X.1 Spočetnost etc.

Definice. Množina A se nazve spočetná ("countable"), jestliže existuje vzájemně jednoznačné zobrazení mezi A a $\mathbb{N}$. Názorně: prvky A lze srovnat do prosté posloupnosti $A = \{a_1, a_2, \dots\}$.

Poznámky. ① příklady spočetných množin: triviálně $\mathbb{N}$, $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots\}$; množina všech prvočísel, množina všech sudých čísel.
Obecně každá nekonečná podmnožina $\mathbb{N}$ je spočetná.
Paradoxní vlastnost spočetných množin: lze je vzájemně jednoznačně zobrazit na jejich podmnožinu.
② množina racionálních čísel $\mathbb{Q}$ je spočetná.
③ sjednocení dvou spočetných množin je spočetné. Obecněji: $\forall j \in \mathbb{N}$ je A_j spočetná $\implies$ $\bigcup_j A_j$ je spočetná

Věta X.1. [Cantor.] Množina $\mathbb{R}$ je nespočetná.

Poznámky. Řekneme, že množina B má mohutnost kontinua, pokud existuje vzájemně jednoznačné zobrazení mezi B a množinou reálných čísel.
• interval $(0, 1)$ má mohutnost kontinua. Dá se ukázat, že každý netriviální interval má mohutnost kontinua. Také množina iracionálních čísel má mohutnost kontinua. Všechny obvyklé podmnožiny $\mathbb{R}$ jsou buď spočetné, nebo mají mohutnost kontinua.
• G. Cantor v roce 1878 zformuloval tzv. hypotézu kontinua (HC):

Je-li $A \subset \mathbb{R}$ nekonečná množina, tak potom
buď A je spočetná, nebo A má mohutnost kontinua.

Jinými slovy, každá nekonečná množina čísel se dá vzájemně jednoznačně zobrazit buď na $\mathbb{N}$, nebo na $\mathbb{R}$.
Dlouho se nevědělo, zda hypotéza kontinua platí nebo ne. V roce 1938 dokázal překvapivě K. Gödel, že hypotézu kontinua nelze vyvrátit. V roce 1963 pak dokázal P. Cohen, že hypotézu kontinua nelze dokázat. Jde tedy o „nerozhodnutelné" tvrzení; přesněji řečeno, tvrzení nezávislé na axiomech teorie množin.

Definice. Číslo x_0 se nazve algebraické ($x_0 \in \mathcal{A}$), pokud existuje nenulový polynom $p(x)$ s celočíselnými koeficienty takový, že $p(x_0) = 0$. V opačném případě se x_0 nazve transcendentní.
Číslo x_0 se nazve vyčíslitelné ($x_0 \in \mathcal{C}$, "computable"), jestliže existuje konečný algoritmus (program), který počítá x_0 s libovolnou přesností. Alternativně: existuje konečný algoritmus, který pro každé $r \in \mathbb{Q}$ rozhodne, zda platí $x_0 < r$.

Poznámky.
① $\mathbb{Q} \subset \mathcal{A}$ striktně, neboť např. $\sqrt{2} \in \mathcal{A} \setminus \mathbb{Q}$
② čísla e, π jsou transcendentní (těžké; Hermite 1873, Lindemann 1882). Ovšem jsou to čísla vyčíslitelná, např. díky vzorcům $e = 1/0! + 1/1! + 1/2! + \dots$, $\pi/4 = 1/1 - 1/3 + 1/5 - 1/7 + \dots$.

③ číslo x_0 se nazve konstruovatelné ($x_0 \in \mathcal{K}$), pokud délku x_0 lze najít eukleidovskou konstrukcí (tj. pomocí kružítka a pravítka; délka 1 je zadána). Lze dokázat $\mathbb{Q} \subset \mathcal{K} \subset \mathcal{A}$. Problém kvadratury kruhu je ekvivalentní konstruovatelnosti $\sqrt{\pi}$, což by ovšem implikovalo konstruovatelnost π, což dle Lindemanna není pravda. Tedy kvadratura kruhu je neřešitelný problém.
④ hierarchie číselných množin:

- základní množina $\mathbb{N} \cup \{0\}$ spolu s operacemi $\cdot$ a $+$
- operace $-$ vede na množinu $\mathbb{Z}$
- operace $/$ vede na množinu $\mathbb{Q}$
- připustíme-li $\sqrt[k]{\ }$, máme algebraická čísla $\mathcal{A}$
- limitní opakování předchozích operací vede na vyčíslitelná čísla $\mathcal{C}$

Neplatí tedy $\mathbb{R} = \mathcal{C}$? Zdaleka ne, jak plyne z následujícího.

Lemma X.2 [„Abecední lemma“] Nechť $\mathcal{Z}$ je konečná nebo spočetná množina („abeceda“), nechť $\mathcal{P}$ je množina všech konečných posloupností („nápisů“) ze $\mathcal{Z}$. Potom $\mathcal{P}$ je spočetná.

Poznámka. V Lemmatu X.2 je podstatné, že uvažujeme jen konečné posloupnosti. Množina nekonečných nápisů je nespočetná již v případě dvouprvkové abecedy, jak snadno dokážeme Cantorovým diagonálním argumentem.

Poznámky. ① Důsledek: množina $\mathcal{A}$ je spočetná. Nechť Π je množina všech polynomů z definice $\mathcal{A}$. Každý $p \in \Pi$ jednoznačně odpovídá konečné posloupnosti koeficientů ze $\mathbb{Z}$. Tedy

$$\mathcal{A} = \bigcup_{p \in \Pi} \{x_0 \in \mathbb{R};\ p(x_0) = 0\}$$

je spočetné sjednocení konečných množin.
② Důsledek: množina $\mathcal{C}$ je spočetná. Neboť program lze chápat jako konečný nápis v konečné abecedě ASCII.
③ Protože $\mathbb{R}$ je nespočetná, jsou nutně množiny $\mathbb{R} \setminus \mathcal{A}$, $\mathbb{R} \setminus \mathcal{C}$ neprázdné. Tedy existují „nevyčíslitelná čísla“ – jejich desetinný rozvoj obsahuje více informace, než kolik lze popsat konečným algoritmem.
Poznamenejme, že nekonečný program by mohl popsat libovolné číslo: První řádek by tiskl první číslici, druhý řádek druhou, ...

X.2 Základy analýzy – teorie množin

V analýze studujeme různé objekty: čísla, funkce, relace, množiny, posloupnosti, ... To vše lze fakticky redukovat na pojem množiny:

- Přirozená čísla reprezentujeme množinami takto:

$$\begin{aligned} &0 \ldots \emptyset \qquad \text{(prázdná množina)} \\ &1 \ldots \{\emptyset\} \qquad \text{(množina, jejímž jediným prvkem je } \emptyset\text{)} \\ &2 \ldots \{\emptyset, \{\emptyset\}\} \\ \text{atd.} \end{aligned}$$

  Operaci $n \mapsto n+1$ odpovídá $x \mapsto x \cup \{x\}$. Relaci $\leq$ odpovídá $\subset$. Všimněme si též, že množina reprezentující n má právě n prvků.

- ,,nevýhodou" množiny je, že nezná pořadí prvků a nepřipouští jejich opakování, tj. $\{a, b, a\} = \{a, b\} = \{b, a\}$, $\{a, a\} = \{a\}$ atd. Užitečným trikem je zavedení *uspořádané dvojice*

$$\langle a, b\rangle = \{a, \{a, b\}\}$$

  Pro tuto množinu (množin) již platí $\langle a, b\rangle = \langle c, d\rangle$ právě když $a = c$ a zároveň $b = d$; tedy $\langle a, b\rangle \neq \langle b, a\rangle$, pokud $a \neq b$.

- racionální čísla nyní můžeme reprezentovat jako dvojice přirozených čísel

- reálná čísla lze reprezentovat aproximujícími posloupnostmi racionálních čísel, přičemž posloupnost $a_1, a_2, a_3, \ldots$ reprezentujeme množinou uspořádaných dvojic $\{\langle 1, a_1\rangle, \langle 2, a_2\rangle, \ldots\}$.

- obecně funkci $x \mapsto f(x)$ reprezentujeme množinou všech uspořádaných dvojic tvaru $\langle x, f(x)\rangle$

- (binární) relaci reprezentujeme jednoduše množinou všech dvojic, pro něž relace platí, tj. např. $<$ bude reprezentována množinou $\{\langle 0, 1\rangle, \langle -2, -1\rangle, \ldots\}$.

Celý ,,svět analýzy" je tak reprezentován v univerzu množin (množin množin, množin množin množin, ...), spočívajícím na prázdné množině coby základním stavebním prvku. Veškeré operace týkající se funkcí, relací, posloupností se tak převádějí na operace s množinami. To má ten praktický význam, že jazyk matematiky se nesmírně zjednodušuje, neboť kromě logických symbolů: $\forall$, $\exists$, $\implies$, $\neg$, $=$ vystačíme s jediným ,,mimologickým" predikátem $\in$.

Popsat ,,základy analýzy" pak znamená popsat (tj. axiomatizovat) operace s množinami. Zmíníme stručně (vybrané) axiomy z tzv. Zermelo-Fraenkelovy axiomatizace teorie množin. (Axiomy uvádíme v přirozené řeči a mírně nepřesně.)

1. **axiom existence množiny**: existuje alespoň jedna množina

2. **axiom extenzionality**: (libovolné dvě) množiny se rovnají, právě když mají stejné prvky. Speciálně: je jenom jedna prázdná množina.

   Všechny další axiomy tvrdí existenci určitých množin, tj. de facto říkají, za jakých okolností je množina ,,dobře definována" (d.d.)

3. **axiom dvojice**: jsou-li a, b d.d., pak $\{a, b\}$ je d.d. Tento axiom sakcionuje výše uvedené vytváření přirozených čísel.

4. **axiom nekonečna**: existuje nekonečná množina (fakticky tvrdí existenci množiny přirozených čísel).

   Zde je vhodné poznamenat, že korektní matematický důkaz je vždy *konečná* posloupnost kroků, dovolených příslušnými axiomy. Tedy pouhý axiom dvojice dokáže vyrobit libovolně velké n, ale nikdy ,,aktuální nekonečno" v podobě množiny $\mathbb{N}$. Proto potřebujeme zvláštní axiom nekonečna.

5. **axiom sumy**: jsou-li a, b d.d., pak $a \cup b$ je d.d. Axiom je fakticky obecnější: je-li $A = \{a_1, a_2, \dots\}$ d.d. libovolná množina množin, pak pak $\bigcup A = a_1 \cup a_2 \cup \dots$ je d.d.

6. **axiom vydělení**: je-li a d.d. množina a $\phi(x)$ formule s volnou proměnnou x, pak $\{x \in a;\ \phi(x) \text{ platí}\}$ je d.d.

   Poznamenejme, že ,,naivní" teorie množin, která by připouštěla množiny $\{x; \phi(x) \text{ platí}\}$ by obsahovala spor (Russell 1901): Definovali bychom totiž $R := \{x;\ x \notin x\}$. Potom ovšem $R \in R \iff R \notin R$

7. **axiom výběru**: je-li A d.d. množina *neprázdných* množin, pak je d.d. ,,selekční" množina S taková, že $S \cap a \neq \emptyset$ pro každé $a \in A$.

   Axiom výběru (AC) má zvláštní postavení. Vypadá přirozeně a občas je nutné jej použít. Na druhou stranu je jím možno ,,vytvořit" množiny velmi zvláštních vlastností (viz například známý Banach-Tarského paradox).

Poznámky. Axiomy ZF (neuvádíme zde všechny) umožňují popsat veškeré běžné operace s množinami a tedy i modelovat ,,svět analýzy". K dokonalé spokojenosti bychom však chtěli vědět, že náš systém axiomů je bezesporný ("consistent"); také bychom na základě těchto axiomů chtěli umět dokázat (či vyvrátit) všechna myslitelná tvrzení.
Slavné Gödelovy věty o neúplnosti říkají, že toto není možné. Pokud ZF je bezesporné, pak: 1. bezespornost ZF nelze dokázat v rámci ZF a 2. v ZF lze formulovat tvrzení, která jsou zde nedokazatelná, leč (viděno zvenčí) jsou pravdivá.
Dobrá zpráva je, že spor v ZF se zatím nepodařilo najít a také že bezespornost ZF je možné dokázat (leč jen v rámci jisté ,,bohatší teorie", která sama může obsahovat spor).
Hypotéza kontinua je příkladem tvrzení, které je v rámci ZF nerozhodnutelné. Přesněji řečeno: je-li ZF bezesporná, pak ZF+HC je bezesporná (Gödel 1938) a také ZF+$\neg$HC je bezesporná (Cohen 1963).