Aritmetika a algebra I

Literatura k předmětu:

[BeDla] Bečvář J., Dlab V.: *Od aritmetiky k abstraktní algebře.* Serifa, Praha, 2016.

[Be] Bečvář J.: *Lineární algebra.* Matfyzpress, Praha, 2010. (pouze po stranu 60)

Podmínky udělení zápočtu:
1. úspěšné napsání průběžné písemné práce v semestru, 2. samostatné vypracovávání domácích úkolů v průběhu semestru (bude ověřeno u testu 2), 3. úspěšné napsání závěrečné písemné práce na konci semestru či začátkem zkouškového období (příklady pokrývající zbytek semestru).

Požadavky ke zkoušce:
ústní část: dobrá znalost teorie v rozsahu probíraném na seminářích (včetně úloh zadávaných k samostatnému rozmyšlení).

Osnova předmětu

1. Definice, věta, důkaz. Typy důkazů vět ve tvaru implikace: přímý, nepřímý, sporem. Poznámka k rozdílu mezi rovnicí a rovností. $a^n \pm b^n$, součet prvních n členů geometrické posloupnosti.

2. Mohutnost (kardinalita) množiny, množiny spočetné a nejvýše spočetné, $|\mathbb{N}| = \aleph_0$, charakterizace nekonečných množin pomocí vlastních podmnožin. Mohutnost jednotlivých číselných oborů: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

3. Úvod do algebraických struktur. Zákon komutativní, asociativní, distributivní. Binární operace.
   - Algebraické struktury s jednou binární operací: grupoid, pologrupa, monoid, grupa. Grupa: motivace, definice, příklady (číselné grupy, translace, matice, ...).
   - Algebraické struktury se dvěma binárními operacemi: pole, těleso; příklady pole ($\mathbb{R}, \mathbb{C}, \mathbb{Z}_p$). Počítání v poli.

4. Relace, zobrazení, funkce. Definice zobrazení, injekce, surjekce, bijekce, graf zobrazení. Rozklad zobrazení na surjekci a injekci. Transformace a permutace množiny.
   Příklady relací. Uspořádaná a neuspořádaná dvojice, kartézský součin, n-tá kartézská mocnina množiny. Binární relace, relace z množiny do množiny, relace v množině, kartézský graf. Relace složená, inverzní. Relace reflexivní, symetrická, tranzitivní, antisymetrická. Asociativita skládání relací (a z toho plynoucí asociativita skládání zobrazení i funkcí), $(R_1 \circ R_2)^{-1} = R_2^{-1} \circ R_1^{-1}$.
   Relace ekvivalence na množině, rozklad množiny, třída (blok) ekvivalence, faktorová množina; ekvivalence na množině indukuje její rozklad.
   Hasseův diagram, svaz dělitelů. Prvek nejmenší, největší, minimální, maximální. Množina uspořádaná částečně, úplně (lineárně). Lexikografické uspořádání.

5. Permutace: skládání permutací, inverzní permutace, inverze, znaménko, rozklad na nezávislé cykly, transpozice, umocňování permutací.

6. Algebraické struktury II:
   - algebraické struktury se dvěma binárními operacemi: okruh, obor integrity; motivace, příklady.

7. Přirozená čísla, zavedení genetickou metodou, čísla von Neumannova. Zavedení sčítání a násobení přirozených čísel. Princip matematické indukce a princip dobrého uspořádání, ekvivalence těchto principů. Důkaz matematickou indukcí. Součty mocnin přirozených čísel.

8. Prvočísla. Eukleidova věta o nekonečném počtu prvočísel. Eratosthenovo síto. Matijasevičova parabola. Mersennova čísla a prvočísla, sudá dokonalá čísla, vztah mezi nimi: věta Eukleidova a Eulerova. Fermatova čísla a jejich vlastnosti, věta o konstruovatelnosti pravidelných n-úhelníků pomocí pravítka a kružítka.

9. Dělitelnost. Dělitel, násobek, největší společný dělitel, nejmenší společný násobek, čísla nesoudělná. $(\mathbb{N}, \leq)$ jako svaz, Hasseovy diagramy. Kongruence modulo n, aritmetické operace v $\mathbb{Z}_n$, dělení v $\mathbb{Z}_n$ a v $\mathbb{Z}_p$. Malá Fermatova věta. Základní kritéria dělitelnosti, odvození.

10. Dělení se zbytkem, Eukleidův algoritmus, Bézoutova věta. Gaussova věta a Eukleidovo lémma, Základní věta aritmetiky. Porovnání Malé Fermatovy věty a věty Bezoutovy. Vyjádření NSD a nsn pomocí součinu mocnin prvočísel. Zápis čísel v jiných numeračních soustavách.

11. Řetězové zlomky: vyjádření racionálních čísel řetězovými zlomky, rozvoj iracionálního čísla do řetězového zlomku, konvergenty a jejich efektivní výpočet pomocí rekurentních formulí. Chování posloupnosti konvergentů (střídavě jsou větší a menší než přesná hodnota řetězového zlomku), ideové zdůvodnění.

12. Konstrukce aditivní grupy celých čísel.

1 Definice, věta, důkaz

Definice: pozor: netvrdíme, že *čtverec je čtyřúhelník takový, že...*, ale měly by se vyskytnout výrazy typu: *říkáme, že...*; *nazýváme*; *označujeme*; ...

Věty (matematické): pozor: není-li pravdivost výroku dokázána, nejedná se o matematickou větu (může se jednat o hypotézu).

V matematice máme zpravidla věty ve tvaru:

- **elementárního výroku** (např. $\sqrt{2}$ je iracionální číslo),
- **implikace** (např. $\forall a, b, c \in \mathbb{R}: \ a = b \implies ac = bc$),
- **ekvivalence** (např. $\forall a, b \in \mathbb{R}: \ a^2 + b^2 = 0 \iff (a = 0 \wedge b = 0)$).

Důkazy vět ve tvaru ekvivalence:
Jak dokazujeme ekvivalenci $A \iff B$? Dokážeme $(A \implies B) \wedge (B \implies A)$. Jak dokazujeme ekvivalenci tří výroků A, B, C? Stačí dokázat „kolečko“, tj. dokážeme

$$(A \implies B) \wedge (B \implies C) \wedge (C \implies A).$$

Důkazy vět ve tvaru implikace:
Typy důkazů vět ve tvaru implikace, tj. ve tvaru $A \implies B$:

- přímý: $A \implies B_1$, $B_1 \implies B_2$, $B_2 \implies B_3$, ..., $B_n \implies B$
- nepřímý: je to vlastně přímý důkaz obměněné implikace: $\neg B \implies \neg A$. Vychází z toho, že implikace je s ní ekvivalentní:

  $$(A \implies B) \iff (\neg B \implies \neg A)$$

- sporem: místo $A \implies B$ dokazujeme $\neg(A \wedge \neg B)$, neboť platí

  $$(A \implies B) \iff \neg(A \wedge \neg B)$$

  Předpokládáme tedy A a to, že neplatí tvrzení, tj. $\neg B$. Typický začátek důkazu sporem je: *kdyby neplatilo B, tak by ...*

Pokud A neplatí, je $A \implies B$ splněno automaticky, nemusíme nic dokazovat.

Příklad důkazu sporem: *Jestliže má posloupnost $\{a_n\}$ limitu, pak je tato limita právě jedna.*
Důkaz sporem: Kdyby neplatilo B, tj. kdyby měla posloupnost více limit, tak by měla aspoň dvě různé limity, ozn. je a a b, tj. ... $a - \varepsilon < a_n < a + \varepsilon$ a $b - \varepsilon < a_n < b + \varepsilon$. Bez újmy na obecnosti nechť např. je $a < b$. Pak z předpokladu A a negace $\neg B$ plyne (po úvahách a úpravách):

$$a_n < a + \varepsilon < b - \varepsilon < a_n \,,$$

tj. $a_n < a_n$, což není možné; říkáme, že jsme došli ke sporu. Neplatí tedy $A \wedge \neg B$, tj. platí $\neg(A \wedge \neg B)$, což je ekvivalentní s $A \implies B$, takže je tato implikace dokázána. □

Poznámka k rozdílu mezi rovnicí a rovností $L(x) = P(x)$
(pro jednoduchost uvažujeme jednu neznámou / proměnnou):

- rovnice: úloha najít všechna x z dané množiny taková, aby $L(x) = P(x)$,
- rovnost: výrok, že pro všechna x z dané množiny platí: $L(x) = P(x)$.

2 Množiny

Jak je tomu s definicí množiny? Množina je tzv. *primitivní pojem*, je to tedy cokoli, co vyhovuje axiómům teorie množin. S axiómy teorie množin (existuje několik různých přístupů) se seznámíme v 5. ročníku.

Axiómaticky budovaná teorie je založena na souboru axiómů, které vypovídají něco o vlastnostech jinak nespecifikovaných a nedefinovaných pojmů, tzv. *primitivních pojmů*. Například v planimetrii jsou primitivními pojmy *bod* a *přímka*.

Výhoda axiómatického přístupu k matematice: za primitivní pojmy lze dosadit cokoli, co vyhovuje podmínkám (axiómům). Matematika se tak stává abstraktní, tj. nemá konkrétní obsah.

S nadsázkou a humorem lze říci: matematika budovaná axiómaticky je o ničem, což je moc dobře.

Mohutnost (kardinalita) množiny
Říkáme, že množiny A a B mají stejnou mohutnost, existuje-li bijekce množiny A na množinu B. (samozřejmě pak také existuje bijekce množiny B na množinu A, je to inverzní zobrazení k původní bijekci)

bijekce – vzájemně jednoznačné zobrazení, tj. zobrazení, které je zároveň prosté (*injektivní*) a na (*surjektivní*).

Jak si představit mohutnost množiny intuitivně? U konečné množiny jako počet jejích prvků. U nekonečné to začne být skutečně zajímavé, lze například dokázat, že

$$|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| < |\mathbb{R}| = |\mathbb{C}| \ .$$

Mohutnost množiny A značíme $|A|$. Mohutnost množiny $\mathbb{N}$ značíme $\aleph_0$, čteme *alef nula* (alef je první písmeno hebrejské abecedy). O množinách, které mají mohutnost $\aleph_0$ (neboli stejnou mohutnost, jako množina přirozených čísel), říkáme, že jsou *spočetné*. Množiny, které jsou buď konečné, nebo spočetné, nazýváme *nejvýše spočetné*.

Příklady spočetných množin:

- množina všech přirozených čísel větších než milion $\{10^6+1, 10^6+2, 10^6+3, 10^6+4, ...\}$,
- množina všech uspořádaných dvojic přirozených čísel $\mathbb{N}^2$,
- množina všech uspořádaných trojic přirozených čísel $\mathbb{N}^3$,
- množina všech prvočísel $\mathbb{P}$,
- množina všech kladných sudých čísel $2\mathbb{N}$,
- množina všech celočíselných násobků sedmnácti $17\mathbb{Z}$,
- množina všech uspořádaných n-tic racionálních čísel $\mathbb{Q}^n$.

Příklady nespočetných množin:

- množina všech uspořádaných n-tic reálných čísel $\mathbb{R}^n$.
- množina všech komplexních čísel $\mathbb{C}$,
- množina všech uspořádaných n-tic komplexních čísel $\mathbb{C}^n$,
- množina všech funkcí $\{f : \mathbb{R} \to \mathbb{R}\}$.

Pozor: množina všech funkcí $\{f : \mathbb{R} \to \mathbb{R}\}$ má mohutnost ostře větší než $|\mathbb{R}|$.

Charakterizace nekonečných množin:
Pro nekonečnou množinu je charakteristické, že existuje nějaká její vlastní[1] podmnožina.

[1] Vlastní podmnožina množiny A – takto se nazývá podmnožina množiny A, která není rovna celé množině A.

- Všimněte si, že nekonečnou množinu od konečné odlišuje tato vlastnost: nekonečná množina obsahuje vlastní podmnožinu, která je s ní ekvivalentní (tj. mají stejnou mohutnost, tj. existuje mezi nimi bijekce). U konečných množin už tohle neplatí. Takto definoval nekonečnou množinu Richard Dedekind, viz [BeDla], str. 26 nahoře:

  Řekneme, že množina M je nekonečná, jestliže existuje injektivní (neboli prosté) zobrazení $f : M \to M$ takové, že $f(M) \neq M$.

- Probádejte definici kartézské mocniny. Zpočátku to vypadá jednoduše: $A^2 := A \times A$, dále $A^3 := A \times A \times A$, ...
  Dohodneme-li se, že místo $[a]$ budeme psát pouze samotný prvek a, můžeme dodefinovat $A^1 := A$.
  Proč však (pouze pro $A \neq \emptyset$) dodefinováváme $A^0 := \{\emptyset\}$? Bude pak platit, že

$$A^m \times A^n = A^{m+n} \,?$$

  Konkrétně: bude $A^n \times A^0 = A^n$?

2.1 Mohutnost číselných oborů

Jak ukážeme, že množiny $\mathbb{Z}, \mathbb{Q}$ jsou spočetné? Stačí zkonstruovat bijekci těchto množin na množinu $\mathbb{N}$ (jednoduše řečeno: stačí ukázat, že lze všechny prvky těchto množin očíslovat přirozenými čísly).

$\mathbb{Z}$ je spočetná množina: $0 \mapsto 1$, $1 \mapsto 2$, $-1 \mapsto 3$, $2 \mapsto 4$, $-2 \mapsto 5$, $3 \mapsto 6$, $-3 \mapsto 7$, $4 \mapsto 8$, $-4 \mapsto 9$, ...

Zkonstruovali jsme tedy bijekci mezi množinami $\mathbb{N}$ a $\mathbb{Z}$, mají tedy stejnou mohutnost, tj.

$$|\mathbb{N}| = |\mathbb{Z}| \ .$$

$\mathbb{Q}$ je spočetná množina: stačí ukázat, že množina kladných zlomků je spočetná.

$\frac{1}{1}$ (1)	$\frac{1}{2}$ (2)	$\frac{1}{3}$ (4)	$\frac{1}{4}$ (7)	$\frac{1}{5}$ (11)	$\frac{1}{6}$ (16)	...
$\frac{2}{1}$ (3)	$\frac{2}{2}$ (5)	$\frac{2}{3}$ (8)	$\frac{2}{4}$ (12)	$\frac{2}{5}$ (17)	$\frac{2}{6}$ (23)	...
$\frac{3}{1}$ (6)	$\frac{3}{2}$ (9)	$\frac{3}{3}$ (13)	$\frac{3}{4}$ (18)	$\frac{3}{5}$ (24)	$\frac{3}{6}$ (31)	...
$\frac{4}{1}$ (10)	$\frac{4}{2}$ (14)	$\frac{4}{3}$ (19)	$\frac{4}{4}$ (25)	$\frac{4}{5}$ (32)	$\frac{4}{6}$ (40)	...
$\frac{5}{1}$ (15)	$\frac{5}{2}$ (20)	$\frac{5}{3}$ (26)	$\frac{5}{4}$ (33)	$\frac{5}{5}$ (41)	$\frac{5}{6}$ (50)	...
$\frac{6}{1}$ (21)	$\frac{6}{2}$ (27)	$\frac{6}{3}$ (34)	$\frac{6}{4}$ (42)	$\frac{6}{5}$ (51)	$\frac{6}{6}$ (61)	...
...	...	...	...	...	...	...

Číslování jednotlivých zlomků probíhá ve směru vedlejší diagonály. Je zřejmé, že stejně bychom postupovali u množiny všech uspořádaných dvojic přirozených čísel – její prvky by šlo očíslovat přirozenými čísly stejným způsobem, tj. $|\mathbb{N}| = |\mathbb{N}^2|$.

Pokud bychom chtěli číslovat nejen kladné, ale i záporné zlomky, tak bychom výše uvedený postup snadno modifikovali (podobně jako u číslování celých čísel): $0 \mapsto 1$, $\frac{1}{1} \mapsto 2$, $-\frac{1}{1} \mapsto 3$, $\frac{1}{2} \mapsto 4$, $-\frac{1}{2} \mapsto 5$, $\frac{2}{1} \mapsto 6$, $-\frac{2}{1} \mapsto 7$, $\frac{1}{3} \mapsto 8$, $-\frac{1}{3} \mapsto 9$, ..., tj.

$$|\mathbb{N}| = |\mathbb{Q}| \ .$$