, kde $N = \{1, 2, \ldots n\}$ je $\binom{n}{\lfloor n/2 \rfloor}$.*

TODO Chromatický polynóm

10.6 Pólyova teória

Definícia 1. Nech A je množina a G je grupa permutácií na A.
$Stab(a) = \{\pi \in G; \pi(a) = a\}$
$Inv(\pi) = \{a \in A; \pi(a) = a\}$
Pre $a, b \in A$ definujeme $a \sim b \Leftrightarrow (\exists \pi \in G)\pi(a) = b$.
$\theta(a) = \{b \in A; a \sim b\}$ je *orbita* grupy G.

Lema 1. *Ak $a \sim b$, tak $|Stab(a)| = |Stab(b)|$. Pre každé $a \in A$ platí $|G| = |Stab(a)||\theta(a)|$.*

Veta 1 (Burnsidova lema). *Nech G je grupa permutácií na A, $N(G)$ je počet orbít grupy G. Potom*

$$N(G) = \frac{1}{|G|} \sum_{\pi \in G} |Inv(\pi)|$$

(počet orbít je priemerný počet pevných bodov pre permutácie z G).

D je množina, G je grupa permutácií na D.
$C(D, R) = \{f \colon D \to R\}$
$\pi^*(f) = g$; $f(\pi(x)) = g(x)$
π^* je permutácia na $C(D, R)$
$f \sim^* g \Leftrightarrow (\exists \pi \in G)\pi^*(f) = g$
$\sim^*$ je ekvivalencia na $C(D, R)$
$G^* = \{\pi^*; \pi^* \in G\}$
$(G^*, \circ)$ je grupa, $|G^*| = |G|$, platí teda

$$N(G^*) = \frac{1}{|G|} \sum_{\pi \in G} |Inv(\pi^*)|$$

($f \in Inv(\pi^*) \Leftrightarrow f$ je konštantná na každom cykle π)

Každému $\pi \in G$ priradíme polynóm $x_1^{b_1} \dots x_n^{b_n}$, kde b_i je počet cyklov dĺžky i v rozklade π. *Cyklový index* grupy G je

$$Z(G) = \frac{1}{|G|} \sum_{\pi \in G} x_1^{b_1} \dots x_n^{b_n}.$$

Cyklové číslo $cyc(\pi)$ permutácie π je počet cyklov v rozklade π na disjunktné cykly. ($b_1 + \dots + b_n$)

Veta 2 (Špeciálny prípad Pólyovej vety). *Nech G je grupa permutácií na D, nech R je množina, $|R| = m$, $C(D, R) = \{f; f \colon D \to R\}$. Potom*

$$N(G^*) = \frac{1}{|G|} \sum_{\pi \in G} m^{cyc(\pi)}.$$

Iný tvar: ak označíme $c_k(G)$ počet permutácií z G, ktoré majú v rozklade práve k cyklov, tak

$$N(G^*) = \frac{1}{|G|} \sum_{k=1}^{\infty} c_k(G) m^k.$$

Vyjadrenie pomocou cyklového indexu:

$$N(G^*) = Z(m, m, \dots, m)$$

Veta 3 (Ohraničená Burnsidova lema). *Nech G je grupa permutácií na A, Y je zjednotenie nejakých orbít grupy G. Nech $G|Y$ označuje permutácie zúžené na Y. Potom*

$$N(G|Y) = \frac{1}{|G|} \sum_{\pi \in G} |Inv(\pi|Y)|$$

???

Ak navyše definujeme váhovú funkciu $w\colon R \to \mathbb{N}_0$ a definujeme $w(f) = \sum_{d \in D} w(f(d))$, tak všetky prvky ľubovoľnej orbity majú rovnakú váhu. Ak označíme C_k počet orbít váhy k a $C(x) = \sum_{k=0}^{\infty} C_k x^k$ a $c(x) = \sum_{k=0}^{\infty} c_k x^k$, kde c_k je počet prvkov v R s váhou k, tak

Veta 4 (Pólya). *$C(x) = Z(G, c(x^r))$ (do cyklového indexu grupy G dosadíme za každú premennú $c(x^r)$).*

10.7 Cayleyho veta

Veta 5 (Cayley). *Počet neizomorfných označených stromov rádu $n > 2$ je rovný n^{n-2}.*

10.8 Systém rozličných reprezentantov

Definícia 2. Nech $A_1, \ldots, A_n$ je systém podmnožín množiny X. Potom $x_1, \ldots, x_n$ nazývame *systém rozličných reprezentantov (transverzála),* aj $x_i \in A_i$ pre $i = 1, \ldots, n$ a $x_i \neq x_j$ pre $1 \leq i < j \leq n$.

Veta 6 (Hall). *Systém rozličných reprezentantov pre $A_1, \ldots, A_n$ existuje práve vtedy, keď*

$$|A_{i_1} \cup \ldots \cup A_{i_k}| \geq k$$

pre ľubovoľné $1 \leq i_1 < \ldots < i_k \leq n$.

Veta 7 (Zovšeobecnenie Hallovej vety). *Nech $A_1, \ldots, A_n$ je systém podmnožín množiny X a nech $1 \leq r \leq n$. V systém $A_1, A_2, \ldots, A_n$ existuje r-množinový podsystém s transverzálou práve vtedy, keď pre každé $k = 1, 2, \ldots, n$ a pre každý výber $i_1, i_2, \ldots, i_k$ taký, že $1 \leq i_1 < i_2 \ldots i_k \leq n$ platí*

$$|A_{i_1} \cup A_{i_2} \cup \ldots \cup A_{i_k}| \geq k - (n - r).$$

Veta 8 (König). *Nech A je matica obsahujúca len 0 a 1. Minimálny počet riadkov A, ktoré obsahujú všetky jednotky je rovný maximálnemu počtu jednotiek v A takých, že žiadne dve neležia na jednom riadku.*

Veta 9 (König). *Počet hrán maximového párovania párneho grafu G je rovný minimálnemu počtu vrcholov vrcholového pokrytia G.*

Algoritmus na nájdenie systému rozličných reprezentantov = ?
Použitá literatúra: [LW], [KN].

Je to prirovnanie, ktoré kríva na všetky štyri nohy, pokiaľ ich má.
Korbaš

11 Logika 0. rádu

Výrokový počet, výrokové formy, dokázateľnosť, interpretácie, tautológie, veta o úplnosti. Boolovské algebry, filtre a ich súvis s výrokovým počtom.

11.1 Výrokový počet

Definícia 1. *Výrokové formy* – $VF(P)$ je najmenšia množina konečných postupností znakov jazyka výrokového počtu (t.j. premenné (prvky P), logické spojky a pomocné znaky (zátvorky)) taká, že

(i) $P \subseteq VF(P)$

(ii) Ak $A, B \in VF(P)$, tak $\neg A$, $(A \,\&\, B)$, $(A \Rightarrow B)$, $(A \Leftrightarrow B)$ patria do $VF(P)$.

Interpretácia je ľubovoľné zobrazenie $I\colon VF(P) \to \{0,1\}$ také, že pre ľubovoľné $A, B \in VF(P)$ platí $I(\neg A) = \neg I(A)$, $I(A \,\&\, B) = I(A) \,\&\, I(B)$, ...

Definícia 2. Nech $A \in VF(P)$. Hovoríme, že

(i) A je *tautológia,* ak $I(A) = 1$ pre ľubovoľnú interpretáciu $I\colon VF(P) \to \{0,1\}$.

(ii) A je *splniteľná,* ak $I(A) = 1$ pre aspoň jednu interpretáciu $I\colon VF(P) \to \{0,1\}$.

(iii) A je *nesplniteľná,* ak $I(A) = 0$ pre každú interpretáciu $I\colon VF(P) \to \{0,1\}$.

(iv) A je *vyvrátiteľná,* ak $I(A) = 0$ pre aspoň jednu interpretáciu $I\colon VF(P) \to \{0,1\}$.

Definícia 3. *Teória* vo výrokovom počte je ľubovoľná množina $T \subseteq VF(P)$. Jej prvky sa nazývajú *axiómy* teórie T.

Logické axiómy a definíciu dôkazu v teórii T tu nebudeme vypisovať, je rovnaká ako v ďalšej otázke, s tým rozdielom, že tu nemáme axiómy kvantifikátorov a generalizáciu.

Definícia 4. Hovoríme, že $B \in VF(P)$ je *dokázateľná* v teórii T, ak existuje dôkaz $A_0, \ldots, A_n$ v T taký, že $A_n \equiv B$. Značíme $T \vdash B$.

Hovoríme, že $B \in VF(P)$ je *splnená* v teórii T ($T \models B$), ak pre každú interpretáciu teórie T platí $I(B) = 1$.

Veta 1 (korektnosť). *Ak $T \vdash B$, tak $T \models B$.*

Veta 2 (úplnosť). *Ak $T \models B$, tak $T \vdash B$.*

Veta 3 (slabá verzia vety o úplnosti). *Ak A je tautológia, tak $\vdash A$.*

Veta 4 (o dedukcii). *$T \cup \{A\} \vdash B$ práve vtedy, keď $T \vdash (A \Rightarrow B)$.*

Definícia 5. Teória T sa nazýva *sporná* (protirečivá, nekonzistentná), ak existuje nejaká $A \in VF(P)$ taká, že $T \vdash A$ aj $T \vdash \neg A$. V opačnom prípade sa T nazýva *bezosporná* (neprotirečivá, konzistentná).

Tvrdenie 1. *T je sporná práve vtedy, keď $T \vdash A$ pre každú výrokovú formu A.*

Pre $A \in VF(P)$ definujeme $A^I = \begin{cases} A, & \text{ak } I(A) = 1 \\ \neg A, & \text{ak } I(A) = 0 \end{cases}$

Tvrdenie 2 (Lema o interpretácii). *Nech $A \in VF(P)$ a $p_1, \ldots, p_n$ sú všetky výrokové premenné v A. Potom $\{p_1^I, \ldots, p_n^I\} \vdash A^I$.*

Definícia 6. Interpretácia teórie T = taká interpretácia, v ktorej má každá axióma teórie T pravdivostnú hodnotu 1.

Veta 5 (úplnosť). *Ak T je bezosporná, tak T má aspoň jednu interpretáciu.*

Definícia 7. Teória T sa nazýva *úplná,* ak je bezosporná a pre ľubovoľnú výrokovú formu platí $T \vdash A$ alebo $T \vdash \neg A$.

Úplná teória má práve jednu interpretáciu.

Tvrdenie 3. *Ku každej bezospornej teórii T existuje úplná $\overline{T} \supseteq T$.*

Veta 6 (o kompaktnosti). *Ak $T \vdash A$, tak existuje konečná $T_0 \subseteq T$ taká, že $T_0 \vdash A$.*
T je sporná práve vtedy, keď existuje konečná $T_0 \subseteq T$, ktorá je sporná.
T je bezosporná práve vtedy, keď každá konečná $T_0 \subseteq T$ je bezosporná.
T má interpretáciu práve vtedy, keď každá konečná $T_0 \subseteq T$ má interpretáciu.

11.2 Boolovské algebry

Definícia 8. *Boolovská algebra* je množina B s 2 binárnymi operáciami $\wedge$ (priesek), $\vee$ (spojenie), jednou unárnou operáciou $'$ (doplnok) a dvoma význačnými prvkami 0, 1 taká, že pre všetky $x, y, z \in B$ platí:

$x \wedge x = x$	$x \vee x = x$	idempotentnosť
$x \wedge y = y \wedge x$	$x \vee y = y \vee x$	komutatívnosť
$x \wedge (y \wedge z) = (x \wedge y) \wedge z$	$x \vee (y \vee z) = (x \vee y) \vee z$	asociatívnosť
$x \wedge (x \vee y) = x$	$(x \wedge y) \vee y = y$	zákony absorbcie
$0 \wedge x = 0$	$0 \vee x = x$	
$1 \wedge x = 1$	$1 \vee x = 1$	
$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$	$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$	distributívne zákony
$x \wedge x' = 0$	$x \vee x' = 1$	$x'' = x$
$0' = 1$	$1' = 0$	
$(x \wedge y)' = x' \vee y'$	$(x \vee y)' = x' \wedge y'$	

Definícia 9. Ak B je boolovská algebra, tak $S \subseteq B$ je *podalgebra* B, keď $0, 1 \in S$ a S je uzavretá na $\wedge$, $\vee$, $'$.

Ak A, B sú boolovské algebry, tak $h\colon A \to B$ je *homomorfizmus* boolovských algebier, ak zachováva operácie, doplnok, 0 a 1. *Izomorfizmus* je bijektívny homomorfizmus boolovských algebier.

Definícia 10. $J \subseteq B$ sa nazýva *ideál*, ak $J \neq \emptyset$ a

$$x \in J, y \leq x \Rightarrow y \in J,$$
$$x, y \in J \Rightarrow x \vee y \in J.$$

$F \subseteq B$ sa nazýva *filter (duálny ideál),* ak $F \neq \emptyset$ a

$$x \in F, y \geq x \Rightarrow y \in F,$$
$$x, y \in F \Rightarrow x \wedge y \in F.$$

J je ideál $\Leftrightarrow \{x', x \in J\}$ je filter.
F je filter $\Leftrightarrow \{x', x \in F\}$ je ideál.

Kongruencie na boolovských algebrách a faktorové boolovské algebry sa definujú rovnakým spôsobom ako pre ľubovoľné algebry. Je tu korešpondencia medzi filtrami a kongruenciami, definuje sa aj B/F, kde F je filter na B. Kongruencia prislúchajúca filtru F je $x \equiv_F y$ pvk $x \leftrightarrow y \in F$. $(x \leftrightarrow y = (x \to y) \wedge (y \to x))$

Veta 7 (Boolean Prime Ideal Theorem). *Nech B je ľubovoľná boolovská algebra, potom pre každé $0 \neq x \in B$ existuje ultrafilter F v B taký, že $x \in F$.*

Dôkaz predchádzajúcej vety sa robí pomocou princípu maximality.

Veta 8. *Nech B je ľubovoľná boolovská algebra. Označme I množinu všetkých ultrafiltrov v B. Zobrazenie $\varphi\colon B \to \mathcal{P}(I)$, kde*

$$\varphi(x) = \{i \in I; x \in i\}$$

je prostý homomorfizmus boolovských algebier. (Teda každá boolovská algebra je izomorfná s podalgebrou potenčnej algebry $\mathcal{P}(I)$ pre vhodné I.)

Tvrdenie 4. *$F \subseteq B$ je filter práve vtedy, keď $1 \in F$ a*

$$(\forall x, y \in B)(Ak\ x \in F, x \to y \in F\ tak\ y \in F),$$

kde $x \to y = x' \vee y$.

Definícia 11. $a \in B$ je *atóm*, ak $0 < a \,\&\, \neg(\exists x \in B)(0 < x < a)$ (teda $0 \prec a$).

B je *atomická*, ak pre každé $x \in B$ existuje a také, že $a \leq x$ a a je atóm. B je *bezatomická,* ak neobsahuje žiaden atóm.

Veta 9. *Ak B je atomická boolovská algebra a I je množina atómov v B, tak $h(x) = \{i \in I : i \leq x\}$ je prostý homomorfizmus boolovských algebier $h\colon B \to \mathcal{P}(I)$. (Každá atomická boolovská algebra je izomorfná s podalgebrou nejakej $\mathcal{P}(I)$.)*

Ultrafilter je maximálny vlastný filter.

Veta 10. *Nech F je filter v B. Nasledujúce podmienky sú ekvivalentné:*

(i) *F je ultrafilter.*

(ii) *$0 \notin F$ a $(\forall x, y \in B)(x \vee y \in F \Rightarrow x \in F$ alebo $y \in F)$.*

(iii) *Pre každé $x \in B$ F obsahuje práve jeden z prvkov x a x'.*

(iv) *$B/F \cong \{0, 1\}$.*

Súvis filtrov s výrokovým počtom

Ak na $VF(P)$ definujeme reláciu ekvivalencie $A \equiv B$ pvk $\vdash (A \Leftrightarrow B)$ a prirodzeným spôsobom definujeme operácie, dostaneme boolovskú algebru $\mathcal{B}(P)$.

Pre $T \subseteq VF(P)$ definujeme $A \equiv_T B$ pvk $T \vdash (A \Leftrightarrow B)$.
$VF(P)/\equiv_T =: \mathcal{B}(T)$
Dokázateľné formuly v T tvoria filter (obsahuje 1 a je uzavretý na modus ponens), označujeme ho $\mathcal{F}(T)$.

Tvrdenie 5. *T je sporná práve vtedy, keď $\mathcal{F}(T)$ je nevlastný.*
T je bezosporná práve vtedy, keď $\mathcal{F}(T)$ je vlastný.
T je úplná práve vtedy, keď $\mathcal{F}(T)$ je ultrafilter.
T je sporná práve vtedy, keď $\mathcal{B}(T) \cong \mathcal{B}(P)/\mathcal{F}(T)$ je jednoprvková.
T je úplná práve vtedy, keď $\mathcal{B}(T) \cong \mathcal{B}(P)/\mathcal{F}(T)$ je dvojprvková.

Súčet = sčítanec + sčítanec, konjunkcia = konjuganec $\wedge$ konjuganec.
Zlatoš

12 Jazyky

Jazyky a štruktúry prvého rádu, (prenexný tvar formúl). [Termy, formuly a teórie prvého rádu.] Spĺňanie formúl, modely teórií. Dokázateľnosť a veta o dedukcii. Bezosporné, úplné a henkinovské teórie. Gödelova veta o úplnosti. Veta o kompaktnosti a jej dôsledky. Príklady teórií.

12.1 Jazyky a teórie prvého rádu

Definícia 1. *Jazyk prvého rádu* je trojica $L = (F, R, \tau)$, $F \cup R = \emptyset$, $\tau\colon F \cup R \to \mathbb{N}$, $\tau(r) > 0$ pre $r \in R$. Prvky F sú *funkcionálne (operačné) symboly*, prvky R sú *relačné (predikátové) symboly*. τ sa nazýva *árnosť*. Prvky $F \cup R$ nazývame *špecifické symboly*.

Logické symboly sú
a) logické spojky: &, $\vee$, $\Rightarrow$, $\Leftrightarrow$, $\neg$
b) premenné: $x, y, z, x_1, x_2, y_0, z', \ldots$
c) kvantifikátory $\exists$, $\forall$
d) pomocné symboly (,).

Štruktúra jazyka L (model jazyka L) je usporiadaná dvojica $\mathcal{A} = (A, I)$, kde $A \neq \emptyset$, I je zobrazenie s definičným oborom $F \cup R$ také, že pre $f \in F_n$ $I(f)\colon A^n \to A$ a pre $r \in R_n$ $I(r) \subseteq A^n$. $I(f)$, $I(r)$ je *interpretácia* symbolu f resp. r. A sa nazýva *základná množina (nosič)*.

Termy jazyka L $\mathrm{Term}(L)$= najmenšia množina slov zostavená zo znakov L taká, že
(1) ak x je premenná, tak $x \in \mathrm{Term}(L)$
(2) ak $f \in F_n$, $t_1, \ldots, t_n \in \mathrm{Term}(L)$, tak $f(t_1, \ldots, t_n) \in \mathrm{Term}(L)$.

Interpretácia termov: Ak $\mathcal{A} = (A, I)$ je štruktúra na L, definujeme $I(t) = t^{\mathcal{A}} = t$ pre všetky $t \in \mathrm{Term}(L)$. Nech $t(x_1, \ldots, x_n)$ je term. Potom $I(t)\colon A^n \to A$ je zobrazenie také, že pre ľubovoľné $a_1, \ldots, a_n \in A$ platí:
1) ak $t = x_i$, tak $I(t)(a_1, \ldots, a_n) = a_i$
2) ak $t = f(t_1, \ldots, t_n)$, $f \in F_n$, $t_j(x_1, \ldots, x_n)$ sú termy, tak
$I(t)(a_1, \ldots, a_n) = I(f)(I(t_1)(a_1, \ldots, a_n), \ldots, I(t_n)(a_1, \ldots, a_n))$.

Formuly jazyka L: $\mathrm{Form}(L)$ = najmenšia množina taká, že
1) obsahuje tzv. *atomické formuly* $t_1 = t_2$ $(t_1, t_2 \in \mathrm{Term}(L))$, $r(t_1, \ldots, t_n)$ $(r \in R_n,\ t_i \in \mathrm{Term}(L))$
2) Ak $\varphi_1, \varphi_2 \in \mathrm{Form}(L)$, tak aj $\neg\varphi_1$, $(\varphi_1 \& \varphi_2)$, $(\varphi_1 \vee \varphi_2)$, $(\varphi_1 \Rightarrow \varphi_2)$, $(\varphi_1 \Leftrightarrow \varphi_2) \in \mathrm{Form}(L)$
3) Ak φ je formula a x premenná, tak $(\forall x)\varphi$, $(\exists x)\varphi$ sú formuly.

Mohutnosť jazyka $L = \|L\| = |\mathrm{Form}(L)| = \max(|F|, |R|, \aleph_0)$.

Ak $\varphi(x_1, \ldots, x_n)$ je formula jazyka L, $\mathcal{A}$ je štruktúra jazyka L a $a_1, \ldots, a_n \in A$, tak $\mathcal{A} \models \varphi(a_1, \ldots, a_n)$, čiže $\varphi(a_1, \ldots, a_n)$ je splnená v $\mathcal{A}$:
1) Ak φ je atomická formula tvaru $t_1 = t_2$ (t_i sú termy), tak $\mathcal{A} \models \varphi(a_1, \ldots, a_n)$ práve vtedy, keď $t_1^{\mathcal{A}}(a_1, \ldots, a_n) = t_2^{\mathcal{A}}(a_1, \ldots, a_n)$.
2) Ak φ je atomická formula tvaru $r(t_1, \ldots, t_n)$, tak $\mathcal{A} \models \varphi(a_1, \ldots, a_n)$ práve vtedy, keď $(t_1^{\mathcal{A}}(a_1, \ldots, a_n), \ldots, t_n^{\mathcal{A}}(a_1, \ldots, a_n)) \in r^{\mathcal{A}}$.
3) Ak φ je tvaru $\neg\psi$, tak $\mathcal{A} \models \varphi(a_1, \ldots, a_n)$ práve vtedy, keď nie je pravda, že $\mathcal{A} \models \psi(a_1, \ldots, a_n)$.
Ak φ je tvaru $\psi_1 \& \psi_2$, tak $\mathcal{A} \models \varphi(a_1, \ldots, a_n)$ práve vtedy, keď $\mathcal{A} \models \psi_1(a_1, \ldots, a_n)$ a zároveň $\mathcal{A} \models \psi_2(a_1, \ldots, a_n)$. Podobne pre ostatné logické spojky.
4) Ak φ je tvaru $(\exists x)\psi(x, x_1, \ldots, x_n)$, tak $\mathcal{A} \models \varphi(a_1, \ldots, a_n)$ práve vtedy, keď existuje $a \in A$ také, že $\mathcal{A} \models \psi(a, a_1, \ldots, a_n)$.
Ak φ je tvaru $(\forall x)\psi(x, x_1, \ldots, x_n)$, tak $\mathcal{A} \models \varphi(a_1, \ldots, a_n)$ práve vtedy, keď pre každé $a \in A$ také, že $\mathcal{A} \models \psi(a, a_1, \ldots, a_n)$.

Definícia 2. *Teória prvého rádu* v jazyku L je ľubovoľná podmnožina $T \subseteq \mathrm{Form}(L)$. Prvky množiny T sú *špecifické axiómy.*

Štruktúra $\mathcal{A}$ jazyka L je *modelom* teórie T (*spĺňa* teóriu T), ak $\mathcal{A} \models \varphi$ pre každé $\varphi \in T$, označujeme $\mathcal{A} \models T$.

$\mathrm{Mod}(T)$ = trieda všetkých modelov teórie T.

$\mathrm{Mod}(L)$ = trieda všetkých modelov jazyka L.

Formula φ je *splnená* v T (je nevyhnutným dôsledkom axióm teórie T), ak $\mathcal{A} \models \varphi$ pre každé $\mathcal{A} \in \mathrm{Mod}(T)$, t.j. pre všetky $\mathcal{A}$ platí $\mathcal{A} \models T \Rightarrow \mathcal{A} \models \varphi$.

Logické axiómy

Axiómy výrokového počtu

$$\varphi \Rightarrow (\psi \Rightarrow \varphi)$$

$$(\varphi \Rightarrow (\psi \Rightarrow \chi)) \Rightarrow ((\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \chi))$$

$$(\neg\psi \Rightarrow \neg\varphi) \Rightarrow ((\neg\psi \Rightarrow \varphi) \Rightarrow \psi)$$

Axiómy rovnosti

$$x = x$$

$$x = y \Rightarrow y = x$$

$$(x = y \& y = z) \Rightarrow x = z$$

$$(x_1 = y_1 \& \ldots \& x_n = y_n \& r(x_1, \ldots, x_n)) \Rightarrow r(y_1, \ldots, y_n), r \in R_n$$

$$(x_1 = y_1 \& \ldots \& x_n = y_n) \Rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n), f \in F_n$$

Axiómy kvantifikátorov

$$\varphi(t|x) \Rightarrow (\exists x)\varphi$$

$$(\forall x)\varphi \Rightarrow \varphi(t|x)$$

$\varphi(t|x)$ znamená dosadenie termu t za každý voľný výskyt premennej x. Substitúcia $\varphi(t|x)$ je prípustná, ak žiadna premenná termu t nie je viazaná v mieste voľného výskytu x.

$$\neg(\forall x)\varphi \Leftrightarrow (\exists x)\neg\varphi$$

$$\neg(\exists x)\varphi \Leftrightarrow (\forall x)\neg\varphi$$

$$(\forall x)(\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow (\forall x)\psi),$$

ak x nie je voľná vo φ

Odvodzovacie pravidlá

$$\frac{\varphi, \varphi \Rightarrow \psi}{\psi} \qquad \text{(MP)}$$

$$\frac{\varphi}{(\forall x)\varphi} \qquad \text{(Gen)}$$

Prenexný tvar formúl

Formula je v prenexnej normálnej forme, ak žiadna premenná vo φ nevystupuje súčasne ako voľná aj viazaná, žiadna premenná sa nevyskytuje pri viacerých kvantifikátoroch a výskyty kvantifikátorov predchádzajú výskyty všetkých spojok. Ku každej formule φ existuje formula φ' v prenexnom normálnom tvare, ktorá je s ňou logicky ekvivalentná (t.j. $\models \varphi \Leftrightarrow \varphi'$).

12.2 Dokázateľnosť a veta o dedukcii

Definícia 3. *Dôkaz* v teórii T je postupnosť $\varphi_0, \ldots, \varphi_n$ formúl jazyka L taká, že každé φ_i je:
1) logická axióma,
2) $\varphi_i \in T$,
3) vyplýva z predošlých na základe odvodzovacích pravidiel, teda existujú $j, k < i$ také, že $\varphi_k \equiv \varphi_j \Rightarrow \varphi_i$ (modus ponens), alebo existujú $j < i$ a premenná x také, že $\varphi_i \equiv (\forall x)\varphi_j$ (generalizácia).

Formula φ je *dokázateľná* v T, ak existuje jej dôkaz v T, t.j. dôkaz, ktorého posledným členom je φ. Označujeme $T \vdash \varphi$.

$T \models \varphi$ sa týka sémantiky, zatiaľ čo $T \vdash \varphi$ hovorí o dokázateľnosti, teda o syntaxi.

Veta 1 (o korektnosti). *Ak $T \vdash \varphi$, tak $T \models \varphi$.*

Veta 2 (o dedukcii). *$T \cup \{\varphi\} \vdash \psi$ práve vtedy, keď $T \vdash (\varphi \Rightarrow \psi)$, ak φ je uzavretá formula (t.j. φ nemá voľné premenné).*

Veta 3 (o dedukcii). *Nech φ je uzavretá. Potom $T \vdash \varphi$ práve vtedy, keď $T \cup \{\neg\varphi\}$ je sporná.*

Definícia 4. Teória T sa nazýva *sporná*, ak existuje formula φ taká, že $T \vdash \varphi$ a $T \vdash \neg\varphi$, *bezosporná (konzistentná)* inak.

Teória T sa nazýva *úplná*, ak je bezosporná a pre každú uzavretú formulu φ platí $T \vdash \varphi$ alebo $T \vdash \neg\varphi$. (Teda úplná teória je taká, ktorá je maximálna bezosporná).

Veta 4 (o úplnosti Gödelova). *Ak $T \models \varphi$, tak $T \vdash \varphi$.*

Veta 5 (o úplnosti Gödelova). *T je bezosporná práve vtedy, keď má model.*

Definícia 5. Nech $\varphi(x)$ je formula jazyka L a c je konštanta v L. Hovoríme, že c *dosvedčuje* tvrdenie $(\exists x)\varphi(x)$ v T, ak $T \vdash (\exists x)\varphi(x) \Rightarrow \varphi(c)$. Množina konštánt jazyka L sa nazýva *množina svedkov* teórie T, ak pre ľubovoľné tvrdenie $(\exists x)\varphi(x)$ v nej existuje konštanta, ktorá ho dosvedčuje. Teória sa nazýva *henkinovská*, ak má nejakú množinu svedkov.

Veta 6. *Nech T je bezosporná teória v jazyku L. Potom existuje obohatenie L_H jazyka L o nové konštanty a úplná henkinovská teória T_H v jazyku L_H taká, že $T \subseteq T_H$.*

Veta 7. *Každá úplná henkinovská teória má model.*

Veta 8. *Každá bezosporná teória v jazyku L má model mohutnosti nanajvýš $\|L\|$.*

Dôsledok 1. *Každá bezosporná teória v spočítateľnom jazyku má spočítateľný model.*

Skolemov paradox

Teória množín je teória v spočítateľnom jazyku. ($F = \{\emptyset\}$, $R = \{\in\}$) Má teda spočítateľný model $\mathcal{M}$. V modeli $\mathcal{M}$ vieme zostrojiť $\mathbb{N}^{\mathcal{M}}$, $\mathbb{R}^{\mathcal{M}}$. Obe tieto množiny sú spočítateľné, preto existuje medzi nimi bijekcia. Ale nebude to bijekcia v modeli $\mathcal{M}$. (Mohutnosť množiny je relatívny pojem.)

Veta o kompaktnosti

Veta 9 (o kompaktnosti). *$T \vdash \varphi$ práve vtedy, keď existuje konečná $T_0 \subseteq T$ taká, že $T_0 \vdash \varphi$.*
$T \models \varphi$ práve vtedy, keď existuje konečná $T_0 \subseteq T$ taká, že $T_0 \models \varphi$.
T je bezosporná práve vtedy, keď každá konečná podteória je bezosporná.
T má model práve vtedy, keď každá konečná podteória má model.

Tvrdenie 1. *Peanova aritmetika má neštandardné modely.*

12.3 Príklady teórií

Reálne uzavreté polia

Usporiadané polia: $F = \{+, ., 0, 1\}$, $R = \{\leq\}$
Axiómy poľa, lineárne usporiadaná množina a navyše

$$x \leq y \Rightarrow x + z \leq y + z$$
$$x \leq y \,\&\, 0 \leq z \Rightarrow x.z \leq y.z$$

Reálne uzavreté polia (RCF - real closed field) - navyše platí veta o supréme:
Pre každú formulu $\varphi(x)$ je axióma:

$$(\exists y)(\forall x)(\varphi(x) \Rightarrow x \leq y) \Rightarrow (\exists z)((\forall x)(\varphi(x) \Rightarrow x \leq z)\&(\forall y)((\forall x)(\varphi(x) \Rightarrow x \leq y) \Rightarrow z \leq y))$$

t.j. ak je množina určená formulou $\varphi(x)$ zhora ohraničená, tak má suprémum.

RCF je bezosporná, lebo jej modelom je $\mathbb{R}$. Keďže je to bezosporná teória v spočítateľnom jazyku, má spočítateľný model.

V matematickej analýze sa ukazuje, že ak niečo spĺňa axiómy RCF (pričom veta o supréme platí pre ľubovoľnú podmnožinu), tak je to izomorfné s $\mathbb{R}$. $\mathcal{P}(\mathbb{R}) = 2^{2^{\aleph_0}} > 2^{\aleph_0} > \aleph_0$. My však máme vetu o supréme len pre množiny tvaru $\{x, \varphi(x)\}$, ktorých je $\aleph_0$, teda to nie je spor.

Reálne algebraické čísla sú reálne uzavreté pole.

RCF je úplná teória.

Peanova aritmetika

Jazyk: $+, ., 0, 1$
Axiómy:

$$0 + 1 = 1$$
$$x + 1 = y + 1 \Rightarrow x = y$$
$$x + 0 = x$$
$$(x + y) + 1 = x + (y + 1)$$
$$x.0 = 0$$
$$x.(y + 1) = x.y + x$$

Schéma indukcie: Pre ľubovoľnú formulu $\varphi(x, \ldots)$ nasledujúca formula je axióma:

$$(\varphi(0)) \,\&\, (\forall x)(\varphi(x) \Rightarrow \varphi(x + 1)) \Rightarrow (\forall x)\varphi(x)$$

Teória grúp

V jazyku $TG(\cdot)$:

$$(xy)z = x(yz)$$
$$(\exists u)(\forall x)(xu = x = ux)$$
$$(\forall x)(\exists y)(\forall z)((xy)z = z = z(xy) = (yx)z = z(yx))$$

V jazyku $TG(\cdot, e)$

$$(xy)z = x(yz)$$
$$ex = x (= xe)$$
$$(\forall x)(\exists y)(yx = e)$$

V jazyku $TG(\cdot, e, ^{-1})$

$$(xy)z = x(yz)$$
$$ex = x$$
$$x^{-1}x = e$$

Ak chápeme grupu ako štruktúru v jazyku $TG(\cdot)$ alebo $TG(\cdot, e)$, tak jej podštruktúra nemusí byť grupa. (Napríklad $(N, +) \subseteq (Z, +)$.) To znamená, že teóriu grúp v týchto jazykoch nemožno axiomatizovať pomocou univerzálnych axióm.

Neexistuje teória konečných grúp (v zmysle teórie 1. rádu). (Dôsledok vety o kompaktnosti.)

Teória polí

$$(+, ., 0, 1) \quad \begin{array}{cc} x + y = y + x & xy = yx \\ x + (y + z) = (x + y) + z & (xy)z = x(yz) \\ x + 0 = 0 & 1.x = x \\ \forall x \exists y(x + y = 0) & \forall x \exists y(x \neq 0 \Rightarrow xy = 1) \\ x(y + z) = xy + xz & \end{array}$$

Axiómy sú univerzálno-existenčné.

Neexistuje teória T (1.rádu) v jazyku polí taká, že $\mathrm{Mod}(T)$ by boli všetky polia konečnej charakteristiky. (Dôsledok vety o kompaktnosti.)

Máme reťazcový komplex, ktorý vyzerá neškodný, a škodný vcelku nie je, ale je užitočný.
Korbaš

13 Podštruktúry a homomorfizmy

Podštruktúry, homomorfizmy a reťazce štruktúr. Elementárna ekvivalencia, elementárne podštruktúry a elementárne reťazce. Tarského kritérium. Diagramy. Axiomatické a konečne axiomatizovateľné triedy. Univerzálne, existenčné, univerálno-existenčné a pozitívne formuly. Zachovávanie teórií pri algebraických konštrukciách.

13.1 Podštruktúry a homomorfizmy

Definícia 1. Štruktúra $\mathcal{B} = (B, \ldots)$ jazyka L sa nazýva *podštruktúrou* štruktúry $\mathcal{A}$ (značíme $\mathcal{B} \subseteq \mathcal{A}$), ak $B \subseteq A$ a pre ľubovoľné n, $f \in F_n$, $r \in R_n$ a prvky $a_1, \ldots, a_n \in \mathcal{B}$ platí:

$$f^{\mathcal{B}}(a_1, \ldots, a_n) = f^{\mathcal{A}}(a_1, \ldots, a_n)$$

$$(a_1, \ldots, a_n) \in r^{\mathcal{A}} \text{ práve vtedy, keď} (a_1, \ldots, a_n) \in r^{\mathcal{B}}$$

Platnosť univerzálnych formúl sa prenáša na podštruktúry. Existenčné vlastnosti sa naopak prenášajú na nadštruktúry. Takisto sa samozrejme prenášajú univerzálne a existenčné teórie.

Definícia 2. Nech $\mathcal{A}$, $\mathcal{B}$ sú štruktúry, $h\colon A \to B$. Hovoríme, že h je *homomorfizmus*, ak pre ľubovoľné $a_1, \ldots, a_n \in A$, $f \in F_n$, $r \in R_n$ platí

$$hf^{\mathcal{A}}(a_1, \ldots, a_n) = f^{\mathcal{B}}(ha_1, \ldots, ha_n)$$

$$(a_1, \ldots, a_n) \in r^{\mathcal{A}} \Rightarrow (ha_1, \ldots, ha_n) \in r^{\mathcal{B}}$$

Hovoríme, že $\mathcal{B}$ je *homomorfný obraz* $\mathcal{A}$, ak existuje surjektívny homomorfizmus $h\colon \mathcal{A} \to \mathcal{B}$.

Definícia 3. $\mathcal{A}$, $\mathcal{B}$ sú štruktúry jazyka L, $h\colon A \to B$. Hovoríme, že h je *vnorenie* $\mathcal{A}$ do $\mathcal{B}$ ($h\colon \mathcal{A} \hookrightarrow \mathcal{B}$), ak je injektívne a pre ľubovoľné $a_1, \ldots, a_n \in A$, $f \in F_n$, $r \in R_n$ platí:

$$hf^{\mathcal{A}}(a_1, \ldots, a_n) = f^{\mathcal{B}}(ha_1, \ldots, ha_n)$$

$$(a_1, \ldots, a_n) \in r^{\mathcal{A}} \text{ práve vtedy, keď } (ha_1, \ldots, ha_n) \in r^{\mathcal{B}}$$

Izomorfizmus je surjektívne vnorenie. Je to ekvivalentné s tým, že je to bijekcia a aj inverzné zobrazenie je homomorfizmus.

Pozitívne formuly (t.j. tie, ktoré sú vytvorené len pomocou $\vee$, $\wedge$, $\exists$ a $\forall$) sa prenášajú na homomorfné obrazy. Existenčno-pozitívne formuly (tie nesmú obsahovať všeobecný kvantifikátor) sa prenesú z $\mathcal{A}$ na $\mathcal{B}$, ak existuje homomorfizmus $h\colon \mathcal{A} \to \mathcal{B}$.

Tvrdenie 1. *$\mathcal{A} \subseteq \mathcal{B}$ práve vtedy, keď $id_A\colon \mathcal{A} \hookrightarrow \mathcal{B}$.*
$h\colon \mathcal{A} \to \mathcal{B}$ je vnorenie práve vtedy, keď h je izomorfizmus $\mathcal{A}$ na $h(\mathcal{A})$.

Definícia 4. Nech $\mathcal{A}, \mathcal{B} \in \mathrm{Mod}(L)$ a $h\colon A \to B$. Hovoríme, že h je *elementárne vnorenie* $\mathcal{A}$ do $\mathcal{B}$, ak pre ľubovoľnú formulu $\varphi(x_1, \ldots, x_n)$ a prvky $a_1, \ldots, a_n \in A$ platí $(\mathcal{A} \models \varphi(\vec{a})) \Rightarrow (\mathcal{B} \models \varphi(h\vec{a}))$.

Elementárne vnorenie je vnorenie (zachovávajú sa atomické aj negatomické formuly). Ekvivalentná definícia elementárneho vnorenia je $(\mathcal{A} \models \varphi(\vec{a})) \Leftrightarrow (\mathcal{B} \models \varphi(h\vec{a}))$.

Definícia 5. Ak $\mathcal{A} \subseteq \mathcal{B}$, hovoríme, že $\mathcal{A}$ je *elementárna podštruktúra* $\mathcal{B}$ (označujeme $\mathcal{A} \prec \mathcal{B}$), keď pre ľubovoľnú formulu $\varphi(\vec{x})$ $a_1, \ldots, a_n \in A$ platí $(\mathcal{A} \models \varphi(\vec{a})) \Rightarrow (\mathcal{B} \models \varphi(\vec{a}))$.
Elementárna ekvivalencia: $\mathcal{A} \equiv \mathcal{B}$ $(\mathcal{A}, \mathcal{B} \in \mathrm{Mod}(L))$ práve vtedy, keď pre ľubovoľnú uzavretú formulu φ platí $\mathcal{A} \models \varphi \Leftrightarrow \mathcal{B} \models \varphi$.

Tvrdenie 2. *Ak $\mathcal{A} \prec \mathcal{B}$, tak $\mathcal{A} \equiv \mathcal{B}$.*
Ak $h : \mathcal{A} \xrightarrow{\prec} \mathcal{B}$, tak $\mathcal{A} \equiv \mathcal{B}$.

Príklad 1. $\mathbb{Q} \not\prec \mathbb{R} \not\prec \mathbb{C}$ (ako polia). Dá sa ukázať, že pre pole algebraických čísel $(\mathbb{A}, +, ., 0, 1)$ platí $\mathbb{A} \prec \mathbb{C}$, $\mathbb{A} \cap \mathbb{R} \prec \mathbb{R}$.

Tvrdenie 3. *Ak $\mathcal{A} \prec \mathcal{B}$ a $\mathcal{B} \prec \mathcal{C}$, tak $\mathcal{A} \prec \mathcal{C}$.*

Tvrdenie 4. *Ak $\mathcal{A} \prec \mathcal{B}$ a $\mathcal{B}$ je konečné, tak $\mathcal{A} = \mathcal{B}$.*

Tvrdenie 5. *Ak $\mathcal{A} \prec \mathcal{C}$, $\mathcal{B} \prec \mathcal{C}$ a $\mathcal{A} \subseteq \mathcal{B}$, tak $\mathcal{A} \prec \mathcal{B}$.*

Definícia 6. $\mathrm{Th}(\mathcal{A}) = \{\varphi; \varphi \text{ je uzavretá a } \mathcal{A} \models \varphi\}$ je *teória* štruktúry $\mathcal{A}$.

$\mathrm{Th}(\mathcal{A}_A)$ je *elementárny diagram* štruktúry $\mathcal{A}$.

$D^+(\mathcal{A}) = \{\varphi; \varphi$ je uzavretá atomická formula L_A taká, že $\mathcal{A} \models \varphi\}$ je *pozitívny atomický diagram* štruktúry $\mathcal{A}$.

Diagram (atomický diagram) štruktúry $\mathcal{A}$ je $D(\mathcal{A}) = \{\varphi; \varphi$ je uzavretá atomická alebo negatomická formula jazyka L_A taká, že $\mathcal{A} \models \varphi\}$.

$\mathrm{Th}(\mathcal{A})$ je úplná teória. Štruktúra $\mathcal{A}$ je jednoznačne daná pomocou $D^+(\mathcal{A})$. Z Gödelovej vety vyplýva, že každá úplná teória má tvar $\mathrm{Th}(\mathcal{A})$.

Tvrdenie 6. *Nech $h\colon A \to B$. Potom h je elementárne vnorenie $\mathcal{A}$ do $\mathcal{B}$ práve vtedy, keď $(\mathcal{B}, h(a))_{a\in A} \models \mathrm{Th}(\mathcal{A}_A)$.*

Tvrdenie 7. *Nech $\mathcal{A}, \mathcal{B} \in \mathrm{Mod}(L)$. Potom $\mathcal{A}$ možno elementárne vnoriť do $\mathcal{B}$ práve vtedy, keď existuje rozšírenie $(\mathcal{B}, b_a)_{a\in A}$ štruktúry $\mathcal{B}$ do štruktúry jazyka L_A taká, že $(\mathcal{B}, b_a) \models \mathrm{Th}(\mathcal{A}_A)$.*

Tvrdenie 8. *Nech $\mathcal{A}, \mathcal{B} \in \mathrm{Mod}(L)$, $h\colon \mathcal{A} \to \mathcal{B}$ práve vtedy, keď $(\mathcal{B}, h(a))_{a\in A} \models D^+(\mathcal{A})$.*

Tvrdenie 9. *Nech $\mathcal{A}, \mathcal{B} \in \mathrm{Mod}(L)$. Potom $\mathcal{A} \subseteq \mathcal{B}$ práve vtedy, keď $A \subseteq B$ a $\mathcal{B}_A \models D(\mathcal{A})$.*

Tvrdenie 10. *Nech $\mathcal{A}, \mathcal{B} \in \mathrm{Mod}(L)$, $h\colon A \to B$. Potom $h\colon \mathcal{A} \hookrightarrow \mathcal{B}$ je vnorenie práve vtedy, keď $(\mathcal{B}, h(a))_{a\in A} \models D(\mathcal{A})$.*

Nech $\mathcal{A}, \mathcal{B} \in \mathrm{Mod}(L)$. Potom $\mathcal{A}$ možno vnoriť do $\mathcal{B}$ práve vtedy, keď existuje rozšírenie $(\mathcal{B}, b_a)_{a\in A}$ štruktúry $\mathcal{B}$ do jazyka L_A také, že $(\mathcal{B}, b_a) \models D(\mathcal{A})$.

Veta 1 (Tarského kritérium pre elementárne podštruktúry). *Nech $\mathcal{A} \subset \mathcal{B}$. Potom $\mathcal{A} \prec \mathcal{B}$ práve vtedy, keď pre ľubovoľnú formulu $\varphi(x)$ jazyka L_A platí: Ak $\mathcal{B} \models (\exists x)\varphi(x)$, tak existuje $a \in A$ také, že $\mathcal{B} \models \varphi(a)$.*

Veta 2 (Löwenheim-Skolem-Tarski↑). *Nech $\mathcal{A}$ je nekonečná, $\mathcal{A} \in \mathrm{Mod}(L)$, β je kardinálne číslo také, že $\|L\| \leq \beta$, $|A| \leq \beta$. Potom existuje elementárne rozšírenie $\mathcal{B}$ štruktúry $\mathcal{A}$ ($\mathcal{B} \succ \mathcal{A}$) také, že $|B| \geq \beta$ ($|B| = \beta$).*

Veta 3 (Löwenheim-Skolem-Tarski↓). *Nech $\mathcal{A} \in \mathrm{Mod}(L)$. Potom pre každé kardinálne číslo β také, že $\|L\| \leq \beta \leq |A|$ existuje $\mathcal{B} \prec \mathcal{A}$ také, že $|\mathcal{B}| = \beta$. Dokonca pre ľubovoľnú $X \subseteq A$ takú, že $|X| \leq \beta$ existuje $\mathcal{B} \prec \mathcal{A}$ taká, že $|\mathcal{B}| = \beta$, $X \subseteq B$.*

Dôsledok 1. *Každá nekonečná štruktúra spočítateľného jazyka má spočítateľnú elementárnu podštruktúru.*

Lema 1 (o vzájomnej bezospornosti). *Teória $T \cup S$ je sporná práve vtedy, keď existujú $\varphi_1(\vec{x}), \ldots, \varphi_n(\vec{x}) \in S$ také, že $T \vdash (\exists \vec{x})(\neg\varphi_1(\vec{x}) \vee \ldots \vee \neg\varphi_n(\vec{x}))$.*

Γ je množina axióm pre teóriu T, ak $\mathrm{Mod}(\Gamma) = \mathrm{Mod}(T)$.

Lema 2 (axiomatizačná lema). *Nech T je bezosporná teória v jazyku L a $\triangle$ je množina uzavretých formúl jazyka L uzavretá na konečné disjunkcie. Potom nasledovné podmienky sú ekvivalentné.*

(i) T má množinu axióm $\Gamma \subseteq \triangle$.

(ii) Pre ľubovoľné $\mathcal{A}, \mathcal{B} \in \mathrm{Mod}(L)$ platí: $\mathcal{A} \models T$, $\mathcal{B} \models \mathrm{Th}(\mathcal{A}) \cap \triangle \Rightarrow \mathcal{B} \models T$.

Veta 4. *Nech T je bezosporná teória. Potom T sa prenáša na podštruktúry práve vtedy, keď T má množinu univerzálnych axióm.*

Veta 5. *Nech T je bezosporná teória. Potom trieda* $\mathrm{Mod}(T)$ *je uzavretá vzhľadom na nadštruktúry, práve vtedy, keď T má množinu existenčných axióm.*

Definícia 7. *Univerzálno-existenčná formula:* $\forall\vec{x}\exists\vec{y}\varphi(\vec{x},\vec{y},\vec{z})$, kde φ je bez kvantifikátorov.
Existenčno-univerzálna formula: $\exists\vec{x}\forall\vec{y}\varphi(\vec{x},\vec{y},\vec{z})$, kde φ je bez kvantifikátorov.

Π_1^0= uzavreté formuly logicky ekvivalentné s univerzálnymi
Σ_1^0= uzavreté formuly logicky ekvivalentné s existenčnými
Π_2^0= uzavreté formuly logicky ekvivalentné s univerzálno-existenčnými
Σ_2^0= uzavreté formuly logicky ekvivalentné s existenčno-univerzálnymi

Definícia 8. *Reťazec štruktúr* jazyka L nad lineárne usporiadanou množinou $(I,\leq)$ je systém štruktúr v jazyku L $(\mathcal{A}_i, i\in I)$ taký, že pre $i\leq j$ je $\mathcal{A}_i\subseteq\mathcal{A}_j$.
Zjednotenie reťazca $(\mathcal{A}_i, i\in I)$ je štruktúra $\mathcal{A}=\bigcup\limits_{i\in I}\mathcal{A}_i=(\bigcup\limits_{i\in I}A_i,\ldots)$,

$$f^{\mathcal{A}}(a_1,\ldots,a_n)=f^{\mathcal{A}_i}(a_1,\ldots,a_n)$$

$$(a_1,\ldots,a_n)\in r^{\mathcal{A}} \text{ práve vtedy, keď } (a_1,\ldots,a_n)\in r^{\mathcal{A}_i}$$

Elementárny reťazec je taký, ktorý spĺňa aj $\mathcal{A}_i\prec\mathcal{A}_j$.

Ak $\mathcal{A}_i$ tvoria reťazec, tak každé $\mathcal{A}_i$ je podštruktúrou $\bigcup_{i\in I}\mathcal{A}_i$. Ak ide o elementárny reťazec, tak je to elementárna podštruktúra.

Tvrdenie 11. *Nech φ je uzavretá univerzálno-existenčná formula a $(\mathcal{A}_i)_{i\in I}$ je reťazec štruktúr jazyka L. Ak $\mathcal{A}_i\models\varphi$ pre každé $i\in I$, tak $\bigcup\limits_{i\in I}\mathcal{A}_i\models\varphi$ (t.j. univerzálno-existenčné formuly sa zachovávajú pri zjednotení reťazca).*

Veta 6. *Každé pole F má algebraický uzáver (algebraicky uzavreté nadpole), algebraicky uzavreté algebraické rozšírenie $\overline{F}$.*

Veta 7. *Nech T je bezosporná teória v jazyku L. Potom nasledovné podmienky sú ekvivalentné.*

(i) *T má množinu univerzálno-existenčných axióm.*

(ii) $\mathrm{Mod}(T)$ *je uzavretá na zjednotenie ľubovoľných reťazcov.*

(iii) $\mathrm{Mod}(T)$ *je uzavretá na zjednotenie reťazcov nad* $(\mathbb{N},\leq)$.

Veta 8. *Nech T je bezosporná teória v jazyku L, potom trieda* $\mathrm{Mod}(T)$ *je uzavretá na homomorfné obrazy práve vtedy, keď T má množinu pozitívnych axióm.*

Flaša, z ktorej sa nič nevyleje. Ibaže sa tam ani nič nedá naliať.
Korbaš - o Kleinovej flaši

14 Modely

Filtrovaný súčin, ultrasúčin a ultramocnina. Łosova veta. Veta o kompaktnosti v jazyku ultraproduktov. Charakterizácia elementárnej ekvivalencie a (konečne) axiomatizovateľných tried. (Charakterizácia elementárnych tried. Peanova aritmetika, formalizácia dokázateľnosti. Gödelove vety o neúplnosti, Gödelova-Rosserova veta. Tarského veta o nedefinovateľnosti relácie spĺňania.)

14.1 Priamy a filtrovaný súčin

Definícia 1. $\prod_{i\in I}\mathcal{A}_i$ - *priamy súčin* systému $(\mathcal{A}_i, i\in I) = (\prod A_i, \ldots)$, $\prod_{i\in I} A_i = \{\alpha\colon I \to \cup A_i; \forall i\ \alpha(i)\in A_i\}$, $f^{\prod \mathcal{A}_i}(\alpha_1,\ldots,\alpha_n)(i) = f^{\mathcal{A}_i}(\alpha_1(i),\ldots,\alpha_n(i))$, $(\alpha_1,\ldots,\alpha_n)(i)\in r^{\prod \mathcal{A}_i}$ práve vtedy, keď $(\alpha_1(i),\ldots,\alpha_n(i))\in r^{\mathcal{A}_i}$.

Ak $\mathcal{A}_i = \mathcal{A}$ pre všetky $i\in I$, tak $\prod \mathcal{A}_i$ sa nazýva *priama mocnina* a označuje sa $\mathcal{A}^I$.

Diagonálne vnorenie $d\colon \mathcal{A}\to\mathcal{A}^I$, $a\mapsto d(a)$, $d(a)\colon I\to A$, $d(a)(i) = a$.

14.2 Ultraprodukt a Łosova veta

Definícia 2. *Zovšeobecnená pravdivostná hodnota*

$$[\varphi(\alpha_1,\ldots,\alpha_n)] = \{i\in I; \mathcal{A}_i \models \varphi(\alpha_1(i),\ldots,\alpha_n(i))\}$$

Tvrdenie 1. $[\varphi\&\psi(\vec{\alpha})] = [\varphi(\vec{\alpha})]\cap[\psi(\vec{\alpha})]$
$[\varphi\vee\psi(\vec{\alpha})] = [\varphi(\vec{\alpha})]\cup[\psi(\vec{\alpha})]$
$[\neg\varphi(\vec{\alpha})] = [\varphi(\vec{\alpha})]^C = I\setminus[\varphi(\vec{\alpha})]$
$[(\exists x)\varphi(x,\vec{\alpha})] = \bigcup_{\beta\in\prod A_i}[\varphi(\beta,\vec{\alpha})] = [\varphi(\vec{\alpha}_0,\vec{\alpha})]$ *pre nejaké* $\alpha_0\in\prod A_i$ – *princíp maxima*
$[(\forall x)\varphi(x,\vec{\alpha})] = \bigcap_{\beta\in\prod A_i}[\varphi(\beta,\vec{\alpha})] = [\varphi(\vec{\alpha}_0,\vec{\alpha})]$ *pre nejaké* $\alpha_0\in\prod A_i$ – *princíp minima*

Definícia 3. Ak D je filter na I, tak definujeme $\alpha\equiv_D\beta$ práve vtedy, keď $[\alpha=\beta]\in D$.

Filtrovaný súčin $\prod_{i\in I}\mathcal{A}_i/D = (\prod A_i/D,\ldots)$,

$$f(\alpha_1^D,\ldots,\alpha_n^D) = f(\alpha_1,\ldots,\alpha_n)^D,$$

$$(\alpha_1^D,\ldots,\alpha_n^D)\in r \text{ práve vtedy, keď } [r(\alpha_1,\ldots,\alpha_n)]\in D.$$

$\mathcal{A}^I/D$ sa nazýva *filtrovaná (redukovaná) mocnina.*

V prípade, že D je ultrafilter na I, nazývame filtrovaný súčin *ultraprodukt* a filtrovaná mocnina je *ultramocnina.*

Veta 1 (Łosova). *Nech $\mathcal{B}$ je ultrasúčin $\mathcal{A}^I/D$, a nech I je indexová množina. Potom pre ľubovoľnú formulu $\varphi(x_1,\ldots,x_n)$ a $\alpha_1,\ldots,\alpha_n\in\prod A_i$ platí*

$$\mathcal{B}\models\varphi(\alpha_1^D,\ldots,\alpha_n^D) \text{ vtedy a len vtedy, keď } [\varphi(\alpha_1,\ldots,\alpha_n)]\in D.$$

Tvrdenie 2. *Ak D je ultrafilter, tak $d\colon\mathcal{A}\xrightarrow{\prec}\mathcal{A}^I/D$.*

Veta o kompaktnosti v jazyku ultraproduktov

Definícia 4. $C\subseteq P(I)$ je *centrovaný systém*, ak prienik jeho ľubovoľného konečného podsystému je neprázdny. (Zrejme každý filter je centrovaný systém.)

Veta 2 (o kompaktnosti). *Nech Σ je množina uzavretých formúl jazyka L uzavretá vzhľadom na konečné konjunkcie a pre každé $\sigma\in\Sigma$ nech $\mathcal{A}_\sigma$ je štruktúra jazyka L taká, že $\mathcal{A}_\sigma\models\sigma$. Potom existuje ultrafilter D nad Σ taký, že $\prod_{\sigma\in\Sigma}A_\sigma/D\models\Sigma$.*

Veta 3 (Keisler-Shelah). *Ak $\mathcal{A}\equiv\mathcal{B}$, tak existuje množina I a ultrafilter D na I taký, že $\mathcal{A}^I/D\cong\mathcal{B}^I/D$.*

Veta 4. *Nech $\mathcal{A},\mathcal{B}\in\mathrm{Mod}(L)$. Potom $\mathcal{A}\equiv\mathcal{B}$ práve vtedy, keď existuje množina I a ultrafilter D na I tak, že $h\colon\mathcal{B}\xrightarrow{\prec}\mathcal{A}^I/D$.*

14.3 Triedy štruktúr

Definícia 5. Nech $\mathbb{K} \subseteq \mathrm{Mod}(L)$. *Teória triedy* $\mathbb{K}$ je $\mathrm{Th}(\mathbb{K}) = \{\varphi; \varphi \text{ je uzavretá a } \mathbb{K} \models \varphi\} = \bigcap_{\mathcal{A} \in \mathbb{K}} \mathrm{Th}(\mathcal{A})$.

$\overline{\mathbb{K}} = \mathrm{Mod}\,\mathrm{Th}\,\mathbb{K}$

$\overline{T} = \mathrm{Th}\,\mathrm{Mod}(T) = \{\varphi \text{ je uzavretá}; T \vdash \varphi\}$. (deduktívny uzáver)

Tvrdenie 3. $T_1 \subseteq T_2 \Rightarrow \mathrm{Mod}(T_1) \supseteq \mathrm{Mod}(T_2)$

$K_1 \subseteq K_2 \Rightarrow \mathrm{Th}(K_1) \supseteq \mathrm{Th}(K_2)$

$\mathrm{Mod}(\mathrm{Th}(\mathrm{Mod}(T))) = \mathrm{Mod}(T)$

Definícia 6. $\mathbb{K} \subseteq \mathrm{Mod}(L)$ sa nazýva *axiomatická trieda,* ak existuje teória T v jazyku L taká, že $\mathbb{K} = \mathrm{Mod}(T)$.

Veta 5. *Nech $\mathbb{K} \subseteq \mathrm{Mod}(L)$ je ľubovoľná trieda štruktúr. Potom sú ekvivalentné:*

(i) $\mathbb{K}$ *je axiomatická trieda.*

(ii) $\mathbb{K}$ *je uzavretá vzhľadom na izomorfizmy, elementárne podštruktúry a ultraprodukty.*

(iii) $\mathbb{K}$ *je uzavretá na elementárne ekvivalencie a ultraprodukty.*

Definícia 7. $\mathbb{K} \subseteq \mathrm{Mod}(L)$ je *varieta*, ak existuje množina atomických formúl T taká, že $\mathbb{K} = \mathrm{Mod}(T)$.

Veta 6. $\mathbb{K}$ *je varieta práve vtedy, keď* $\mathbb{K}$ *je uzavretá na podštruktúry, homomorfné obrazy a priame súčiny.*

Definícia 8. *Bázické Hornove formuly* sú formuly tvaru $\varphi_1 \vee \ldots \vee \varphi_n$, kde φ_i sú atomické alebo negatomické, ale najviac jedna z nich je atomická.

Hornove formuly sú vyrobené z bázických Hornových formúl pomocou &, $\exists$, $\forall$.

Bázické Hornove formuly môžu byť:
1. žiadna atomická: $\neg\psi_1 \vee \ldots \vee \neg\psi_n \equiv \neg(\psi_1 \& \ldots \& \psi_n)$ (ψ_i sú atomické)
2. žiadne negatomické: φ – atomická
3. nejaká atomická a nejaké negatomické: $\neg\psi_1 \vee \ldots \vee \neg\psi_n \vee \varphi \equiv (\psi_1 \& \ldots \& \psi_n) \Rightarrow \varphi$

Ak I je vlastný filter, hovoríme o vlastnom filtrovanom súčine.

Veta 7. *T sa prenáša na vlastné filtrované súčiny práve vtedy, keď T má množinu Hornových axióm.*

Veta 8. *Ak T je univerzálna teória, tak*

(i) T sa prenáša na priame súčiny práve vtedy, keď

(ii) sa prenáša na konečné priame súčiny práve vtedy, keď

(iii) má univerzálne Hornove axiómy.

Definícia 9. Trieda $\mathbb{K} \subseteq \mathrm{Mod}(L)$ (resp. teória T) sa nazýva *konečne axiomatizovateľná*, ak existuje konečná množina formúl S taká, že $\mathbb{K} = \mathrm{Mod}(S)$ (resp. $\mathrm{Mod}(T) = \mathrm{Mod}(S)$).

Veta 9. *Trieda $\mathbb{K} \subseteq \mathrm{Mod}(L)$ je konečne axiomatizovateľná práve vtedy, keď $\mathbb{K}$ aj $\mathrm{Mod}(L) \setminus \mathbb{K}$ sú axiomatické triedy.*

Predpoklad, že táto teória je sporná, vedie k sporu.
Zlatoš

15 Teória množín

Základné pojmy teórie množín (Boolovská algebra množín, relácie a zobrazenia, ekvivalencia a rozklad, usporiadanie). Konštrukcie usporiadaných množín, Hasseovej diagramy, zväzy, úplnosť. Naivná teória množín a jej paradoxy, axiomatizácia teórie množín, systém ZF. (Axióma výberu a všeobecný karteziánsky súčin.) Množinová ekvivalencia a subvalencia. Mohutnosť množiny, aritmetika kardinálnych čísel. Cantorova-Bernsteinova veta. Diagonalizácia, Cantorova veta, mohutnosti $\aleph_0$ a c, mohutnosti niektorých dôležitých množín.

Pri príprave tejto otázky boli okrem poznámok použité [BŠ], [H], [ŠS] a [Z].

15.1 Základné pojmy teórie množín

Tu sú len také samé ľahké veci, ktoré je možno až škoda písať.

$$X \cup Y = \{x : x \in X \vee x \in Y\}$$
$$X \cap Y = \{x : x \in X \wedge x \in Y\}$$
$$X \setminus Y = \{x : x \in X \wedge x \notin Y\}$$
$$X \times Y = \{(x, y) : x \in X \wedge x \in Y\}$$

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

Relácie

Definícia 1. *Reláciou* medzi prvkami množín A, B nazývame akúkoľvek podmnožinu karteziánskeho súčinu $A \times B$. Ak $A = B$, tak hovoríme o relácii na množine A.

Definícia 2. Ak $R \subseteq X \times Y$, $S \subseteq Y \times Z$ sú relácie, tak *kompozíciou (zložením)* relácií R a S nazývame reláciu $S \circ R \subseteq X \times Z$ takú, že $(x, z) \in S \circ R \Leftrightarrow \exists y; (x, y) \in R \wedge (y, z) \in S$.

$$(S \circ R)^{-1} = R^{-1} \circ S^{-1}$$
$$R[A] = \{b \in Y; (\exists a \in A)(a, b) \in R\}$$
$$R^{-1}[A] = \{a \in X; (\exists b \in B)(a, b) \in R\}$$
$$R[A \cup B] = R[A] \cup R[B]$$
$$R[A \cap B] \subseteq R[A] \cap R[B]$$
$$f[A \cup B] = f[A] \cup f[B]$$
$$f[A \cap B] \subseteq f[A] \cap f[B]$$
Ak f je bijekcia:
$$f^{-1}[A \cup B] = f^{-1}[A] \cup f^{-1}[B]$$
$$f^{-1}[A \cap B] = f^{-1}[A] \cap f^{-1}[B]$$

Definícia 3. Nech D je relácia na množine A.

D je *reflexívna*	$(\forall x \in A)(x,x) \in D$
D je *symetrická*	$(x,y) \in D \Rightarrow (y,x) \in D$
D je *asymetrická*	$(x,y) \in D \Rightarrow (y,x) \notin D$
D je *tranzitívna*	$(x,y) \in D \wedge (y,z) \in D \Rightarrow (x,y) \in D$
D je *trichotomická*	$x \neq y \Rightarrow ((x,y) \in D \vee (y,x) \in D)$
D je *antisymetrická*	$((x,y) \in D \wedge (y,x) \in D) \Rightarrow x = y$

Asymetrická relácia sa tiež zvykne volať silne antisymetrická, antisymetrická sa tiež volá slabo antisymetrická.

Ekvivalencia

Definícia 4. Relácia D na množine A sa nazýva *relácia ekvivalencie* na A, ak je reflexívna, symetrická a tranzitívna.

Veta 1. *Nech D je relácia ekvivalencie na množine $A \neq \emptyset$. Pre $x \in A$ označme $A(x) = \{y \in A : (y,x) \in D\}$. Potom systém množín $\{A(x) : x \in A\}$ tvorí rozklad množiny A. (Nazýva sa* rozklad indukovaný *ekvivalenciou D. $A(x)$ sa nazýva* trieda ekvivalencie *prvku x.)*

Nech A je neprázdna množina a $\mathcal{S}$ je jej rozklad. Definujme na množine A reláciu D ako $D = \{(x,y) \in A \times A : (\exists M \in \mathcal{S})(x \in M \wedge y \in M)\}$. Potom D je relácia ekvivalencie na A a $\mathcal{S}$ je ňou indukovaný rozklad.

Usporiadanie

Definícia 5. Relácia $\leq$ na množine X sa nazýva *čiastočné usporiadanie,* ak je reflexívna, antisymetrická a tranzitívna. (Alternatívna definícia: relácia $<$, ktorá je antireflexívna, silne antisymetrická a tranzitívna.) Dvojicu $(X, \leq)$ potom voláme *čiastočne usporiadaná množina.*

Nech $(X, \leq)$ je čiastočne usporiadaná množina. Ak platí

$$(\forall x, y \in X)(x \leq y \vee y \leq x),$$

tak $(X, \leq)$ sa nazýva *lineárne (totálne) usporiadaná množina.*

Definícia 6. Nech $(X, \leq)$ je čiastočne usporiadaná množina. Hovoríme, že prvok x je *pokrytý* prvkom y, ak $(x < y) \wedge (\nexists z) x < z < y$. Značíme $x \prec\!\!\!- y$.

Hasseovej diagram: x je spojené s y stúpajúcou hranou, ak $x \prec\!\!\!- y$.

Definícia 7. a je *najväčší* prvok čiastočne usporiadanej množiny A, ak $(\forall x \in A) x \leq a$.

a je *najmenší* prvok čiastočne usporiadanej množiny A, ak $(\forall x \in A) x \geq a$.

a je *maximálny* prvok A, ak $(\nexists x \in A) a < x$, *minimálny*, ak $(\nexists x \in A) x < a$.

a je *horné (dolné) ohraničenie* podmnožiny $B \subseteq A$, ak $(\forall b \in B) a \geq b$ $(a \leq b)$.

Infimum je najväčší prvok množiny dolných ohraničení a *suprémum* je najmenší prvok množiny horných ohraničení.

Čiastočne usporiadaná množina sa nazýva *úplná,* ak každá jej ohraničená podmnožina má suprémum a infimum.

Definícia 8. Nech $(A, \leq)$, $(B, \leq)$ sú čiastočne usporiadané množiny. Zobrazenie $f\colon A \to B$ je *izotónne*, ak $x \leq y \Rightarrow f(x) \leq f(y)$. f je *antitónne*, ak $x \leq y \Rightarrow f(x) \geq f(y)$. f je *monotónne,* ak je izotónne alebo antitónne.

Izomorfizmus čiastočne usporiadaných množín je zobrazenie $f\colon A \to B$, ktoré je bijektívne a platí $x \leq y \Leftrightarrow f(x) \leq f(y)$. (Ekvivalentne: bijekcia taká, že f aj f^{-1} sú izotónne.)

15.2 Naivná teória množín a jej paradoxy

Cantorova definícia množiny bola intuitívna. „Množina je súhrn objektov rozlíšiteľných našou intuíciou."

Cantorov (vymedzovací) princíp: ak $\varphi(x)$ je nejaká dosť presne definovaná vlastnosť, tak $\{x; \varphi(x)\}$ je množina.

Russelov paradox: $\{x; x \notin x\}$

Berryho paradox: $B = \{x \in \mathbb{N} : x$ možno jednoznačne popísať slovným spojením najviac 20 slov slovenského jazyka$\}$ (Keď m definujeme ako najmenšie prirodzené číslo, ktoré nemožno jednoznačne ..., dostali by sme $m \in B$ aj $m \notin B$.)

15.3 Zermelov-Fraenkelov axiomatický systém teórie množín

Axióma extenzionality	$(\forall A, B)(A = B \Leftrightarrow \forall x(x \in A \Leftrightarrow x \in B))$
Axióma dvojice	$(\forall x, y)(\exists Z)(\forall z)(z \in Z \Leftrightarrow (z = x \vee z = y))$
Axióma zjednotenia	$(\forall S)(\exists X)(\forall x)(x \in X \Leftrightarrow (\exists s \in S)(x \in s))$
Axióma potencie	$(\forall X)(\exists P)(\forall C)(C \in P \Leftrightarrow C \subseteq X)$
Schéma axióm vymedzenia:	Nech $\varphi(x)$ je výroková formula jednej voľnej premennej x $(\forall A)(\exists X)(\forall x)(x \in X \Leftrightarrow (x \in A \wedge \varphi(x)))$
Schéma axióm obrazu (substitúcie):	Nech F je zobrazenie $(\forall A)(\exists B)(\forall y)(y \in B \Leftrightarrow (\exists x)(x \in A \wedge F(x) = y))$
Inak:	Nech $\psi(u, v)$ je formula neobsahujúca voľné premenné w, z $(\forall u)(\forall v)(\forall w)((\psi(u, v) \wedge \psi(u, w)) \Rightarrow v = w) \Rightarrow$ $(\forall a)(\exists z)(\forall v)(v \in z \Leftrightarrow (\exists u)(u \in a \wedge \psi(u, v)))$
Axióma regularity (fundovanosti)	$(\forall A)(A \neq \emptyset \Rightarrow (\exists x \in A)x \cap A = \emptyset)$
Axióma existencie:	$(\exists x)(x = x)$
Axióma nekonečnej množiny:	$(\exists A)(\emptyset \in A \wedge (\forall x)(x \in A \Rightarrow x \cup \{x\} \in A)$

Nasleduje vysvetlenie, aký je význam jednotlivých axióm (pozri [Z] alebo [H].) Axióma extenzionality udáva, že dve množiny sa rovnajú práve vtedy, keď majú rovnaké prvky. (Prvky sa na množine podieľajú len svojou prítomnosťou.) Axióma dvojice, zjednotenia a potencie nám umožňuje vytvárať z daných množín nové množiny. (Axióma dvojice sa tiež použije pri definícii usporiadanej dvojice.) Axióma nekonečna postuluje existenciu nekonečnej množiny. Schéma axióm vymedzenia upresňuje Cantorov vymedzovací princíp. Schéma axióm obrazu rozširuje schému axióm vydelenia. Axióma regularity zakazuje nekonečné klesajúce reťazce $\ldots \in x_2 \in x_1 \in x_0$ a zaručuje, že celé univerzum množín možno získať pomocou iterácií operácii potenčnej množiny, t.j. $V_0 = \emptyset$, $V_{\alpha+1} = \mathcal{P}(V_\alpha)$ a $V_\lambda = \bigcup_{\alpha<\lambda} V_\alpha$ pre limitný ordinál λ.

15.4 Axióma výberu

Princíp výberu: Pre každý rozklad r množiny X existuje *výberová množina,* to znamená množina $v \subseteq X$, pre ktorú platí $(\forall u \in r)(\exists x)(v \cap u = \{x\})$.

Definícia 9. Funkcia f definovaná na množine X, pre ktorú platí $(y \in X \wedge y \neq \emptyset) \Rightarrow f(y) \in y$, sa nazýva *selektor* na množine X.

Axióma výberu (AC): Na každej množine existuje selektor.

Definícia 10. Nech J je množina. *Karteziánsky súčin* systému množín $\{F_j : j \in J\}$ definu-

jeme ako

$$\prod_{j\in J} F_j = \{f : f\colon J \to \bigcup F_j \wedge (\forall j \in J)(f(j) \in F_j)\}.$$

Tvrdenie 1. *Nasledujúce tvrdenia sú ekvivalentné:*

(i) axióma výberu,

(ii) princíp výberu,

(iii) pre každú množinovú reláciu s existuje funkcia f taká, že $f \subseteq s$ a $Dom(f) = Dom(s)$.

(iv) Karteziánsky súčin neprázdneho súčinu neprázdnych množín je neprázdny.

ZFC = ZF + AC

15.5 Množinová ekvivalencia, kardinálne čísla

Definícia 11. Hovoríme, že množiny A, B sú *ekvivalentné* $(A \approx B)$, ak existuje bijekcia $f\colon A \to B$.

Hovoríme, že A je *subvalentná* B, $A \preceq B$, ak existuje injekcia $f\colon A \to B$.

A je *ostro subvalentná* B, $A \prec B$, ak $A \preceq B$ a $A \not\approx B$.

Veta 2 (Cantor-Bernstein). *Ak $A \preceq B$ a $B \preceq A$, tak $A \approx B$.*

Bez AC nemusí platiť, že každé dve množiny sú porovnateľné v relácii $\preceq$.

Kardinálne číslo možno chápať ako najmenšie ordinálne číslo s danou kardinalitou. Cantorova definícia bola taká, že to boli vlastne typy (triedy) mohutnosti množín.

Existuje funkcia $\aleph$, ktorá zobrazuje triedu všetkých ordinálnych čísel na triedu všetkých nekonečných kardinálnych čísel. Je hodnoty označujeme $\aleph(\alpha) =: \aleph_\alpha$. Funkcia $\aleph$ je monotónna a spojitá (t.j. zachováva usporiadanie a supréma).

Kardinálna aritmetika

Definícia 12. Ak $\varkappa$, λ sú kardinálne čísla, tak definujeme kardinálny súčet, súčin a kardinálnu mocninu:

$$\varkappa + \lambda = |(\{0\} \times \varkappa) \cup (\{1\} \times \lambda)|$$
$$\varkappa.\lambda = |\lambda \times \varkappa|$$
$$\varkappa^\lambda = |\{f\colon \lambda \to \varkappa\}|$$

$$\aleph_\alpha + \aleph_\beta = \aleph_\alpha.\aleph_\beta = \max\{\aleph_\alpha, \aleph_\beta\}$$

$$\alpha^{\beta+\gamma} = \alpha^\beta.\alpha^\gamma$$
$$\alpha^{\beta.\gamma} = (\alpha^\beta)^\gamma$$
$$(\alpha.\beta)^\gamma = \alpha^\gamma.\beta^\gamma$$

Veta 3 (Cantorova). $2^\varkappa > \varkappa$

Diagonalizačná metóda, ktorou sa dokazuje Cantorova veta, má veľmi široké uplatnenie.

$$2^{\aleph_\alpha} = \aleph_\alpha^{\aleph_\alpha}$$

Hypotéza kontinua: $2^{\aleph_0} = \aleph_1$.

Zovšeobecnená hypotéza kontinua (GCH): Pre každé nekonečné kardinálne číslo $\aleph_\alpha$ platí $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ (t.j. medzi $\aleph_\alpha$ a $2^{\aleph_\alpha}$ už nie sú žiadne iné kardinálne čísla).

Gödel dokázal, že zovšeobecnená hypotéza kontinua je bezosporná vzhľadom k axiómam ZF. Cohen (a nezávisle od neho Vopěnka) ukázal, že hypotéza kontinua je nezávislá na axiómach teórie množín (t.j. nevyplýva z nich).

$\aleph_0 = |\mathbb{N}|$, $c = |\mathcal{P}(\mathbb{N})|$.

Množina A je spočítateľná, ak $A \preceq \mathbb{N}$. Ekvivalentná podmienka: $A = \emptyset$ alebo existuje surjekcia $g\colon \mathbb{N} \to A$.

Spočítateľné množiny: Množina všetkých prirodzených čísel, konečné postupnosti prirodzených čísel, algebraické čísla. Spočítateľné zjednotenie spočítateľných množín je spočítateľná množina. (Na dôkaz treba axiómu výberu.)

Nespočítateľné: $\mathbb{R}$, postupnosti prirodzených čísel, transcendentné čísla, Cantorovo diskontinuum.

Princíp matematickej indukcie je ekvivalentný s tým, že množina prirodzených čísel $\mathbb{N}$ je dobre usporiadaná.

Zbytočné a najvonkajšejšie zátvorky vynechávame.
Zlatoš

16 Ordinálne čísla

Izomorfizmus čiastočne usporiadaných množín, ordinálny typ. Dobre usporiadané množiny, ordinálne čísla a ich aritmetika. Ordinály ω_0 a ω_1.

Dobré usporiadanie

Definícia 1. Usporiadaná trieda sa nazýva *dobre usporiadaná*, ak každá jej neprázdna podmnožina má najmenší prvok.

Dobre usporiadaná trieda je lineárne usporiadaná.

Veta 1. *Každá podtrieda dobre usporiadanej triedy je dobre usporiadaná.*

Veta 2. *Nech $(A, <)$ je dobre usporiadaná množina a nech f je izotónne zobrazenie množiny A do A. Potom pre žiadne $a \in A$ neplatí $f(a) < a$.*

Definícia 2. Množina $I \subset A$ je *úsek* usporiadanej množiny $(A, <)$, ak existuje také $a \in A$, že $I = \{x \in A; x < a\}$; označujeme $I = A_a$.

Veta 3 (Základná veta o ordinálnych číslach). *Nech $(A, <_A)$, $(B, <_B)$ sú dobre usporiadané množiny. Potom alebo A a B sú izomorfné množiny, alebo jedna z nich je izomorfná úseku druhej.*

Ordinálne čísla

Ordinálne čísla sú typy dobre usporiadaných množín, to znamená, že všetkým navzájom izomorfným dobre usporiadaným množinám zodpovedá to isté ordinálne číslo.

Ordinálne čísla možno zaviesť viacerými ekvivalentnými spôsobmi.

Usporiadaná množina A sa nazýva ordinálne číslo, ak $a = A_a$ pre každé $a \in A$. (Šalát, Smítal; Hart) Množina A je ordinálne číslo, ak je tranzitívna (t.j. $x \in X \Rightarrow x \subseteq X$) a $\in$ je dobré ostré usporiadanie na X. (Balcar, Štěpánek)

Veta 4. *Ku každej dobre usporiadanej množine A existuje ordinál $Ord(A)$ s týmito vlastnosťami:*

(i) $A \cong Ord(A)$

(ii) *Ak $(A, <)$, $(A^*, <^*)$ sú dobre usporiadané množiny, tak $A \cong A^*$ platí práve vtedy, keď $Ord(A) = Ord(A^*)$.*

$Ord(A)$ sa nazýva ordinálne číslo množiny A.

Veta 5. *Každá dobre usporiadaná množina je izomorfná práve s jedným ordinálnym číslom.*

Definícia 3. Ordinálne číslo α je menšie ako ordinálne číslo β, ak α je podobné nejakému úseku množiny β. Namiesto $\alpha \cong \beta_b$ potom píšeme $\alpha < \beta$.

Veta 6. *Pre ľubovoľné dve ordinálne čísla α, β sú nasledujúce výroky ekvivalentné:*

(i) $\alpha < \beta$

(ii) $\alpha \subset \beta$

(iii) $\alpha \in \beta$

Aritmetika ordinálnych čísel

Lema 1. *Nech $(A, <_A)$, $(B, <_B)$ sú disjunktné dobre usporiadané množiny. Potom množina $C = A \cup B$ je dobre usporiadaná reláciou $<_C = (<_A) \cup (<_B) \cup A \times B$.*

Definícia 4. Nech $(A, <_A)$, $(B, <_B)$ sú disjunktné dobre usporiadané množiny. Nech $C = A \cup B$ je množina usporiadaná reláciou z predchádzajúcej definície. Potom ordinálne číslo $\gamma = Ord(C)$ sa nazýva súčet ordinálnych čísel $\alpha = Ord(A)$ a $\beta = Ord(B)$. Píšeme $\gamma = \alpha + \beta$.

Veta 7. *Ak α, β sú ordinálne čísla, $\beta \neq 0$, tak $\alpha < \alpha + \beta$.*

$$\omega + 1 \neq \omega = 1 + \omega$$

Definícia 5. Nech $(A, <_A)$ a $(B, <_B)$ sú usporiadané množiny. Potom usporiadanie $<_C$ karteziánskeho súčinu $C = A \times B$ dané vzťahom

$$[x_1, y_1] <_C [x_2, y_2] \Leftrightarrow (y_1 <_B y_2) \vee (y_1 = y_2 \wedge x_1 <_A x_2)$$

sa nazýva *lexikografické usporiadanie* množiny $A \times B$.

Lema 2. *Ak $(A, <_A)$ a $(B, <_B)$ sú dobre usporiadané množiny, tak lexikografické usporiadanie súčinu $A \times B$ je tiež dobré usporiadanie.*

Definícia 6. Nech A, B sú dobre usporiadané množiny. Nech C je karteziánsky súčin $A \times B$ s lexikografickým usporiadaním. Potom $\gamma = Ord(C)$ sa nazýva *súčin ordinálnych čísel* $\alpha = Ord(A)$ a $\beta = Ord(B)$. Píšeme $\gamma = \alpha.\beta$ alebo len $\gamma = \alpha\beta$.

$$\omega.2 = \omega + \omega \neq 2.\omega = \omega$$

Ordinály ω a Ω

Ordinálne číslo množiny $\mathbb{N}$ s obvyklým usporiadaním sa označuje ω. Je to najmenšie nekonečné ordinálne číslo.

Množina ordinálnych čísel všetkých dobrých usporiadaní množiny $\mathbb{N}$, čiže množina všetkých spočítateľných ordinálnych čísel, je tiež ordinálne číslo, ktoré sa zvykne označovať Ω alebo ω_1. Je to najmenšie nespočítateľné ordinálne číslo.

Literatúra k ordinálnym číslam: [BŠ], [H], [ŠS].

...čo je nesporne spor.
Činčura

17 Axióma výberu

Transfinitná indukcia. Princíp dobrého usporiadania, axióma výberu, Zornova lema a ich ďalšie ekvivalenty a dôsledky.

Táto časť je podľa [Z2]. Tu sa dolným rezom (počiatočným úsekom) rozumie to, čo bol v predchádzajúcej časti úsek, ale môže to byť navyše aj celá množina. Ďalej sa používa značenie $X^{(a)} = \{x \in X : x < a\}$.

17.1 Transfinitná indukcia a rekurzia

Veta 1 (o transfinitnej indukcii). *Nech $(X, <)$ je dobre usporiadaná množina. Nech $A \subseteq X$ je množina taká, že*

$$(\forall a \in X)(X^{(a)} \subseteq A \Rightarrow a \in A).$$

Potom $A = X$.

Veta 2 (o transfinitnej rekurzii). *Nech $(X, <)$ je dobre usporiadaná množina, Z je ľubovoľná množina a g je funkcia taká, že*

$$\operatorname{dom} g = \bigcup_{a \in X} Z^{X^{(a)}}.$$

Potom existuje jediná funkcia $f\colon X \to Z$ taká, že pre každé $a \in X$ platí

$$f(a) = g(f \restriction X^{(a)}).$$

Triedu všetkých ordinálnych čísel budeme značiť $\mathbf{\Omega}$. *Tranzitívna trieda* je taká trieda $\mathbf{X}$, že $z \in y \,\&\, y \in \mathbf{X} \Rightarrow z \in \mathbf{X}$. Transfinitná indukcia a rekurzia sa najčastejšie používajú pre ordinálne čísla, čiže v nasledovnej formulácii.

Veta 3 (o transfinitnej indukcii). *Nech $\mathbf{X} \subseteq \mathbf{\Omega}$ je tranzitívna trieda, $\mathbf{A} \subseteq \mathbf{X}$ je trieda taká, že*

$$(\forall \alpha \in \mathbf{X})(\alpha \subseteq \mathbf{A} \Rightarrow \alpha \in \mathbf{A}).$$

Potom $\mathbf{A} = \mathbf{X}$.

Veta 4 (o transfinitnej rekurzii). *Nech $\mathbf{X} \subseteq \mathbf{\Omega}$ je tranzitívna trieda, $\mathbf{Z}$ je ľubovoľná trieda a $\mathbf{G}$ je triedová funkcia taká, že*

$$\operatorname{dom} \mathbf{G} = \bigcup_{\alpha \in \mathbf{X}} \mathbf{Z}^{\alpha}.$$

Potom existuje jediná funkcia $\mathbf{F}\colon \mathbf{X} \to \mathbf{Z}$ taká, že pre každé $\alpha \in \mathbf{X}$ platí

$$\mathbf{F}(\alpha) = \mathbf{G}(\mathbf{F} \restriction \alpha).$$

Dôkaz transfinitnou indukciou aj konštrukcia transfinitnou rekurziou sa obvykle delí na dva kroky: pre limitné a pre nelimitné ordinály.

17.2 Ekvivalentné formy axiómy výberu

Definícia 1. Podmnožina A čiastočne usporiadanej množiny $(X, <)$ sa nazýva *reťazec,* ak je lineárne usporiadaná. Hovoríme, že podmnožina A čiastočne usporiadanej množiny $(X, <)$ je *usmernená*, ak pre ľubovoľné $x, y \in A$ existuje $z \in A$ také, že $x \leq z$ a $y \leq z$.

Veta 5. *Axióma výberu je ekvivalentná s každým z nasledujúcich tvrdení:*

(i) Nech E je ekvivalencia na množine X. Potom existuje množina $Y \subseteq X$ taká, že $(\forall x \in X)(\exists! y \in Y)(xEy)$.

(ii) Na každej množine X (ktorej prvkami sú množiny) existuje selektor, t.j. zobrazenie $h\colon X \to \bigcup X$ také, že $(\forall x \in X)(x \neq \emptyset \Rightarrow h(x) \in x)$.

(iii) Pre každú reláciu R existuje funkcia f taká, že $\operatorname{dom} f = \operatorname{dom} R$ a $f \subseteq R$.

(iv) Ku každej surjekcii $f\colon X \to Y$ existuje pravé inverzné zobrazenie, t.j. zobrazenie $g\colon Y \to X$ také, že $f \circ g = id_Y$.

(v) Karteziánsky súčin systému neprázdnych množín je neprázdny.

Axióma výberu sa používa napríklad aj v dôkaze ekvivalencie Heineho a Cauchyho definície spojitosti a tiež v dôkaze tvrdenia, že zjednotenie spočítateľného systému spočítateľných množín je spočítateľná množina. (V oboch prípadoch stačí tzv. slabá axióma výberu, ktorá postuluje existenciu selektora pre spočítateľné systémy množín nanajvýš mohutnosti kontinua.)

Princíp dobrého usporiadania (WO). *Každú množinu možno dobre usporiadať.*

Veta 6. *Princíp dobrého usporiadania je ekvivalentný s každým z nasledujúcich tvrdení:*

(i) Pre každú množinu X platí $|X| \in \mathbf{\Omega}$.

(ii) Pre každú nekonečnú množinu X existuje $\alpha \in \mathbf{\Omega}$ také, že $|X| = \aleph_\alpha$.

(iii) Pre ľubovoľné množiny X, Y platí $X \preceq Y$ alebo $Y \preceq X$.

(iv) Pre ľubovoľné kardinálne čísla α, β platí $\alpha \preceq \beta$ alebo $\beta \preceq \alpha$.

Princípy maximality sú najčastejšie označované názvom Zornova lema. Všetky nasledujúce formulácie princípu maximality sú ekvivalentné.

Princíp maximality (MP0). *Nech $(X, <)$ je čiastočne usporiadaná množina, v ktorej je každý reťazec zhora ohraničený. Potom pre každé $x \in X$ existuje maximálny prvok $m \in X$ taký, že $x \leq m$.*

Princíp maximality (MP1). *Nech X je ľubovoľná množina a $\mathcal{S} \subseteq \mathcal{P}(X)$ je systém jej podmnožín taký, že pre každý usmernený podsystém $\mathcal{D}$ v $(\mathcal{S}, \subseteq)$ platí $\bigcup \mathcal{D} \in \mathcal{S}$. Potom $\mathcal{S}$ obsahuje maximálny prvok.*

Princíp maximality (MP0'). *Nech $(X, <)$ je čiastočne usporiadaná množina, v ktorej každá usmernená podmnožina má suprémum. Potom v $(X, <)$ existuje maximálny prvok.*

Princíp maximality (MP1') *Nech X je ľubovoľná množina a $\mathcal{S} \subseteq \mathcal{P}(X)$ je systém jej podmnožín taký, že každý reťazec v $(\mathcal{S}, \subseteq)$ je zhora ohraničený. Potom pre každé $A \in \mathcal{S}$ existuje maximálna množina $M \in \mathcal{S}$ taká, že $A \subseteq M$.*

Použitím princípu maximality možno napríklad dokázať, že pre každý centrovaný systém existuje ultrafilter, ktorý ho obsahuje.

Veta 7. *Axióma výberu (AC), princíp dobrého usporiadania (WO) a princíp maximality sú ekvivalentné.*

Dôležité je uvedomiť si medze toho, čo môžeme vedieť o našom vedení.
Zlatoš

18 Univerzálne algebry a zväzy

Univerzálne algebry, základné algebraické konštrukcie (faktorová algebra, priamy a polopriamy súčin), zväz kongruencií algebry, variety algebier, Birkhoffova veta. Distributívne a modulárne zväzy. Boolovské algebry a ich reprezentácia.

18.1 Univerzálne algebry

Definícia 1. *Typom algebier* rozumieme množinu F, ktorej prvky nazývame operačné symboly. Každému prvku $f \in F$ patrí nezáporné celé číslo $o(f)$, nazývané jeho *árnosťou*. Ak $o(f) = n$, hovoríme, že f je n-árny operačný symbol. Nulárne operačné symboly sa nazývajú *konštanty*. F_n budeme označovať množinu všetkých n-árnych operačných symbolov typu F.

Definícia 2. Nech F je typ algebier. *Algebrou typu* F nazývame dvojicu $\mathcal{A} = (A; F)$, kde A je neprázdna množina a každému operačnému symbolu $f \in F$ je priradená n-árna operácia f^A na množine A, pričom $n = o(f)$.

Homomorfizmy a kongruencie

Definícia 3. Nech $\mathcal{A}$, $\mathcal{B}$ sú algebry typu F. Zobrazenie $\varphi\colon A \to B$ sa nazýva *homomorfizmus* (tiež *homomorfné zobrazenie*), ak pre každé $f \in F$ (nech $o(f) = n$) a každé $a_1, \ldots, a_n \in A$ je $\varphi(f(a_1, \ldots, a_n)) = f(\varphi a_1, \ldots, \varphi a_n)$.

Homomorfizmy sú uzavreté na skladanie, obraz a vzor algebry v homomorfizme sú podalgebry danej algebry. Obraz podalgebry generovanej nejakou množinou je podalgebra generovaná obrazom tej množiny.

Lema 1. *Nech $\varphi\colon A \to B$ je bijektívny homomorfizmus algebier. Potom $\varphi^{-1}\colon B \to A$ je tiež homomorfizmus.*

Definícia 4. Bijektívny homomorfizmus algebier sa nazýva *izomorfizmus*. Hovoríme, že algebry A, B sú izomorfné ($A \cong B$), ak existuje izomorfizmus $A \to B$.

Definícia 5. Ekvivalencia θ na algebre A, pre ktorú platí

$$a_i \theta b_i \ (i = 1, \ldots, n) \ \Rightarrow \ f(a_1, \ldots, a_n) \theta f(b_1, \ldots, b_n)$$

pre všetky $f \in F$ (t.j. θ je kompatibilná s operáciami algebry A), sa nazýva *kongruencia*. Množinu všetkých kongruencií na A budeme označovať $\operatorname{Con} A$.

Na každej algebre existujú dve triviálne kongruencie ω (najmenšia) a ι (plná).

Jadro homomorfizmu je kongruenciou, naopak každá kongruencia je jadrom prirodzeného homomorfizmu:

Definícia 6. Nech θ je ľubovoľná kongruencia algebry $\mathcal{A} = (A; F)$. Na faktorovej množine A/θ definujeme operácie pre všetky $f \in F$ takto: $f([a_1]\theta, \ldots, [a_n]\theta) = [f(a_1, \ldots, a_n)]\theta$. Dostaneme tak algebru $\mathcal{A}/\theta$, ktorú nazývame *faktorovou algebrou*.

$\varphi\colon a \mapsto [a]\theta$ je homomorfizmus algebry $\mathcal{A}$ na algebru $\mathcal{A}/\theta$ a $\operatorname{Ker} \varphi = \theta$. φ nazývame *prirodzený homomorfizmus*.

Priame a polopriame súčiny

Definícia 7. Nech $(\mathcal{A}_i; i \in I)$ je systém algebier typu F, $A = \prod(A_i; i \in I)$. Definujme algebru $\prod(\mathcal{A}_i; i \in I)$ takto: Ak $f \in F$ je n-árny operačný symbol, $a^1, \ldots, a^n \in A$, je $f(a^1, \ldots, a^n)$ taký prvok karteziánskeho súčinu A, že pre každé $i \in I$ je $f(a^1, \ldots, a^n)(i) = f(a^1(i), \ldots, a^n(i))$. Algebra $(\mathcal{A}; F)$ sa nazýva *priamy súčin algebier* $\mathcal{A}_i$. Súčin konečného počtu algebier sa označuje $A_0 \times A_1 \times \ldots \times A_n$.

Definícia 8. Izomorfizmus $\varphi\colon B \to \prod(A_i; i \in I)$ algebry B na priamy súčin algebier A_i nazveme *priamym rozkladom algebry* B. Hovoríme, že B sa dá rozložiť na priamy súčin algebier A_i, ak taký izomorfizmus existuje. A_i nazveme faktormi priameho rozkladu.

Definícia 9. Podalgebru A priameho súčinu $\prod(A_i; i \in I)$ nazývame *polopriamy súčin* tých algebier, ak pre každé $i \in I$ je projekcia $\pi_i|_A\colon A \to A_i$ surjektívna. Injektívny homomorfizmus $\varphi\colon B \to \prod(A_i; i \in I)$, pre ktorý $\varphi[B]$ tvorí polopriamy súčin algebier nazývame *polopriamym rozkladom* algebry B, algebry A_i nazývame jeho *faktormi*. Ak taký homomorfizmus φ existuje, hovoríme tiež, že B sa dá rozložiť na polopriamy súčin algebier A_i $(i \in I)$.

Polopriamy rozklad nazveme *vlastným*, ak pre žiadne $i \in I$ nie je $(\pi_i|\varphi[B]) \circ \varphi\colon B \to A_i$ izomorfizmus. Algebra, ktorá nemá vlastný polopriamy rozklad sa nazýva *polopriamo nerozložiteľná*.

Veta 1. *Ak* $\varphi\colon B \to \prod(A_i; i \in I)$ *je polopriamy rozklad algebry* B, $\theta_i = Ker(\pi \circ \varphi)$ $(i \in I)$. *Potom* $\bigcup(\theta_i : i \in I) = \omega$ *a* $A_i \cong B_i/\theta_i$ *pre každé* $i \in I$.

Veta 2. *Nech* A *je algebra. Nasledujúce podmienky sú ekvivalentné.*

(i) A *je polopriamo nerozložiteľná.*

(ii) $\cap(\theta : \theta \in \operatorname{Con} A \wedge \theta \neq \omega) \neq \omega$.

Okruh Z celých čísel je priamo nerozložiteľný, ale je polopriamo rozložiteľný.

18.2 Zväzy a úplné zväzy

Zavedieme označenie $a \vee b$ pre $\sup\{a, b\}$ a $a \wedge b$ pre $\inf\{a, b\}$.

Definícia 10. Usporiadaná množina P, v ktorej pre každé $a, b \in P$ existuje $a \vee b$ $(a \wedge b)$ sa nazýva $\vee$-*polozväz* ($\wedge$-*polozväz*) alebo *horný (dolný) polozväz*. P sa nazýva *zväz,* ak pre každé $a, b \in P$ existuje $a \vee b$ aj $a \wedge b$. P sa nazýva *úplný zväz*, ak pre každú podmnožinu $A \subset P$ existuje $\sup A$ aj $\inf A$.

Veta 3. *Usporiadaná množina* P *je práve vtedy úplným zväzom, keď každá jej podmnožina má infimum. (Ekvivalentne: keď* P *má najväčší prvok a každá neprázdna podmnožina* P *má infimum.)*

Veta 4 (Tarski). *Ak* P *je úplný zväz, tak každé izotónne zobrazenie* $f\colon P \to P$ *má pevný bod.*

Tarskiho vetu možno použiť na dôkaz Cantor–Bernsteinovej vety. Máme injekcie $f\colon A \to B$ a $g\colon B \to A$ a hľadáme pevný bod funkcie $F\colon \mathcal{P}(A) \to \mathcal{P}(A)$, $F(X) = A \setminus g(B \setminus f(X))$.

Lema 2. *Nech P je zväz. Operácie $\wedge$ a $\vee$ spĺňajú identity (idempotentnosť, komutatívnosť, asociatívnosť, absorpcia)*

$$x \wedge x = x \tag{L1}$$
$$x \wedge y = y \wedge x \tag{L2}$$
$$(x \wedge y) \wedge z = x \wedge (y \wedge z) \tag{L3}$$
$$(x \wedge y) \vee x = x \tag{L4}$$
$$x \vee x = x \tag{L1'}$$
$$x \vee y = y \vee x \tag{L2'}$$
$$(x \vee y) \vee z = x \vee (y \vee z) \tag{L3'}$$
$$(x \vee y) \wedge x = x \tag{L4'}$$

Veta 5. *Existuje navzájom jednojednoznačná korešpondencia medzi zväzmi $(L; \leq)$ a algebrami $(L; \wedge, \vee)$ spĺňajúcimi identity* (L1) *až* (L4) *a* (L1') *až* (L4'). *Algebra patriaca zväzu L má operácie $x \wedge y = \inf\{x, y\}$ a $x \vee y = \sup\{x, y\}$, usporiadanie zväzu prislúchajúceho algebre $(L; \wedge, \vee)$ je dané vzťahom $x \leq y \Leftrightarrow x \wedge y = x (\Leftrightarrow x \vee y = y)$.*

Vo zväze platí:
$a \leq b \Rightarrow c \wedge a \leq c \wedge b, c \vee a \leq c \vee b$
$a_1 \leq b_1, a_2 \leq b_2 \Rightarrow a_1 \wedge a_2 \leq b_1 \wedge b_2, a_1 \vee a_2 \leq b_1 \vee b_2$
$a \leq c, a \leq d, b \leq c, b \leq d \Rightarrow a \vee b \leq c \wedge d$
$(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$
$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$
$a \leq c \Rightarrow a \vee (b \wedge c) \leq (a \vee b) \wedge c$
$(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \leq (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$
$a_i \leq b_i \Rightarrow t(a_1, \ldots, a_n) \leq t(b_1, \ldots, b_n)$ pre každý termu typu $\{\wedge, \vee\}$
Ak t je term, tak t^d je term, ktorý vznikne z t zámenou $\vee$ a $\wedge$.

Tvrdenie 1 (Princíp duality). *Ak $I \equiv t_1 = t_2$ je identita platiaca vo zväze, tak aj $I^d \equiv t_1^d = t_2^d$ (tzv. duálna identita) je identita platiaca vo zväze.*

Ak $I = I^d$, tak I sa nazýva *samoduálna*.

18.3 Distributívne a modulárne zväzy

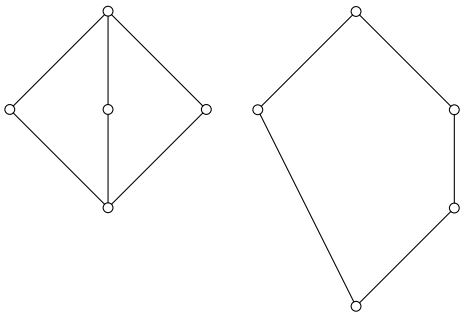
Lema 3. *Nasledujúce identity sú vo zväze ekvivalentné.*

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \tag{L5}$$
$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \tag{L5'}$$

Definícia 11. Zväz, ktorý spĺňa niektorú z identít (L5), (L5') sa nazýva *distributívny*.
Zväz sa nazýva *modulárny*, ak spĺňa podmienku

$$x \leq z \Rightarrow x \vee (y \wedge z) = (x \vee y) \wedge z \tag{18.1}$$

Oba tieto pojmy sú samoduálne. Každý distributívny zväz je modulárny.



M_3 N_5

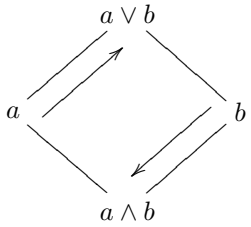
Veta 6. *Zväz je modulárny práve vtedy, keď neobsahuje podzväz izomorfný s N_5.*
Zväz je distributívny práve vtedy, keď neobsahuje podzväz izomorfný s M_3 alebo N_5.

Veta 7. *Zväz je distributívny práve vtedy, keď*

$$(x \wedge y) \vee (y \wedge z) \vee (z \wedge x) = (x \vee y) \wedge (y \vee z) \wedge (z \vee x).$$

Veta 8. *Zväz je modulárny práve vtedy, keď $a \wedge b = a \wedge c$, $a \vee b = a \vee c$, $b \leq c \Rightarrow b = c$.*
Zväz je distributívny práve vtedy, keď $a \wedge b = a \wedge c$, $a \vee b = a \vee c \Rightarrow b = c$.

Veta 9 (Dedekindov princíp transponovania). *Ak a, b sú prvky modulárneho zväzu, potom $\varphi : p \mapsto b \vee p$ a $\psi : q \mapsto a \wedge q$ sú navzájom inverzné izomorfizmy $[a \wedge b, a]$ a $[b, a \vee b]$.*



Operácie uzáveru

Definícia 12. *Operáciou uzáveru* v triede A sa nazýva také zobrazenie $^- : \mathcal{P}(A) \to \mathcal{P}(A)$, že pre každé $X, Y \subset A$ platí

(i) $X \subset X^-$

(ii) $X \subset Y \Rightarrow X^- \subset Y^-$

(iii) $X^{--} = X^-$

Trieda $X \subset A$ sa nazýva *uzavretá* , ak $X^- = X$.
Nech A je trieda. Triedu $U \subset \mathcal{P}(A)$, ktorá má vlastnosti

(i) $A \in U$

(ii) Ak $X_i \in U$ pre každé $i \in I$, tak $\bigcap (X_i : i \in I) \in U$.

nazývame *uzáverovým systémom* v A.

Veta 10. *Existuje jednojednoznačná korešpondencia medzi operátormi uzáveru v triede A a uzáverovými systémami v A.*

Uzáverový systém v množine, usporiadaný množinovou inklúziou, je úplný zväz. V tomto zväze sú prieseky množinové prieniky, spojenie systému množín je uzáver ich množinového zjednotenia.

Ak A je algebra, tak $\mathrm{Con}\, A$ je uzáverový systém v množine $A \times A$. Je to teda úplný zväz.

Ak L je zväz, tak zväz $\mathrm{Con}\, L$ je distributívny.

18.4 Boolovské algebry

Definícia 13. Nech L je zväz s najmenším prvkom 0 a najväčším prvkom I. Prvok $b \in L$ je *komplement* prvku $a \in A$, ak $a \wedge b = 0$, $a \vee b = I$.

Zväz s najmenším a najväčším prvkom nazveme *komplementárnym*, ak každý jeho prvok má komplement.

Definícia 14. Komplementárny distributívny zväz sa nazýva *boolovský zväz*. Ak $(L; \wedge, \vee)$ je boolovský zväz, algebra $(L; \wedge, \vee, ', 0, I)$ sa nazýva *boolovská algebra*.

Podalgebry algebier $P(M)$, kde M je nejaká množina sa nazývajú *množinové boolovské algebry*.

Veta 11. *Atomárna boolovská algebra je izomorfná s množinovou boolovskou algebrou. Boolovská algebra je izomorfná s množinovou algebrou $P(M)$ práve vtedy, keď je atomárna a úplná.*

Boolovskú algebru môžeme teda chápať ako algebru s operáciami $\vee$, $\wedge$, $'$, 0, 1. Podalgebra boolovskej algebry je podmnožina, ktorá je uzavretá na tieto operácie.

18.5 Variety

Definícia 15. Triedu $\mathcal{V}$ algebier rovnakého typu nazveme *varietou*, ak existuje množina I identít taká, že A je prvkom triedy $\mathcal{V}$ práve vtedy, keď spĺňa každú identitu z I.

Veta 12 (Birkhoff). *Trieda algebier rovnakého typu je varietou práve vtedy, keď je uzavretá na homomorfizmy, podalgebry a priame súčiny.*

Každý rozmýšľa, samozrejme.
Tomanová

Táto bibliografia má slúžiť nie len ako zoznam literatúry použitej pri príprave otázok, ale aj ako zoznam literatúry, ktorá sa dá u nás zohnať alebo stiahnuť. (Samozrejme, časom už niektoré linky asi nebudú platiť, ale nájsť tie veci na webe určite nebude problém.)

Literatúra

[AD] J.Adámek: *Kódování*

[ASH] R.B.Ash: *Abstract Algebra: The Basic Graduate Year* (www.math.uiuc.edu/~r-ash)

[ATA] T.Katriňák, M.Gavalec, E.Gedeonová, J.Smítal: *Algebra a teoretická aritmetika 1*

[ATA2] T.Šalát, A.Haviar, T.Hecht, T.Katriňák: *Algebra a teoretická aritmetika 2*

[BŠ] B.Balcar, P.Štěpánek: *Teorie množin.*

[BELL] A.D.Bell: *Modern algebra.* (www.uwm.edu/~adbell)

[BML] G.Birkhoff, S.MacLane: *Prehľad modernej algebry*

[BUR] S.Burris, H.Sankappanavar: *A Course in Universal Algebra* (www.thoralf.uwaterloo.ca/htdocs/ualg.html)

[H] K.P.Hart: *Set Theoretic Methods in General Topology.* (www.cs.vu.nl/~kphart)

[JAB] S.V.Jablonskij: *Úvod do diskrétnej matematiky*

[KN] M.Knor: *Disktrétna matematika I*

[KOL] M.Kolibiar, A.Legéň, T.Šalát, Š.Znám: *Algebra a príbuzné disciplíny*

[GT] J.S.Milne: *Group theory* (www.jmilne.org)

[MA] J.Martinez: *Introduction to universal algebra* (www.math.ufl.edu/~martinez)

[LW] J.H.van Lint, R.M.Wilson: *A Course in Combinatorics.*

[PL] J.Plesník: *Grafové algoritmy*

[ŠS] T.Šalát, J.Smítal: *Teória množín.*

[WM] W.Weiss, A.D'Mello: *Fundamentals of Model Theory.* (www.math.toronto.edu/weiss)

[Z] P.Zlatoš: *Ani matematika si nemôže byť istá sama sebou.*

[Z2] P.Zlatoš: *Čo by mal každý matematik vedieť o axióme výberu*

Okrem Legéňa ostatní napísali otázky na papieriky a človek si vytiahol jeden.

Šalát skúšal veci z teórie čísel. (Čiže úplne každý dostal jednu otázku z teórie čísel. Skúšal aj veci, ktoré neboli napísané v sylaboch na štátnice!!!)
1. Divergencia $\sum \frac{1}{n}$, $\sum \frac{1}{p}$.
Ak $d \mid m.n$, musí platiť, že $d \mid m$ alebo $d \mid m$.
2. Vzťah medzi (a, b) a $[a, b]$.
Môže mať riešenie rovnica $x^n + y^n = z^n$; x, y, z sú prvočísla, $n \geq 2$.
(Ako doplňujúce otázky: prvočísla – počet, ohraničenia, prvočíselná veta.)
3. Dokonalé čísla 1. druhu.
Ak $2^n - 1$ aj $2^n + 1$ sú prvočísla, čo z toho vyplýva pre n.
4. Cantorove rozvoje.
Vlastnosti funkcií $\sigma(n)$ a $\tau(n)$ pre $n \to \infty$.
5. Počet prvočísel, dolný odhad $\pi(x)$, súčet deliteľov 100.

Zlatoš skúšal všetko, čo neskúšali ostatní.
1. Rovinné grafy, Eulerova formula.
Konečne generované moduly nad OHI.
2. Oreho veta.
Reprezentácia Boolovských algebier.
3. Lineárne a Hammingove kódy.
Gödelova veta o úplnosti.
4. Sylowove vety.
Zachovávanie vlastností pri teoreticko–modelových konštrukciách.
5. Ramseyho veta.
Axióma výberu a ekvivalentné formulácie.

Činčura skúšal všeobecnú topológiu.
1. Metrizovateľné priestory a ich vlastnosti. Vety o metrizácii topologických priestorov.
2. Normálne priestory – vlastnosti, zachovávanie na topologické konštrukcie. Urysohnova lema.
3. Úplne regulárne priestory. Veta o reprezentácii.
4. Regulárne a úplne regulárne priestory. Zachovanie pri topologických konštrukciách. Súvis s normálnymi priestormi.
5. Súvislé a lineárne súvislé priestory a ich súvis, vlastnosti, ...

Legéň skúšal algebraickú a diferenciálnu topológiu.
1. Singulárne homologické grupy topologických priestorov. (Doplňujúca otázka: Či pomocou homologických grúp vieme dokázať, že $\mathbb{R}^m$ a $\mathbb{R}^n$ sú nehomeomorfné ak $m \neq n$.)
2. Vnáranie variet do $\mathbb{R}^n$.
3. Fundamentálna grupa.
4. Diferencovateľné variety a diferencovateľné zobrazenia.
5. Homotópia, retrakcie.