

Лекция

22–23 сентября

Множества

Константин Чухарев

Дискретная математика — Осень 2026



Логика множеств

Алгебра щедра: часто она даёт больше, чем у неё просят.

— Жан д'Аламбер

Множества говорят на языке логики

Два занятия строили язык: высказывания и связи, кванторы, методы доказательств.

Самих объектов, к которым язык применяется, ещё не было.

Сегодня появляется первый объект курса — **множество**.

- Принадлежность станет предикатом.
- Включение — импликацией.
- Операции — связками.

Каждое спорное место теории множеств сводится переводу к уже решённому вопросу логики.

Универсум и предикат принадлежности

Зафиксируем **универсум** U — все объекты текущей задачи.

Запись $x \in A$ — предикат от x : на каждом объекте универсума он истинен или ложен.

Пример

- $x \in \mathbb{N}$: истинно при $x = 3$, ложно при $x = \frac{1}{2}$.
- « x — студент группы ПМ-26»: предикат на множестве людей.

Множество полностью описывается предикатом принадлежности $x \in A$.

Знать множество — знать про каждый объект, лежит он внутри или снаружи.

Свойство задаёт множество

Из предиката получается множество объектов, которые его удовлетворяют:

$$\{x \in U \mid P(x)\}$$

Это **нотация порождающего свойства** (*set-builder notation*).

Пример

- $\{x \in \mathbb{N} \mid x \text{ чётно}\}$ — чётные числа.
- $\{x \in \mathbb{R} \mid x^2 = 2\}$ — множество из двух чисел.
- $\{x \in \mathbb{N} \mid x < 5\} = \{0, 1, 2, 3, 4\}$.

Одно множество — много описаний: $\{1, 2, 3\} = \{x \in \mathbb{N} \mid 0 < x < 4\}$.

Состав определяет множество: текст условия — лишь путь к нему.

Включение — импликация

Сравнить множества — сравнить предикаты принадлежности.

Определение 1

A — **подмножество** B (запись $A \subseteq B$), если каждый элемент A лежит в B :

$$\forall x. (x \in A) \rightarrow (x \in B).$$

Пример

Чётные числа — подмножество $\mathbb{Z}$: из « x чётно» следует « x целое».

Импликация с ложной посылкой истинна — поэтому $\emptyset \subseteq A$ для любого A .

Элементов, которые могли бы нарушить условие, нет.

Операции — связки

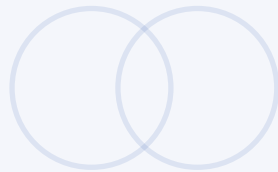
Связки собирают из предикатов новые предикаты — и из множеств новые множества.

Множества	Логика
$A \cup B$	$x \in A \vee x \in B$
$A \cap B$	$x \in A \wedge x \in B$
$\overline{A}$	$\neg(x \in A)$
$A \setminus B$	$x \in A \wedge x \notin B$
$A \subseteq B$	$\forall x. (x \in A) \rightarrow (x \in B)$

Пример

$x \in A \cap B$ означает « $x \in A$ и $x \in B$ » — один предикат, записанный двумя способами.

Каждому закону логики соответствует тождество множеств — переносом связок. Первый пример, де Морган, докажем после формального введения операций.



Наивная теория множеств

Множество — это многое, мыслимое как единое.

— Георг Кантор

Множество

Группировать объекты — базовое действие математики:

- буквы алфавита
- вершины графа
- простые числа

Определение 2

Множество — неупорядоченный набор различных объектов. Объекты, входящие в множество, называются его **элементами**.

Порядок элементов не важен, повторяющиеся элементы считаются один раз.

Пример

$A = \{2, 3, 5, 7\}$ — первые четыре простых числа. $\{2, 3\} = \{3, 2\}$ и $\{2, 2, 3\} = \{2, 3\}$.

Принадлежность

Множество хранит об объекте ровно один бит: внутри он или нет.

Определение 3

- $a \in A$ — « a принадлежит множеству A ».
- $a \notin A$ — « a не принадлежит A ».

Пример (Вложенные множества)

$B = \{a, \{b\}\}$: $a \in B$ и $\{b\} \in B$, но $b \notin B$ — b лежит внутри вложенного множества.

Принадлежность проверяет только *прямых* элементов.

Внутри вложенных множеств она не заглядывает.

Способы задания

Пример (Перечисление)

- $\{1, 2, 3\}$.
- $\{\alpha, \beta, \gamma\}$.

Пример (Свойством)

- $\{x \in \mathbb{N} \mid x \text{ чётно}\}$ — множество чётных натуральных чисел.
- $\{x \in \mathbb{R} \mid x^2 = 2\}$ — множество корней уравнения $x^2 = 2$.

Третий способ — рекурсивный: базовые элементы плюс правила порождения.

Чётные числа:

- База: $0 \in E$.
- Шаг: если $n \in E$, то $n + 2 \in E$.

Так задаются формулы, языки и деревья.

Пустое множество и мощность

Определение 4

Пустое множество $\emptyset$ — множество без элементов: $\emptyset = \{\}$.

Число элементов конечного множества A называется его **мощностью** и обозначается $|A|$.

Пример

- $|\{2, 2, 3\}| = 2$: повторы считаются один раз.
- $|\emptyset| = 0$, а $|\{\emptyset\}| = 1$.
- $\emptyset \in \{\emptyset\}$ и $\emptyset \subseteq \{\emptyset\}$ — истинны оба утверждения.

$\emptyset \neq \{\emptyset\}$: слева нет элементов, справа один элемент — само $\emptyset$.

Пустое множество одно: экстенциональность не оставляет места двум пустотам.

Числа как множества

В чистой теории множеств никаких объектов, кроме множеств, нет — даже чисел.

Натуральные числа строятся из пустого множества:

$$\begin{aligned}0 &= \emptyset, & 1 &= \{\emptyset\}, & 2 &= \{\emptyset, \{\emptyset\}\} \\3 &= \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, & \dots, & & n &= \{0, 1, \dots, n-1\}\end{aligned}$$

Каждое число — множество всех предыдущих: n содержит ровно n элементов.

Следующее число получается добавлением себя как элемента: $n + 1 = n \cup \{n\}$.

Это построение фон Неймана.

В аксиоматической теории множеств на нём стоит вся арифметика: числа, пары и функции сводятся к $\emptyset$ и $\in$.

Равенство множеств

Определение 5

Множества A и B **равны**, если у них одни и те же элементы:

$$A = B \leftrightarrow \forall x. (x \in A) \leftrightarrow (x \in B).$$

Пример

$\{1, 2\} = \{2, 1\} = \{1, 2, 2\}$: порядок и повторы не влияют.

Это **экстенциональность**: состав определяет множество.

В аксиоматической теории множеств она постулируется аксиомой объёмности.

Равенство через два включения

Теорема 1

$A = B$ тогда и только тогда, когда $A \subseteq B$ и $B \subseteq A$.

Доказательство

Прямое направление. Пусть $A = B$. По экстенсionalности $\forall x. (x \in A) \leftrightarrow (x \in B)$, в частности $x \in A \rightarrow x \in B$ и $x \in B \rightarrow x \in A$ — это в точности определения $A \subseteq B$ и $B \subseteq A$.

Обратное. Пусть $A \subseteq B$ и $B \subseteq A$. Для произвольного x из $x \in A$ следует $x \in B$, а из $x \in B$ следует $x \in A$ — вместе $x \in A \leftrightarrow x \in B$, и по экстенсionalности $A = B$.

Стандартный приём доказательства равенства множеств — два включения: эквивалентность из лекции 2, две импликации по отдельности.

Собственные подмножества

Определение 6

A — **собственное** подмножество B (запись $A \subset B$), если $A \subseteq B$ и $A \neq B$.

Пример

- Множество чётных чисел — собственное подмножество $\mathbb{Z}$.
- $\{1, 2\} \subseteq \{1, 2\}$ истинно, а $\{1, 2\} \subset \{1, 2\}$ ложно: множества равны.

$\in$ и $\subseteq$ работают на разных уровнях.

- $1 \in \{1, 2\}$ истинно: 1 — элемент.
- $\{1\} \subseteq \{1, 2\}$ истинно: $\{1\}$ — подмножество.
- $1 \subseteq \{1, 2\}$ не имеет смысла: слева от $\subseteq$ ожидается множество.

Операции над множествами

Все операции — логические связи, применённые к принадлежности.

Дополнение считается относительно зафиксированного универсума U .

Операция	Определение
Объединение	$A \cup B = \{x \mid x \in A \vee x \in B\}$
Пересечение	$A \cap B = \{x \mid x \in A \wedge x \in B\}$
Разность	$A \setminus B = \{x \mid x \in A \wedge x \notin B\}$
Симметрическая разность	$A \Delta B = (A \setminus B) \cup (B \setminus A)$
Дополнение	$\overline{A} = U \setminus A = \{x \mid x \notin A\}$

Операции над множествами [2]

Пример

Пусть $A = \{1, 2, 3\}$, $B = \{2, 3, 4\}$, $U = \{1, 2, 3, 4, 5\}$.

- $A \cup B = \{1, 2, 3, 4\}$
- $A \cap B = \{2, 3\}$
- $A \setminus B = \{1\}$
- $A \Delta B = \{1, 4\}$
- $\overline{A} = \{4, 5\}$

Диаграммы Венна

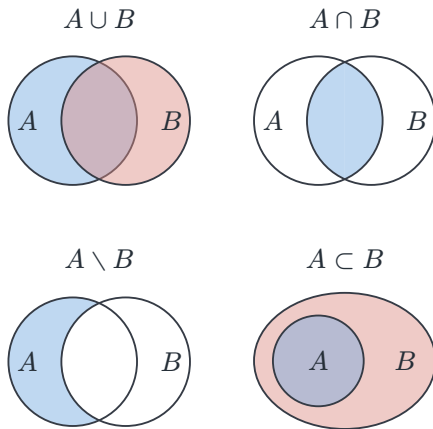


Диаграмма подсказывает тождество и сразу показывает контрпример: несовпадающая область — готовый контрпример.

Законы алгебры множеств

Каждая строка — логический закон в записи множеств.

Закон	Формулы
Идемпотентность	$A \cup A = A, A \cap A = A$
Коммутативность	$A \cup B = B \cup A, A \cap B = B \cap A$
Ассоциативность	$(A \cup B) \cup C = A \cup (B \cup C), (A \cap B) \cap C = A \cap (B \cap C)$
Дистрибутивность	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C), A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Поглощение	$A \cup (A \cap B) = A, A \cap (A \cup B) = A$
Тождество	$A \cup \emptyset = A, A \cap U = A$
Дополнение	$A \cup \bar{A} = U, A \cap \bar{A} = \emptyset$

Доказательства не нужны: это те же законы логики высказываний с переименованными операциями.

Замена $\vee \rightarrow \cup, \wedge \rightarrow \cap, \neg \rightarrow \bar{A}$ переносит каждое тождество.

Симметрическая разность — xor

Элемент попадает в $A\Delta B$, если лежит ровно в одной из двух частей: $x \in A\Delta B \equiv x \in A \oplus x \in B$.

Теорема 2

$$A\Delta B = (A \cup B) \setminus (A \cap B)$$

Доказательство

Цепочка эквивалентностей для произвольного x :

$$\begin{aligned} x \in A\Delta B &\equiv (x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B) \\ &\equiv (x \in A \vee x \in B) \wedge \neg((x \in A) \wedge (x \in B)) \\ &\equiv x \in (A \cup B) \setminus (A \cap B) \end{aligned}$$

Свойства симметрической разности

Второй переход в цепочке — тождество $x \oplus y \equiv (x \vee y) \wedge \neg(x \wedge y)$, знакомое по таблицам истинности.

Из связи с $\oplus$ снимаются свойства:

- $A \Delta A = \emptyset$: элемент не отличается от самого себя.
- $A \Delta (A \Delta B) = B$: двойное переключение возвращает исходное.
- $A \Delta \overline{A} = U$: каждый элемент универсума лежит ровно в одной части.
- Δ коммутативна и ассоциативна — как $\oplus$.

Второй приём: разбор случаев

Теорема 3

$$A \cup (\bar{A} \cap B) = A \cup B$$

Доказательство

Докажем двумя включениями.

Включение $\subseteq$. Пусть $x \in A \cup (\bar{A} \cap B)$. При $x \in A$ элемент уже лежит в $A \cup B$. При $x \notin A$ от $x \in \bar{A} \cap B$ остаётся $x \in B$.

Включение $\supseteq$. Пусть $x \in A \cup B$. При $x \in A$ элемент лежит и слева. При $x \notin A$ из $x \in B$ следует $x \in \bar{A} \cap B$.

Это упрощение $a \vee (\neg a \wedge b) \equiv a \vee b$: так сокращают булевы условия компиляторы и оптимизаторы SQL-запросов.

Доказательство де Моргана

Теорема 4 (Законы де Моргана для множеств)

$$\overline{A \cap B} = \overline{A} \cup \overline{B} \quad \text{и} \quad \overline{A \cup B} = \overline{A} \cap \overline{B}$$

Доказательство

Докажем первый закон цепочкой эквивалентностей для произвольного x :

$$\begin{aligned} x \in \overline{A \cap B} &\equiv x \notin (A \cap B) \equiv \neg(x \in A \wedge x \in B) \\ &\equiv (x \notin A) \vee (x \notin B) \equiv x \in \overline{A} \cup \overline{B} \end{aligned}$$

Третий переход — де Морган из логики, остальные — по определению. Эквивалентность верна для каждого x , значит, множества совпадают.

Второй закон доказывается аналогично.

Тождество с разностью

Теорема 5

$$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$$

Доказательство

Цепочка эквивалентностей для произвольного x :

$$\begin{aligned} x \in A \setminus (B \cup C) &\equiv x \in A \wedge x \notin (B \cup C) \\ &\equiv x \in A \wedge (x \notin B \wedge x \notin C) \\ &\equiv (x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C) \\ &\equiv x \in (A \setminus B) \cap (A \setminus C) \end{aligned}$$

Арифметическая аналогия здесь ошибается: $A \setminus (B \cup C) \neq (A \setminus B) \cup (A \setminus C)$.

Контрпример: $A = \{1, 2, 3\}$, $B = \{2\}$, $C = \{3\}$ — слева $\{1\}$, справа $\{1, 2, 3\}$.

Булеан

Определение 7

Булеан (*power set*) множества A — множество всех его подмножеств:

$$\mathcal{P}(A) = \{S \mid S \subseteq A\}.$$

Пример

$$\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}.$$

Крайние случаи: $\mathcal{P}(\emptyset) = \{\emptyset\}$, $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$.

Теорема 6

Для конечного множества из n элементов $|\mathcal{P}(A)| = 2^n$.

Мощность булеана

Доказательство

Для каждого из n элементов есть два независимых выбора: включить его в подмножество или нет.

Всего подмножеств 2^n .

Та же арифметика, что у таблиц истинности:

n атомов — 2^n строк, n элементов — 2^n подмножеств.

Подмножество отвечает на n вопросов «включать ли элемент» — как интерпретация на n атомах.

Рост экспоненциальный: при $n = 20$ подмножеств больше миллиона.

Декартово произведение

Определение 8

Декартово произведение множеств A и B :

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

Пример

Пусть $A = \{1, 2\}$, $B = \{x, y\}$, тогда их декартово произведение:

$$A \times B = \{(1, x), (1, y), (2, x), (2, y)\}.$$

Декартово произведение [2]

Теорема 7

Для конечных A и B выполнено $|A \times B| = |A| \cdot |B|$.

Доказательство

Первая компонента пары выбирается $|A|$ способами, вторая — $|B|$.

Выборы независимы, поэтому перемножаются.

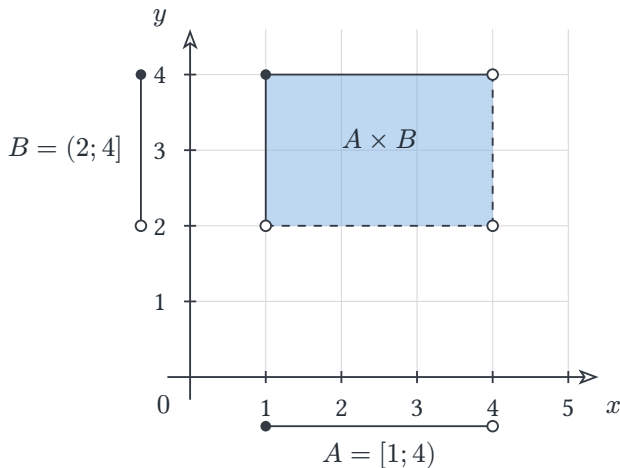
Декартово произведение на плоскости

Пара (a, b) — точка плоскости.

Декартово произведение $\mathbb{R} \times \mathbb{R}$ — вся координатная плоскость.

Произведение интервалов — прямоугольник:
 $[1, 4) \times (2, 4]$.

Заполненная точка — конец включён,
пустая — исключён.



Пары и кортежи

Пары упорядочены: $(1, x) \neq (x, 1)$.

Строго говоря, $(A \times B) \times C \neq A \times (B \times C)$: слева пары пар, справа пары с парой на втором месте.

Между ними есть естественное отождествление, поэтому скобки опускают: $A \times B \times C$ — множество троек.

Элементы декартова произведения $A_1 \times A_2 \times \dots \times A_n$ — *кортежи* длины n .

В аксиоматической теории пара — тоже множество: $(a, b) = \{\{a\}, \{a, b\}\}$ (определение Куратовского).

Из него выходит $(a, b) = (c, d)$ только при $a = c$ и $b = d$: порядок и различие компонентов держатся одними множествами.

Поэтому $A \times B$ — законное множество: пары лежат внутри $\mathcal{P}(\mathcal{P}(A \cup B))$.

Разбиения

Определение 9

Разбиение (*partition*) множества X — набор непустых попарно непересекающихся подмножеств, покрывающих X .

Пример

$\{\{0, 2, 4, \dots\}, \{1, 3, 5, \dots\}\}$ — разбиение $\mathbb{N}$ на чётные и нечётные числа.

У $\{1, 2, 3\}$ ровно пять разбиений:

- $\{\{1, 2, 3\}\}$
- $\{\{1, 2\}, \{3\}\}$
- $\{\{1, 3\}, \{2\}\}$
- $\{\{2, 3\}, \{1\}\}$
- $\{\{1\}, \{2\}, \{3\}\}$

Парадокс Расселла

Кантор предполагал: любое свойство $P(x)$ собирает множество $\{x \mid P(x)\}$ — это называют **принципом свёртки**.

Рассел в 1901 году показал, что принцип противоречив.

Свойство « A не содержит себя» порождает:

$$R = \{A \mid A \notin A\}$$

Подставим R в его собственное свойство.

- $R \in R$ — тогда по определению R должно быть $R \notin R$.
- $R \notin R$ — тогда R удовлетворяет свойству, и должно быть $R \in R$.

Обе ветви дают противоречие: множества R не существует.

Свободное порождение множеств любым свойством — некорректная операция.

Выход из парадокса

Бытовой вариант — браздобрей, который брей всех и только тех, кто не бреется сам: бреет ли он себя?

Рассел сообщил о противоречии Фреге, чья арифметика строилась на теории множеств.

Выход предложил Цермело в 1908 году: аксиоматика, где множества строятся поэтапно.

Определение 10

Аксиома выделения (Цермело): для множества A и свойства P существует множество $\{x \in A \mid P(x)\}$.

Универсум и типы

Нотация порождающего свойства в этой лекции всегда ограничена: $\{x \in U \mid P(x)\}$.

Выделение из готового множества противоречий не создаёт: чтобы получить R по свойству « $A \notin A$ », нужно назвать множество, из которого оно выделяется, — а такого множества нет.

Универсум U из начала лекции — условие существования каждого множества.

Множество строится в два шага: сначала универсум, потом выделение по свойству.

В программировании то же правило: `Set<int>` выделяет элементы только из `int`.



Множества в программировании

Абстракция нужна не для тумана, а для нового семантического уровня, на котором можно быть абсолютно точным.

— Эдсгер Дейкстра

SQL: таблица — множество кортежей

Таблица в базе данных — подмножество декартова произведения: строка — кортеж, колонка — компонент кортежа.

student	
id	name

1	Аня
2	Борис
3	Вера

knows	
student	lang

1	python
1	rust
2	python
3	haskell

результат JOIN	
name	lang

Аня	python
Аня	rust
Борис	python
Вера	haskell

```
SELECT student.name, knows.lang  
FROM student JOIN knows ON student.id = knows.student;
```

JOIN — декартово произведение с условием: пар было $3 \cdot 4 = 12$, предикат оставил 4.

Операции над множествами в SQL

Два подмножества одной таблицы, вырезанные предикатом WHERE:

```
SELECT lang FROM knows WHERE student = 1  
INTERSECT SELECT lang FROM knows WHERE student = 2;
```

Пример

- INTERSECT -> python — общий язык.
- EXCEPT -> rust — только у Ани.
- UNION -> python, rust — повторы убраны.
- UNION ALL -> python, rust, python — повторы на месте.

UNION убирает повторы, UNION ALL оставляет: таблицы SQL — мультимножества.

Типы как множества

Тип — множество допустимых значений.

Типизация — прикладная форма универсума: значения выделяются всегда внутри готового типа.

- `bool = {false, true}`.
- `uint8 = {0, 1, ..., 255}`.
- **Тип-произведение** (`struct`) — декартово произведение.
- **Тип-сумма** (`enum`) — дизъюнктивное объединение.
- `Option <T>` — тип-сумма: значение «None» или «Some»(`T`).

Битовые маски

Множество $S \subseteq \{1, \dots, n\}$ кодируется битовой строкой длины n : i -й бит равен 1, если $i \in S$.

- $\cup$ — побитовое OR, $\cap$ — AND, $\bar{S}$ — NOT.
- Δ — XOR: маска переключает присутствие элементов.
- Включение $X \subseteq Y$ проверяется как $x \& y == x$.

Пример

Права доступа (rwx) — три бита: read, write, execute.

Маска 110_2 означает чтение и запись без исполнения.

Маска — элемент булеана: множество кодируется числом от 0 до $2^n - 1$.

Хеширование и принцип Дирихле

Хеш-функция $h : K \rightarrow \{0, \dots, m - 1\}$ отображает ключи в конечное множество корзин.

Коллизия — два разных ключа в одной корзине: $h(k_1) = h(k_2)$ при $k_1 \neq k_2$.

Принцип Дирихле: $n + 1$ объект в n ящиках — найдётся ящик с двумя.

Ключей больше, чем корзин, — коллизия неизбежна при любой хеш-функции.

Пример

- 13 человек и 12 месяцев — двое родились в одном месяце.
- Неудачная функция устраивает коллизии и без принципа: $h(k) = k \bmod 5$ на ключах $\{2, 7, 12, 17\}$ сваливает все четыре в ячейку 2.

Лекция 3: что мы поняли?

- Множество задаётся предикатом принадлежности. Состав важнее описания — экстенциональность.
- Включение — импликация, операции — связки. $\emptyset \subseteq A$ — вакуумная истинность.
- Тожества доказываются цепочками эквивалентностей или двумя включениями с разбором случаев.
- Симметрическая разность — $\oplus$: $A \Delta (A \Delta B) = B$.
- Свойство строит множество только внутри готового универсума: без него — парадокс Расселла.
- Булеан растёт как 2^n — та же арифметика, что у таблиц истинности. Маска кодирует подмножество числом от 0 до $2^n - 1$.
- $|A \times B| = |A| \cdot |B|$ — пары, на которых будут стоять отношения и функции.

Вопросы для самопроверки

1. Почему $\{2, 2, 3\} = \{2, 3\}$?
2. Верно ли, что $\emptyset \in \emptyset$? А что насчёт $\emptyset \subseteq \emptyset$? Чему равен булеан $\{\emptyset\}$?
3. Почему $R = \{A \mid A \notin A\}$ не является множеством?
4. Чему равно $A \Delta (A \Delta B)$? Какая побитовая операция соответствует Δ ?
5. Сколько разбиений у множества $\{1, 2, 3\}$? Придумайте разбиение $\mathbb{Z}$ на три класса.
6. Докажите закон де Моргана $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Чтение к следующей паре

- m04 — «Множество и его элементы», «Операции над множествами», «Булеан», «Декартово произведение», «Парадокс Расселла и аксиоматическая теория множеств».
- Флеш-опросник — в начале лекции 4.