Algebra 3 (MA 0011)

RNDr. Břetislav Fajmon, Ph.D.

Katedra matematiky Pedagogické fakulty Masarykovy univerzity v Brně – verze 2024

Obsah

Úvod

Tento textík je zčásti seznamem otázek k opakování algebraických předmětů na pedagogické fakultě MUNI, zčásti by mohl být textem krátce uvádějícím do pojmu Booleho algebra, a také možná někdy (aspoň v mírné formě prezentované v knize Pinter: The Book of Abstract Algebra) pokusem o prezentaci důkazu, že existují polynomické rovnice stupně pátého a vyššího, které nelze řešit přesným vzorcem.

Břetislav Fajmon,
verze textu únor 2024

1 Otázka 01: Logika a teorie množin

- Co je to výrok? Co je to kvantifikátor? U výroku

  $$\forall n \in N : \quad 6|n \quad \Rightarrow \quad 2|n$$

  napište a) obrácení, b) obměnu, c) negaci, a to včetně kvantifikátorů.

- Uveďte negaci výroku:

  $$\forall n \in N : (6|n \quad \Leftrightarrow \quad (2|n \ \wedge \ 3|n))$$

  (pozor, kvantifikátor patří k celé ekvivalenci, není součástí jen levé části ekvivalence, ale náleží celému výroku a neguje se nejprve ... pak až pokračujeme a negujeme danou ekvivalenci).

- Napište vlastnost neutrálního prvku algebraické operace (vlastnost 3) a vlastnost existence inverzí u algebraické operace (vlastnost 4) ... pečlivě i s kvantifikátory; a ve druhé fázi proveďte negaci těchto výroků.

- Proveďte negace výrokových forem (elementárně, tak aby nezůstal znak negace před žádnou závorkou):

  a) $A \Rightarrow (B \vee C)$;

  b) $(A \Leftrightarrow B) \wedge C$;

  c) $(A \wedge B) \vee C$.

Pojďme dále na témata a označení teorie množin:

- Ze symbolů $A \cup B$, $A \cap B$, $\overline{A}$, $A \setminus B$, $A \div B$, $A \times B$ jen čtyři jsou binární operace, protože $\overline{A}$ je unární operace doplňku a $A \times B$ je kartézský součin, jehož výsledkem je množina uspořádaných dvojic, tj. struktura zcela jiného typu než vstupní množiny.

- Pod pojmem **vztahy mezi množinami** si představte relaci $\subseteq$, nebo rovnost výrazů s množinami a množinovými operacemi (binárními a unárními). Typický množinový vztah je distributivní zákon:

  $$\forall X, Y, Z \in 2^A : X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z),$$

  který dokazujeme Vennovými diagramy nebo pomocí univerzálního prvku x.

K množinám se vrátíme ještě u tématu Booleho algebry.

2 Otázka 02: Relace, ekvivalence, uspořádání, zobrazení

- Co je to binární relace? Uveďte nějaké její vlastnosti a příklad relace, která má danou vlastnost.
- Jak binární relace reprezentujeme? a) výčtem jejích prvků jako množinu uspořádaných dvojic; b) pomocí orientovaného diskrétního grafu; c) pomocí matice; d) pomocí kartézského grafu.
- Co je to relace ekvivalence? Jak relaci ekvivalence reprezentujeme (pomocí určitého rozkladu množiny na podmnožiny, který vždy existuje: v jedné podmnožině rozkladu jsou právě ty prvky, které jsou navzájem v relačním vztahu.
- Co je to relace uspořádání? Jak relaci uspořádání reprezentujeme? (speciálně poocí Hasseho diagramu – vysvětlete, jak v Hasseho diagramu značíme reflexivitu, antisymetrii a tranzitivitu). Uveďte dvě nebo tři velmi typické relace uspořádání.
- Co je to zobrazení? Jaké typy zobrazení známe?[1] U každého typu uveďte nějaký příklad nejlépe reálné funkce, tj. zobrazení $R \to R$ s danou vlastností.

[1] Opakování typů zobrazení, viz Základy matematiky, zaktualizovaný text, str. 69-71 včetně obrázku

3 Otázka 03: Struktury s jednou a se dvěma operacemi

- $A = \{1; 2; 3\}$ je tříprvková množina. Co za vlastnosti splňuje algebraická struktura s jednou operací, a sice a) $(2^A, \cup)$; b) $(2^A, \cap)$; c) $(2^A, \setminus)$; d) $(2^A, \div)$. Nazvěte tyto struktury z hlediska algebry. Uveďte u každé z nich, jaký konkrétně je neutrální prvek. Jestliže neexistují některé inverzní prvky, najděte příklad prvku, který nemá inverzi.

- Dalšími zajímavými vlastnostmi jsou zákon krácení v grupě (vlastnost 7), zákon idempotence (vlastnost 8) a zákon absorbce (vlastnost 9) ... zejména vlastnosti 8 a 9 jsou pak důležitými při studiu Booleho algebry.

- Co je to okruh $(M, \triangledown, \star)$? Uveďte typický příklad (tedy příklad okruhu, který není oborem integrity).

- Co je to obor integrity $(M, \triangledown, \star)$? Uveďte typický příklad (tj. příklad oboru integrity, který není tělesem). Jaký vztah splňují netriviální (či: nenuloví) dělitelé nuly?

- Co je to těleso $(M, \triangledown, \star)$? Uveďte typický příklad.

- Jakými strukturami jsou z algebraického hlediska následující množiny se dvěma operacemi?

  a) $(N_0, +, \cdot)$;
  b) $(Z, +, \cdot)$;
  c) $(Q, +, \cdot)$;
  d) $(R, +, \cdot)$;
  e) $(C, +, \cdot)$;
  f) $(Z_6, +, \cdot)$;
  g) $(Z_7, +, \cdot)$;
  h) $(Z_8, +, \cdot)$;
  i) $(2^A, \cup, \cap)$ pro $A = \{1; 2; 3\}$;
  j) $(2^A, \div, \cap)$ pro $A = \{1; 2; 3\}$.

- Co je to homomorfismus grup? Co je to homomorfismus okruhů? Uveďte příklady tohoto homomorfismu?

- K čemu je ten homomorfismus dobrý? a) surjektivní homomorfismus nám umožňuje studovat jen určitou vlastnost prvků ze vstupní množiny ve výstupní množině, ostatní vlastnosti prvků ze vstupní množiny jsou homomorfismem „ztraceny“. b) injektivní homomorfismus umožňuje rozšířit množinu čísel, se kterými pracujeme, na větší množinu a tím, že vlastnosti sčítání a násobení prvků z dřívější (menší) množiny zůstanou zachovány ... tento injektivní homomorfismus bude ještě zmíněn v otázce 7.

4 Otázka 06: Polynomy

- Co je to polynom? Jakou algebraickou strukturu tvoří množina všech polynomů s reálnými koeficienty $(R[x], +, \cdot)$?
- Co je to kořen polynomu? Co říká základní věta algebry?[2] Co je to násobnost kořene?
- Formulujte pomocí rovnic Eukleidův algoritmus hledání NSD dvou polynomů.
- Uveďte význam Hornerova schématu na příkladu: a) najde kořen polynomu, a současně provede dělení (čeho čím? jaký je výsledek?); b) provede i dělení polynomu se zbytkem ... napište přesně rovnici, ve které jsou obsaženy oba polynomy, jejich podíl i zbytek.[3]
- Co říká věta o racionálních kořenech polynomu z $(Q[x], +, \cdot)$?
- Co říká věta o komplexně sdružených kořenech polynomu z $(R[x], +, \cdot)$?
- Jak se odstraní z polynomu $p(x)$ vícenásobné kořeny? (nemusíte příklad, jen vysvětlení při dobrém označení)
- Co je to algebraický a goniometrický tvar komplexního čísla? Vysvětlete včetně označení a obrázku.
- Co říká Moivreho věta?
- Jakým způsobem vypočteme $n-$tou odmocninu z komplexního čísla $c \in C$? Uveďte vzorec, vyřešte binomickou rovnici $z^6 = 64$ a binomickou rovnici $z^3 = -1$ a vyznačte vždy všechna řešení dané rovnice v Gaussově rovině.
- Uveďte, jakým způsobem řešíme reciprokou rovnici

  $$x^5 - 2x^4 + 3x^3 + 3x^2 - 2x + 1 = 0$$

  (nemusíte vyřešit úplně, jen popište metodu řešení až do chvíle, kdy nám zbývá vyřešit rovnici kvadratickou ... tu už řešit nemusíte).
- Metodou půlení intervalu najděte řešení rovnice $x^3 - x - 2 = 0$ na intervalu $\langle 1; 2\rangle$. Nemusíte řešit moc podrobně, protože nemáte kalkulačku – proveďte jen dva kroky, z nichž bude jasné, jak se postupuje.
- Metodou Newtonovou (tečen) najděte řešení rovnice $x^3-x-2 = 0$ na intervalu $\langle 1; 2\rangle$. Nemusíte řešit moc podrobně, protože nemáte kalkulačku – jeden krok vypočtěte a do druhého dosaďte, aby bylo jasné, jak se postupuje.

---

[2] Základní věta algebry je jakousi obdobou rozkladu přirozeného nebo celého čísla na součin prvočísel.

[3] V otázkách a) i b) nestačí jen projet Hornerovo schéma – musíte ještě v rovnici ukázat, co je důsledkem-výstupem Hornerova schématu.

5 Otázka 04: Vektorové prostory a lineární zobrazení

Jde převážně o zopakování pojmů, příklady těchto pojmů a jejich význam. Otázka sestává ze dvou celků. Prvním celkem je pojem vektorového prostoru a podprostoru.

- Co je to vektorový prostor V nad tělesem T?
- Uveďte příklad vektorového prostoru (prostor aritmetický, prostor polynomů stupně nejvýše 4, prostor polynomů jakéhokoli stupně, prostor spojitých reálných funkcí): jak se na daném VP definuje sčítání vektorů a jak se definuje násobení vektorů skalárem?
- Co je to vektorový podprostor vektorového prostoru?
- Uveďte příklad vektorového podprostoru nějakého vektorového prostoru.
- Co je to lineární kombinace vektorů?
- Co je to lineární závislá množina vektorů?
- Co je to báze (dimenze) vektorového prostoru?
- Co jsou to souřadnice vektoru vzhledem k zadané bázi vektorového prostoru?
- Co je to součet vektorových podprostorů a jak se definuje?
- Co říká věta o dimenzi součtu a průniku vektorových podprostorů?

Právě uvedená část otázky směřuje na zkoumání vlastností afinních podprostorů a studiu jejich vzájemné polohy (vlastnosti a vztahy afinních podprostorů jsou už ovšem jinou státnicovou otázkou z geometrie).

Druhá polovina otázky se věnuje technické podpoře pojmu lineární zobrazení mezi vektorovými prostory a podpoře pojmů vlastní čísla a vlastní vektory lineární transformace:

- Co je to lineární zobrazení φ mezi vektorovými prostory?
- Jak lze lineární zobrazení zadat (vysvětlete tři způsoby zadání na příkladu)?
- Uveďte příklad lineárního zobrazení geometricky, tj. nalezněte jeho matici, jestliže se jedná o osovou souměrnost v rovině nebo o rotaci v rovině se středem v počátku (například pro osovou souměrnost v rovině vzhledem k ose $y = \frac{x}{3}$).
- Co je to lineární transformace?
- Co jsou to vlastní čísla a vlastní vektory lineární transformace?
- Uveďte příklad vlastních čísel a vlastních vektorů geometricky, například u osové souměrnosti vzhledem k ose $y = \frac{x}{3}$.

- Jak nalezneme vlastní čísla a vektory lineární transformace zadané maticí A? Vysvětlete algebraickou metodu (stačí postup bez příkladů, ale v postupu musí vše být dobře označeno).
- Příklad osové souměrnosti v rovině vzhledem k ose $y = \frac{x}{3}$ ... nalezněte matici této lineární transformace a) vzhledem ke standardní bázi, b) vzhledem k ortonormální bázi vlastních vektorů.
- Jak se nazývají matice téže lineární transformace (viz a,b v předchozí odrážce) zadané pouze v různých bázích?

Tolik druhá část otázky – ta se tedy věnuje práci s lineárními zobrazeními (s využitím vlastních čísel, jestliže jsou vlastní čísla reálná různá, pak totiž je zaručeno, že příslušné vlastní vektory jsou navzájem ortogonální).

6 Otázka 05: Soustavy lineárních rovnic, matice a determinanty

Jde převážně o otázku, která se věnuje různým metodám řešení systému lineárních rovnic (dále zkratka: SLR), a pojmům které s tím souvisejí, tj. zejména maticovým operacím a výpočtu determinantu. Metody A,B,C lze vysvětlit na příkladu

$$\begin{aligned} x \quad - z &= 0, \\ 3x + y \quad &= 1, \\ -x + y + z &= 4. \end{aligned}$$

Metodu D vysvětlete na příkladu

$$\begin{aligned} x + y + 2z - 5w &= 1, \\ 2x + 5y - z - 9w &= 4. \end{aligned}$$

A) Gaussova eliminační metoda:
- Slovně stručně vysvětlete, v čem spočívá Gaussova metoda (popřípadě Gaussova-Jordanova metoda) ... můžete i bez příkladu.
- Co jsou to elementární řádkové úpravy?
- Co je to schodový tvar matice?
- Jak se liší Gaussova a Gaussova-Jordanova metoda?
- Co říká Frobeniova věta o řešitelnosti a počtu řešení SLR? (jaké jsou různé případy počtu řešení a ve kterých situacích nastanou?)

B) Maticová metoda:
- Kdy lze matice sčítat a jaké algebraické vlastnosti má operace sčítání matic? (neutrální prvek a inverzní prvky vysvětlete podrobně, na příkladu)
- Kdy lze matice násobit a jaké algebraické vlastnosti má operace násobení matic? (neutrální prvek a inverzní prvky vysvětlete podrobně, na příkladu)
- Otázka nenulových dělitelů nuly v okruhu čtvercových matic: vysvětlete podrobně na příkladu.
- Co je to hodnost matice? Definujte a) pomocí schodového tvaru získaného z matice A pomocí EŘÚ; b) pomocí vektorového podprostoru generovaného řádky matice.
- Vysvětlete maticovou metodu řešení SLR – jen vysvětlete postup, nemusíte řešit konkrétní příklad.

C) Cramerovo pravidlo:
- Uveďte definici determinantu, vysvětlete označení, které s tím souvisí.
- Vypočtěte determinant
$$\begin{vmatrix} 1 & 2 & 0 & 2 \\ 2 & 4 & 1 & 0 \\ 0 & 0 & -1 & 3 \\ 3 & -1 & 1 & 4 \end{vmatrix}$$
a) z definice (aspoň naznačte, vyčíslete jeden až dva členy součtu); b) Laplaceho rozvojem pomocí řádku-sloupce (uvedený rozvoj proveďte, ale nemusíte ho dále vyčíslovat).
- Jaké jsou vlastnosti singulární-regulární matice vzhledem k pojmům a) determinant; b) hodnost matice; c) počet řešení SLR $A \cdot \vec{x} = \vec{b}$; d) inverzní matice?
- Vysvětlete využití determinatů v matodě Cramerovo pravidlo na příkladu z úvodu této otázky.
- Jaké jsou vlastnosti determinantu? Zejména se soustřeďte na rozdíl mezi řádkovými úpravami matice a úpravami determinantu – které úpravy jsou stejné a které se liší a jak?
- Lze chápat determinant jako zobrazení? Jestliže ano, tak mezi kterými množinami („odkud kam“)?
- Jestliže determinant lze chápat jako lineární zobrazení (což lze), tak z linearity zobrazení plyne i vlastnost linearity determinantu – vysvětlete vlastnost linearity determinantu na matici rozměru 2×2.

D) Pripcip superpozice:
- Ad nehomogenní SLR: Co říká Frobeniova věta o řešitelnosti a počtu řešení SLR? (jaké jsou různé případy počtu řešení a ve kterých situacích nastanou?)
- Ad homogenní SLR: Jaké jsou různé případy počtu řešení a ve kterých situacích nastanou?
- Vysvětlete na konkrétním příkladu metodu principu superpozice (nejlépe na příkladu z úvodu této otázky doporučeném k metodě D).

7 Některé části otázky číslo 4 z geometrie

Měli byste znát definici a příklad skalárního součinu vektorů:

- Skalární součin na vektorovém prostoru V nad tělesem T je symetrická pozitivně definitní bilineární forma ... vysvětlete každý z těchto čtyř termínů přesně matematicky.
- Jak se definuje skalární součin na aritmetickém vektorovém prostoru $(R^n, +)$?
- Jak se definuje skalární součin na vektorovém prostoru spojitých funkcí na intervalu $\langle 0; 1\rangle$?

Také musíte znát definici velikosti vektoru a některé vlastnosti velikosti:

- Jak se definuje velikost vektoru pomocí skalárního součinu vektorů? (obecně pomocí vektorového součinu)
- Uveďte vlastnost pozitivní definitnosti velikosti.
- Uveďte vlastnost homogenity velikosti.
- Uveďte trojúhelníkovou nerovnost.
- Každý nenulový vektor lze normovat ... co to znamená?
- Jak se definuje velikost na vektorovém prostoru spojitých funkcí na intervalu $\langle 0; 1\rangle$?

Otázku vektorového součinu budu zkoušet pouze na středoškolské úrovni:

- Vektorovým součinem vektorů $\vec{u}$, $\vec{v}$ je vektor – jaký má tento vektor směr (nakreslete obrázek) a jakou má velikost (nezajímá mne odpověď, že velikost se vypočte podle vzorce pro velikost vektoru, ale jaký je geometrický význam velikosti ve vztahu k vektorům $\vec{u}$, $\vec{v}$)?

8 Otázka 07: Číselné obory a jejich konstrukce

Tato otázka vysvětluje vlastnosti jednotlivých množin čísel ve školské matematice, ale také uvádí algebraické konstrukce každé následné množiny v posloupnosti množin N, Z, Q, R, C pomocí množiny předchozí.

Vlastnosti množiny přirozených čísel:

- uveďte čtyři Peanovy axiomy, které souvisí s Peanovou množinou a relací rovnosti.
- uveďte další čtyři (až pět) zbývajících (tzv. hlavních) Peanových axiomů a vysvětlete, jak souvisí s množinou přirozených čísel.
- Měli byste si pamatovat výrok: Množina přirozených čísel je jediným modelem Peanovy množiny až na izomorfismus (tj. až na přeznačení prvků).
- Dodáním nuly do množiny přirozených čísel dostaneme strukturu $(N_0), +, \cdot)$, která je ...

Konstrukce Z pomocí N:

- Jednoduše řečeno, z $(N, +, \cdot)$ dostaneme $(Z, +, \cdot)$ dodáním ...
- Ale přesněji řečeno, nemůžeme do N jen tak dodávat nějaké prvky, jde tady o mnohem více ... jde tady o dodání prvků a současně zaručení, že dříve definované operace sčítání a násobení na N budou fungovat stejně, a navíc bude množina obohacená o nové prvky ucelenou algebraickou strukturou. To vše zaručuje náročněji popsaná konstrukce. Popište její jednotlivé kroky:
  - Jakou množinu vytvoříme z N nejprve?
  - Na $N \times N$ definujeme relaci ekvivalence – jak?
  - Utvoříme rozkladovou množinu (faktormnožinu) na základě dané ekvivalence – popište, jaké prvky se nacházejí ve stejné podmnožině.
  - Na faktormnožině definujeme operaci sčítání mezi podmnožinami – jak?
  - Jaké vlastnosti daná operace na faktormnožině splňuje?
  - Definujeme zobrazení $N \to N \times N/_\sim$, které je injektivní homomorfismus – jak?
  - V množině $N \times N/_\sim$ se vyskytují i podmnožiny, které nejsou obrazem žádného přirozeného čísla – které to jsou?

9 K Otázce 01 (logika a teorie množin): Booleho algebra

- Co je to svaz? Nakreslete svaz všech dělitelů přirozeného čísla 60, uspořádaný relací dělitelnosti.
- Nakreslete svaz všech dělitelů přirozeného čísla 72, uspořádaný relací dělitelnosti.
- Nakreslete svaz všech podmnožin pětiprvkové množiny (uspořádaný podle relace $\subseteq$).
- Uveďte vlastnosti operací $\vee$, $\wedge$ ve svazu (nově: vlastnost idempotence, vlastnost absorbce).
- Poznámka: vlastnost neutrálního prvku nemusí u daných operací platit, protože v nekonečných svazech nemusí největší (nejmenší) prvek existovat.
- Musí operace $\vee$, $\wedge$ splňovat distributivní zákon? Operace průniku a sjednocení distributivní zákon splňují, ale obecně ve svazu nemusí platit – příkladem jsou svazy M_5 a N_5.
- Naštěstí platí krásná matematická věta: Svaz je distributivní, právě když neobsahuje podsvaz M_5 nebo N_5.
- Definice komplementu, definice komplementárního svazu. Měli byste být schopni najít komplement prvku ve svazu, nebo říct, že neexistuje.
- Věta: Jestliže je komplementární svaz současně distributivní, tak všechny komplementy jsou určeny jednoznačně.
- Příklad: Komplement v množinovém svazu $(2^A, \cup, \cap)$ je doplněk množiny, jak jsme zvyklí na unární operaci doplňku.
- Definice: Booleho algebra je každý komplementární distributivní svaz.
- Příklad: $(2^A, \cup, \cap)$ je Booleho algebra.
- Využití Booleho algebry: Zákonitosti v Booleho algebře dovolují modelovat a zjednodušovat logické výrazy nebo množinové výrazy.
- Co jsou to de Morganova pravidla a) v teorii množin, b) v logice, c) v Booleho algebře?

Seznam literatury:

Beránek, 2011 Jaroslav Beránek: Vybrané kapitoly z algebry. Skriptum Pdf, počet stran 70. Doplnění obsahu předmětů Algebra 1 a Algebra 3 na PdF pro budoucí učitele 2.stupně. Brno 2011.

Budínová, I., 2013 Irena Budínová: Polynomy. Text určený studentům učitelství matematiky, Brno 2013. Počet stran 56.

Horák, 2002 P. Horák: Cvičení z algebry a teoretické aritmetiky I, Brno 2002. Sbírka příkladů na Přírodovědecké fakultě MU. Cvičení pokrývá zhruba látku v předmětech Základy matematiky, Algebra 1, Algebra 2 vyučovaných na Pedagogické fakultě.

Fajmon, 2022 B.Fajmon: Algebra 1. Doplnění přednášek, elektronický text.

Fajmon, 2023 B.Fajmon: Základy matematiky – verze 2023. Doplnění přednášek v předmětu MA0001, počet stran 153.

Fajmon, 2024 B.Fajmon: Algebra 2. Doplnění přednášek, elektronický text.

Kopka, J., 1991 Jan Kopka: Svazy a Booleovy algebry (Ústí nad Labem 1991, zejména str. 19-82). Pan profesor Kopka napsal svůj text z té pozice, že by rád přehledně a srozumitelně podal přehled pojmů algebry a diskrétní matematiky, aby byla vidět její krása. Kniha je hlubším rozvedením pojmu uspořádaná množina uvedeným v předmětu Základy matematiky.

Pinter, 2010 Charles Pinter: A book of Abstract Algebra, 2010. Jedná se o reprint druhého vydání z roku 1990. Neobyčejně čtivý text, napsaný z té pozice, že algebra je důležitá a má důležitá uplatnění.

Rosický, J., 2000 Jiří Rosický: Algebra – grupy a okruhy 2000, reprint textu z roku 1985. Tento text se hodně shoduje s osnovou předmětu Algebra 1 na PdF, nicméně jen až jako doplnění čtivější knihy (Pinter, 2010).