Введение в математическую логику и теорию алгоритмов

Семинар № 1: Множества, отношения, функции.

Из школьного курса вы знаете, что геометрия строится *аксиоматически*: выписан некоторый набор утверждений — *аксиом* — принимаемых без доказательства, а все остальные утверждения из них *выводятся* чисто логическим путем, то есть для них строятся *доказательства*. В учебнике геометрии и аксиомы, и доказательства записываются на русском (не слишком формальном) языке. Но известно, что всё это можно записать на абсолютно точном языке (по аналогии с языком программирования), так что не будет никаких разночтений.

Можно ли подобное сделать для всей математики? Ответ: да, для этого разработана **теория множеств** — это и *язык*, в котором формулируются утверждения (и доказательства), и набор *аксиом*, из которых все дальнейшие математические теоремы предполагается выводить.

Язык теории множеств: все объекты и понятия математики определяются в терминах *множеств* и отношения *принадлежности* $\in$. Выражение $x \in A$ читается как «объект x является *элементом* множества A» или «x принадлежит A». Аксиомы будут выписаны на первых лекциях; правила вывода одних утверждений из других появятся ещё позже. На семинаре же будем рассуждать неформально.

Принцип объемности (или *аксиома равенства множеств*).
Два множества равны $\iff$ *они состоят из одних и тех же элементов:*

$$A = B \qquad \iff \qquad \forall x\ (x \in A \ \Leftrightarrow\ x \in B).$$

Способы построения множеств: перечисление элементов $\{a, b, c\}$; либо указание принципа отбора элементов $\{x \mid P(x)\}$, где P — некоторое свойство. Оба способа чреваты проблемами: перечисление — если множество бесконечно, приходится использовать многоточие $\{1, 1, 2, 3, 5, 8, \ldots\}$, а указание принципа отбора — **парадокс Рассела** $\{x \mid x \notin x\}$ (вспомните рассуждение, приводящее к противоречию). Для того, чтобы избежать известные парадоксы, применяют более слабый способ формирования множества $\{x \in A \mid P(x)\}$. Когда его всё-таки не хватает, например, для определения объединения множеств, требуется каждый раз давать обоснование, почему эта запись корректна (с точки зрения аксиом — почему из этих аксиом можно доказать, что указанное множество существует).

Обозначения: пустое множество $\varnothing$ (по определению, это то (единственное) множество, которое не имеет элементов: $\forall x\,(x \notin \varnothing)$); подмножество $A \subseteq B$; множество всех подмножеств $\mathcal{P}(A) = \{B \mid B \subseteq A\}$; определения операций над множествами — пересечение, объединение, разность и др. Например, $A \cap B = \{x \mid x \in A \text{ и } x \in B\}$.

Задачи

1. **а)** Умейте **доказывать** свойства $\cup$, $\cap$ и др. — коммутативность, ассоциативность, дистрибутивность.
   б) Докажите, что два определения симметрической разности эквивалентны: $A \triangle B \ = \ (A \setminus B) \cup (B \setminus A) \ = \ (A \cup B) \setminus (A \cap B)$.

Как в терминах множеств определить натуральные числа?
Способ **Фон Неймана**: $0 := \varnothing$, $(n+1) := n \cup \{n\}$.

2. Выпишите множества, представляющие числа 1, 2, 3. Сколько в них элементов?

3. Обозначим множество всех построенных выше натуральных чисел через $\mathbb{N} = \{0, 1, 2, \ldots\}$. Докажите, что $(\mathbb{N}, \subseteq)$ — линейный порядок.[1]

Но имеются и другие математические объекты, для которых представление в терминах множеств не так очевидно: функции, векторы, свойства, отношения и др. Оказывается, что ключевым здесь является представление **упорядоченной пары** $\langle x, y\rangle$ множеств x и y. Приведем определение **Куратовского** (есть и другие):

$$\langle x, y\rangle \;=\; \big\{\, \{x\},\ \{x, y\}\,\big\}.$$

4. Докажите, что для указанной кодировки упорядоченных пар справедлив основной закон: *Первая и вторая компонента упорядоченной пары восстанавливаются однозначно*:

$$\langle a, b\rangle = \langle c, d\rangle \quad\Longrightarrow\quad a = c \ \text{ и } \ b = d.$$

Отношения и функции

Декартово произведение: $A \times B \;=\; \{\, \langle a, b\rangle \;\mid\; a \in A,\ b \in B\,\}$,
$A \times B \times C \;:=\; (A \times B) \times C$, и т.д.

n-местное отношение на A — это $R \subseteq A^n$ (т.е. некоторый набор упорядоченных n-ок элементов из A).

Функция (всюду определенная) из A в B (обозначение: $f\colon A \to B$) — это такое двуместное отношение между множествами A и B, т.е. такое $f \subseteq (A \times B)$, для которого выполнены следующие условия:

- (функциональность, «образ единственен»)
$$\forall x \in A\ \forall y_1, y_2 \in B\ \big(\,\langle x, y_1\rangle \in f \text{ и } \langle x, y_2\rangle \in f \Rightarrow y_1 = y_2\,\big).$$
- (всюду определенность, или тотальность, «образ существует»)
$$\forall x \in A\ \exists y \in B\ \langle x, y\rangle \in f.$$

Итак, два условия вместе дают: $\forall x \in A\ \exists! y \in B\ \langle x, y\rangle \in f$. Этот единственный y обозначают $y := f(x)$. Без условия тотальности получаем определение **частично определенной функции из A в B**. Пример: $y = \mathrm{tg}(x)$.

Инъективная функция: $\langle x_1, y\rangle \in f$ и $\langle x_2, y\rangle \in f \Rightarrow x_1 = x_2$.
Иначе говоря: $f(x_1) = y = f(x_2) \Rightarrow x_1 = x_2$.

Сюръективная функция: $\forall y \in B\ \exists x \in A\ \langle x, y\rangle \in f$.

Как видим, эти два условия «двойственны» двум условиям из определения *функции*.

---

[1] Структура $(A, \leqslant)$ называется *линейным порядком*, если выполняются условия:
(рефлексивность) $\forall x\,(x \leqslant x)$
(транзитивность) $\forall x, y, z\,(x \leqslant y \text{ и } \leqslant z \ \Rightarrow\ x \leqslant z)$
(антисимметричность) $\forall x, y\,(x \leqslant y \text{ и } y \leqslant x \ \Rightarrow\ x = y)$
(линейность) $\forall x, y\,(x \leqslant y \text{ или } y \leqslant x)$

Биекция из A **в** B — это одновременно инъективная и сюръективная функция $f\colon A \to B$. **Равномощные множества** A **и** B — если $\exists$ биекция $f\colon A \to B$. Обозначение: $A \sim B$ либо[2] $|A| = |B|$.

Если существует инъекция $f\colon A \to B$, но не существует биекции, то пишем $|A| < |B|$ (мощность меньше). Если $A \sim B' \subseteq B$, то пишем $|A| \leqslant |B|$. Другими словами, $|A| \leqslant |B|$, если существует инъекция $f\colon A \to B$.

Теорема Кантора–Бернштейна: *Если* $|A| \leqslant |B|$ *и* $|B| \leqslant |A|$, *то* $A \sim B$.

Следующее утверждение эквивалентно аксиоме выбора:

Для любых множеств A *и* B *имеем* $|A| \leqslant |B|$ *или* $|B| \leqslant |A|$.

5. **Теорема Кантора.** *Никакое множество* A *не равномощно* $\mathcal{P}(A)$.
   А точнее, всегда $|A| < |\mathcal{P}(A)|$.

   Доказательство. Допустим, существует биекция $f\colon A \to \mathcal{P}(A)$. Покажем, что f — не сюръективна. Для этого предъявим элемент из $\mathcal{P}(A)$, то есть некоторое подмножество $B \subseteq A$, которое не является значением $f(a)$ ни для какого $a \in A$. Возьмем $B := \{x \in A \mid x \notin f(x)\}$. Завершите рассуждение. □

6. Какие из перечисленных множеств равномощны, а где мощность увеличивается: $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$?

Множества, равномощные $\mathbb{N}$, называются **счетными**, а равномощные $\mathcal{P}(\mathbb{N})$ — мощности **континуум**.

Домашнее задание

7. Докажите, что $(\mathcal{P}(A), \triangle, \cap)$ — это кольцо, где $\triangle$ играет роль сложения, а $\cap$ — умножения.

8. Пусть $|A| = m$, $|B| = n$. Докажите, что всех функций $f\colon A \to B$ имеется n^m. Сколько: **а)** инъекций, если $|A| \leqslant |B|$? **б)*** сюръекций, если $|A| \geqslant |B|$? **в)** биекций, если $A \sim B$?

9. **а)** Вспомните, как доказывать равномощность $\mathbb{N} \sim (\mathbb{N} \times \mathbb{N})$, $\mathbb{N} \sim \mathbb{Q}$.
   б) Докажите: $\mathcal{P}(A)$ равномощно множеству всех функций $f\colon A \to \{0, 1\}$.

10. Какова мощность следующих множеств?
    – множество двухэлементных подмножеств $\mathbb{N}$,
    – множество конечных подмножеств $\mathbb{N}$,
    – множество бесконечных подмножеств $\mathbb{N}$,
    – множество конечных последовательностей $(a_1, \ldots, a_n)$ чисел из $\mathbb{N}$,
    – множество бесконечных последовательностей $(a_1, a_2, \ldots)$ чисел из $\mathbb{N}$,
    – множество функций $f\colon \mathbb{N} \to \mathbb{N}$.

11. **Композиция отношений**:
    если $R, S \subseteq (A \times A)$, то $R \circ S = \{\langle a, c\rangle \mid \exists b :\ \langle a, b\rangle \in R \text{ и } \langle b, c\rangle \in S\}$.

    а) Ассоциативная ли операция композиции?
    б) Вычислите всевозможные попарные композиции отношений $=, \neq, <, >, \leqslant, \geqslant$ на $\mathbb{N}$.

[2] Здесь $|A|$ «обозначает» мощность множества A. Точное определение сейчас не даем, но оно существует в теории множеств.

в) Докажите: композиция функций — функция; композиция сохраняет инъективность и сюръективность.

12. Определения рефлексивного, транзитивного отношения $R \subseteq A^2$ см. в сноске 1. Отношение $R \subseteq A^2$ называется *симметричным*, если из xRy всегда следует yRx. Здесь xRy — сокращение записи $\langle x, y\rangle \in R$. Приведите примеры:
а) рефлексивного, транзитивного, но не симметричного отношения на множестве из 2 (из 3) элементов;
б) нетранзитивного отношения на множестве из 2 элементов;
в) транзитивного, симметричного, но не рефлексивного отношения на множестве из 2 элементов.

13. Пусть $f\colon A \to B$, $X \subseteq A$, $Y \subseteq B$.

Образ множества X: $f(X) := \{f(a) \mid a \in X\}$.

Прообраз множества Y: $f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}$.

а) Дистрибутивно ли взятие образа относительно $\cup$? $\cap$? То есть

$f(X \cup X') = f(X) \cup f(X')$?
$f(X \cap X') = f(X) \cap f(X')$?

б) Дистрибутивно ли взятие прообраза относительно $\cup$? $\cap$? То есть

$f^{-1}(Y \cup Y') = f^{-1}(Y) \cup f^{-1}(Y')$?
$f^{-1}(Y \cap Y') = f^{-1}(Y) \cap f^{-1}(Y')$?