Ефремов Евгений Леонидович

МАТЕМАТИЧЕСКАЯ ЛОГИКА

Конспект лекций

Владивосток

2021 г.

ОГЛАВЛЕНИЕ

ГЛАВА I

ТЕОРИЯ МНОЖЕСТВ

Прежде, чем познакомиться с основными разделами математической логики, сформулируем интуитивную (наивную) теорию множеств. Наша цель в этой главе — зафиксировать основные понятия теории множеств и изложить несколько основных результатов. Многие сведения этой главы наверняка Вам уже известны из курса алгебры, математического анализа и дискретной математики. Тем не менее, рекомендуется прочитать их для того, чтобы вспомнить определения и свойства, привыкнуть к обозначениям нашего курса, посмотреть, возможно, другие доказательства известных утверждений.

При попытке систематического изложения математики (впрочем, как и любой другой науки) возникает проблема выбора *начальных понятий*, которые будут положены в основу всего изложения. Таковыми, например, в геометрии являются *точка*, *прямая*, *плоскость*. Мы привыкли под точкой понимать мелкое пятно, оставляемое ручкой на листе бумаги лёгким касанием. Но ведь это пятно по сути является фигурой — геометрическим местом точек. Определить понятие через него само мы не можем. Аналогичная проблема с определением прямой и плоскости.

Как правило, выбор начальных понятий и обоснование этого выбора лежит вне области самой науки. Здесь задействованы философские принципы и методы научного познания. Систематизация математики в конце XIX века выявила, что вполне универсальным является использование понятия *множества* в качестве единственного начального понятия для всей математики. Это породило новую математическую дисциплину — теорию множеств. Была проделана большая работа по теоретико-множественному осмыслению математических и, как следствие, логических понятий такими математиками, как Б. Больцано, Р. Дедекинд, Г. Кантор, Г. Фреге, Б. Рассел. Однако высокая степень абстрактности и универсальности понятия множества привели к трудностям, которые

чаще всего называют теоретико-множественными *парадоксами*.

Дальнейшие работы в области теории множеств привели к устранению подобных проблем. Так, например, Д. Гильберт предложил построить формализацию математики таким образом, что средствами этой системы можно доказать свою собственную непротиворечивость.

§1. Основные понятия и обозначения

Совокупность некоторых объектов будем называть *множеством*, сами объекты при этом будем называть *элементами* этого множества.

Договоримся множества обозначать заглавными буквами латинского алфавита (возможно с индексами), а их элементы — строчными (возможно с индексами). Тот факт, что объект a является элементом множества B, записывается как $a \in B$.

Определение. Среди всех множеств выделим множество, которое не содержит ни одного элемента. Такое множество называется *пустым* и обозначается символом $\varnothing$.

Например, множество всех летающих крокодилов Антарктиды пусто, а множество всех натуральных простых чётных чисел — нет, оно состоит из единственного элемента 2.

В приведённых примерах мы использовали один из способов определения множества — *описательный*. В большинстве случаев мы будем использовать именно этот способ. Если объект x обладает свойством P, то кратко этот факт будем записывать как $P(x)$. Множество всех объектов x, обладающих свойством P, будем обозначать как $\{x \mid P(x)\}$. Например,

$$\{x \mid x \text{ — летающий крокодил Антарктиды}\},$$

$$\{x \mid x \in \mathbb{N},\ x \text{ — простое},\ x \vdots 2\}.$$

В случае, когда количество элементов множества невелико или нам важно наглядно отобразить, какие элементы в нём содержатся, будем также писать {элементы}. Такой способ определения множества называется *перечислением*. Например,

$$\{\text{Саша, Маша, Вова}\},$$

$$\{2, 4, 6, 8, \ldots, 100\}.$$

Определение. Если любой элемент множества A является элементом множества B, то множество A называется *подмножеством* множества B (обозначение: $A \subseteq B$).

Например, множество всех чётных натуральных чисел является подмножеством множества всех натуральных чисел; множество всех студентов Программной инженерии является подмножеством множества всех студентов Института математики и компьютерных технологий ДВФУ; множество всех летающих крокодилов Антарктиды (как бы глобально это ни звучало) является подмножеством множества всех студентов направления Программная инженерия (летающим крокодилам тоже хочется изучать математическую логику).

Посмотрите внимательно на последнее определение. Оно содержит много математических терминов, причём некоторые из них имеют собственные обозначения: мы уже можем с помощью символов записать фразы «элемент множества A», «элемент множества B», «множество A является подмножеством множества B». Было бы удобно, если бы мы и другие слова в этом определении смогли записать символами, что значительно сократило бы его запись. Как известно, математики — люди ленивые, поэтому уже давно придумали специальные обозначения. Например, утверждение «если $\mathcal{A}$, то $\mathcal{B}$» можно кратко записать как $\mathcal{A} \Rightarrow \mathcal{B}$, а слово «любой» обозначают символом $\forall$. Дадим определение подмножества в введённых нами обозначениях:

$$A \subseteq B \overset{df}{\Longleftrightarrow} \forall x\,(x \in A \Rightarrow x \in B).$$

Как Вы уже наверняка догадались, символ $\Longleftrightarrow$ можно прочитать как «тогда и только тогда, когда». Запись df над стрелкой подразумевает, что мы *определяем* отношение «быть подмножеством» (от английского definition — определение). Всюду дальше будем использовать аналогичные обозначения, чтобы отделять термин от его определения.

Но и приведённая формулировка ещё не окончательный вариант! Можно сократить эту запись до

$$A \subseteq B \overset{df}{\Longleftrightarrow} \forall x \in A\,(x \in B).$$

Упражнение 1. Прочитайте следующее определение *равенства* множеств.

Определение. $A = B \overset{df}{\Longleftrightarrow} \forall x\,(x \in A \Leftrightarrow x \in B)$.

Равенство множеств можно определить и по-другому:

$$A = B \overset{df}{\Longleftrightarrow} A \subseteq B \text{ и } B \subseteq A.$$

Очевидно, что если A — множество, то $\varnothing$ и A являются подмножествами A. Эти множества называют *тривиальными*.

Определение. Множество A называется *собственным* подмножеством множества B, если $A \subseteq B$ и $A \neq B$ (обозначение: $A \subset B$).

Дадим немного другое определение:

$$A \subset B \overset{df}{\Longleftrightarrow} A \subseteq B \text{ и } \exists x \in B\,(x \notin A).$$

Новый символ $\exists$ читается как «существует». Символы $\forall$ и $\exists$ называются *кванторами всеобщности* и *существования* соответственно, они играют важную роль в логике предикатов, с которой мы познакомимся с Вами позднее. А пока мы будем использовать их для сокращения формулировок определений и теорем.

Наряду с $\subseteq$ и $\subset$ будем также использовать символы $\supseteq$ и $\supset$.

Упражнение 2. Запишите определения отношений $\supseteq$ и $\supset$, используя только математические обозначения.

Определение. Множество всех подмножеств множества A называется *булеаном* A (обозначение: $\mathcal{P}(A)$).

Например, булеан множества $A = \{a, b, c\}$ состоит из 8 элементов:

$$\mathcal{P}(A) = \big\{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, A\big\}.$$

Нетрудно понять, что имеет место следующая

Теорема 1. *Если множество A состоит из n элементов, то $\mathcal{P}(A)$ содержит ровно 2^n множеств.*

Доказательство.

Пусть $A = \{a_1, a_2, \ldots, a_n\}$, $B \subseteq A$. Про любой элемент $a_i \in A$, где $i \leqslant n$, мы можем однозначно сказать, какое из утверждений $a_i \in B$ и $a_i \notin B$ верно. Запишем последовательность из 0 и 1 длины n следующим образом: для $i \leqslant n$

— если элемент a_i принадлежит множеству B, то на i-ом месте последовательности запишем 1;

— если элемент a_i не принадлежит множеству B, то на i-ом месте последовательности запишем 0.

Таким образом, множеству B поставлена в соответствие последовательность из 0 и 1 длины n, причём единственным образом. Более того, если мы возьмём какую-нибудь последовательность из 0 и 1, состоящую из n элементов, то она по введённым нами правилам будет соответствовать некоторому подмножеству множества A. Следовательно, подмножеств у множества A ровно столько, сколько n-элементных последовательностей из 0 и 1. Читатель, знакомый с комбинаторным правилом произведения, с лёгкостью подсчитает количество таких последовательностей: так как каждый элемент последовательности может быть одним из двух чисел, а всего элементов в ней n, то число таких последовательностей равно 2^n. $\square$

§2. Операции над множествами

Определение. Пусть даны два произвольных множества A и B. Определим следующие операции:

1. *Пересечение* (обозначение: $A \cap B$)

$$A \cap B \stackrel{df}{=} \{x \mid x \in A \text{ и } x \in B\}.$$

Иными словами, под пересечением двух множеств понимают множество, состоящее из их общих элементов. Графически множества удобно изображать в виде так называемых *кругов Эйлера*. На рисунке 1 закрашено пересечение множеств A и B.

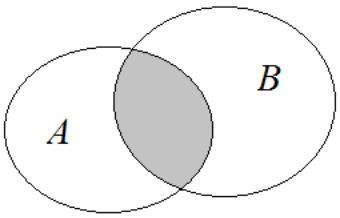

Рисунок 1

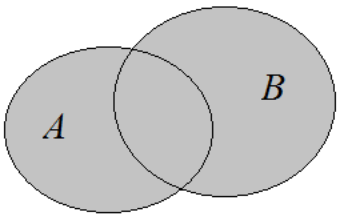

Рисунок 2

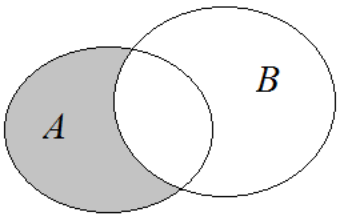

Рисунок 3

2. *Объединение* (обозначение: $A \cup B$)

$$A \cup B \stackrel{df}{=} \{x \mid x \in A \text{ или } x \in B\}.$$

Т.е. объединение — это множество всех элементов, входящих хотя бы в одно из множеств A и B (рисунок 2).

3. *Разность* (обозначение: $A \setminus B$)

$$A \setminus B \stackrel{df}{=} \{x \mid x \in A \text{ и } x \notin B\}.$$

Т.е. разность — это множество всех элементов, входящих во множество A и не входящих во множество B (рисунок 3). Эта операция отличается от пересечения и объединения тем, что в разности важен порядок множеств: при пересечении и объединении множеств порядок самих множеств, очевидно, не имеет значения (такие операции называют коммутативными).

4. Если $A \subseteq B$, то множество $B \setminus A$ (рисунок 4) называют *дополнением множества A до множества B* (обозначение: $\overline{A}_B$).

Если известно, что все рассматриваемые в рамках одной проблемы множества являются подмножествами какого-либо одного множества U, то вместо $\overline{A}_U$ пишут просто $\overline{A}$, а вместо «дополнение множества A до множества U» говорят просто «дополнение множества A». Множество U при этом называют *универсальным множеством*. На рисунке 5 изображено дополнение множества A.

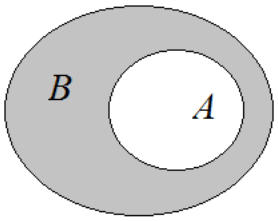

Рисунок 4

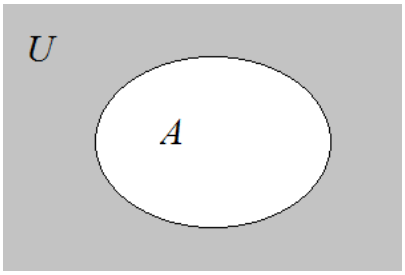

Рисунок 5

Теорема 2. *Для любых множеств A, B, C выполняются следующие свойства:*

1. Идемпотентность
a) $A \cap A = A$,
b) $A \cup A = A$.
2. Коммутативность
a) $A \cap B = B \cap A$,
b) $A \cup B = B \cup A$.
3. Ассоциативность
a) $A \cap (B \cap C) = (A \cap B) \cap C$,
b) $A \cup (B \cup C) = (A \cup B) \cup C$.
4. Дистрибутивность
a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
5. $\overline{\overline{A}} = A$.
6. Законы де Моргана
a) $\overline{A \cap B} = \overline{A} \cup \overline{B}$,
b) $\overline{A \cup B} = \overline{A} \cap \overline{B}$.
7. Законы поглощения
a) $A \cap (A \cup B) = A$,
b) $A \cup (A \cap B) = A$.
8. $A \cup \varnothing = A$.
9. $A \cap \varnothing = \varnothing$.

Доказательство.

Докажем, например, равенство 5. Так как ничего, кроме определения равенства двух множеств и определения дополнения множества, у нас нет, то и доказывать нужно, опираясь на эти определения. Пусть $a \in \overline{\overline{A}}$. Тогда $a \notin \overline{A}$. Следовательно, $a \in A$. Очевидно, рассуждения в обратную сторону приведут к тому, что если $a \in A$, то $a \in \overline{\overline{A}}$. Свойство 5 доказано. Запишем наше доказа-

тельство в более простой форме:

$$a \in \overline{\overline{A}} \overset{\text{по опр}}{\iff} a \notin \overline{A} \overset{\text{по опр}}{\iff} a \in A.$$

Докажем закон де Моргана (6b):

$$c \in \overline{A \cup B} \overset{\text{по опр}}{\iff} c \notin A \cup B \iff c \notin A \text{ и } c \notin B \overset{\text{по опр}}{\iff}$$

$$\overset{\text{по опр}}{\iff} c \in \overline{A} \text{ и } c \in \overline{B} \overset{\text{по опр}}{\iff} c \in \overline{A} \cap \overline{B}.$$

Домашнее задание. Докажите остальные пункты теоремы 2.

§3. Декартово произведение множеств

Интуитивно понятно, что под *упорядоченным набором* (или последовательностью) из n элементов понимается n-элементное множество, в котором важно, в каком порядке записаны его элементы. Но такое определение с математической точки зрения неверно — во множестве нет никакого порядка. К тому же любое множество определяется своими элементами, а значит, не может содержать двух одинаковых элементов, в то время как упорядоченный набор может состоять из сотни копий одного и того же элемента. Дадим более строгое определение упорядоченного набора индукцией по n — числу элементов в этом наборе. Упорядоченный набор элементов $a_1, \ldots, a_n$ будем обозначать через $\langle a_1, \ldots, a_n \rangle$ и иногда называть *кортежем*, а число n — *длиной* кортежа $\langle a_1, \ldots, a_n \rangle$.

Определение. Если $n = 0$, то под упорядоченным набором $\langle\ \rangle$ будем понимать множество $\varnothing$.

Если $n = 1$, то упорядоченный набор $\langle a_1 \rangle$ равен $\{a_1\}$.

Если $n = 2$, то упорядоченный набор $\langle a_1, a_2 \rangle$ равен $\{\{a_1\}, \{a_1, a_2\}\}$. Такой набор чаще будем называть *упорядоченной парой* или просто *парой*.

Если $n > 2$, то упорядоченный набор $\langle a_1, \ldots, a_{n-1}, a_n \rangle$ равен упорядоченной паре $\langle \langle a_1, \ldots, a_{n-1} \rangle, a_n \rangle$.

Упражнение 3. Проверьте, что данное определение корректно. То есть покажите, что

$$\langle a_1, a_2 \rangle = \langle b_1, b_2 \rangle \iff a_1 = b_1 \text{ и } a_2 = b_2.$$

Определение. *Декартовым произведением* множеств $A_1, \ldots, A_n$ (обозначение: $A_1 \times \ldots \times A_n$) называется множество

$$\{\langle x_1, \ldots, x_n \rangle \mid x_1 \in A_1, \ldots, x_n \in A_n\}.$$

Например, если $A = \{1, 2\}$, $B = \{a, b, c\}$, то

$$A \times B = \{\langle 1, a\rangle, \langle 1, b\rangle, \langle 1, c\rangle, \langle 2, a\rangle, \langle 2, b\rangle, \langle 2, c\rangle\},$$

$$B \times A = \{\langle a, 1\rangle, \langle a, 2\rangle, \langle b, 1\rangle, \langle b, 2\rangle, \langle c, 1\rangle, \langle c, 2\rangle\},$$

$$A \times A = \{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 2, 1\rangle, \langle 2, 2\rangle\}.$$

Определение. Если $A_1 = \ldots = A_n = A$, то $A_1 \times \ldots \times A_n$ называется *n-ой декартовой степенью* множества A и обозначается через A^n.

Упражнение 4. Верно ли, что $A \times (B \times C) = (A \times B) \times C$?

§4. Бинарные отношения

Определение. Множество $\rho \subseteq A_1 \times \ldots \times A_n$ называется *n-местным отношением* на наборе множеств $A_1, \ldots, A_n$. Если $A_1 = \ldots = A_n = A$, то $\rho \subseteq A^n$ называется *n-местным отношением* на множестве A. Если $n = 2$, то соответствующее двухместное отношение будем называть *бинарным*.

Например, множество

$$\rho = \{\langle 1, a\rangle, \langle 1, c\rangle, \langle 2, c\rangle\}$$

является бинарным отношением на паре множеств $A = \{1, 2\}$, $B = \{a, b, c\}$.

Определение. Пусть $\rho \subseteq A \times B$. Множество

$$\mathrm{D}(\rho) \stackrel{df}{=} \{x \in A \mid \exists y \in B\,(\langle x, y\rangle \in \rho)\}$$

называется *областью определения* бинарного отношения ρ, а множество

$$\mathrm{Im}(\rho) \stackrel{df}{=} \{y \in B \mid \exists x \in A\,(\langle x, y\rangle \in \rho)\}$$

называется *множеством значений* бинарного отношения ρ.

Всюду дальше, если не оговорено противное, под отношением будем подразумевать бинарное отношение. Иногда вместо $\langle x, y\rangle \in \rho$ будем писать $\rho(x, y)$ или $x \rho\, y$.

Определение. Пусть ρ — бинарное отношение. Отношение

$$\rho^{-1} \stackrel{df}{=} \{\langle y, x\rangle \mid \langle x, y\rangle \in \rho\}$$

называется *обратным к* ρ.

Упражнение 5. Для $\rho = \{\langle x, y\rangle \mid y = x^2\} \subseteq \mathbb{Z}^2$ найдите $\mathrm{D}(\rho)$, $\mathrm{Im}(\rho)$, ρ^{-1}.

Определение. Определим свойства бинарного отношения $\rho \subseteq A^2$:

ρ *рефлексивно* $\overset{df}{\iff} \forall\, x \in A\, (\langle x, x\rangle \in \rho)$,

ρ *симметрично* $\overset{df}{\iff} \forall\, x, y \in A\, (\langle x, y\rangle \in \rho \Rightarrow \langle y, x\rangle \in \rho)$,

ρ *транзитивно* $\overset{df}{\iff} \forall\, x, y, z \in A\, (\langle x, y\rangle \in \rho$ и $\langle y, z\rangle \in \rho \Rightarrow \langle x, z\rangle \in \rho)$,

ρ *антирефлексивно* $\overset{df}{\iff} \forall\, x \in A\, (\langle x, x\rangle \notin \rho)$,

ρ *антисимметрично* $\overset{df}{\iff} \forall\, x, y \in A\, (\langle x, y\rangle \in \rho$ и $\langle y, x\rangle \in \rho \Rightarrow x = y)$,

ρ *связно* $\overset{df}{\iff} \forall\, x, y \in A\, (\langle x, y\rangle \in \rho$ или $\langle y, x\rangle \in \rho$ или $x = y)$.

Упражнение 6. Какими свойствами обладает отношение параллельности двух прямых на плоскости? отношение перпендикулярности двух прямых на плоскости? отношение скрещиваемости двух прямых в пространстве?

§5. Отношение эквивалентности

Определение. Бинарное отношение ρ на множестве A называется *отношением эквивалентности*, если оно рефлексивно, симметрично и транзитивно.

Упражнение 7. Являются ли отношения из упражнений 5 и 6 отношениями эквивалентности? Почему?

С каждым отношением эквивалентности на множестве A можно связать разбиение A на непересекающиеся подмножества.

Определение. *Классом эквивалентности* элемента $a \in A$ по отношению эквивалентности ρ называется множество

$$\bar{a} \overset{df}{=} \{x \in A \mid \langle a, x\rangle \in \rho\}.$$

Теорема 3. *Пусть ρ — отношение эквивалентности на A, $a, b \in A$. Тогда либо $\bar{a} \cap \bar{b} = \varnothing$, либо $\bar{a} = \bar{b}$.*

Доказательство.

Предположим, что $\bar{a} \cap \bar{b} \neq \varnothing$, т.е. существует элемент $c \in \bar{a} \cap \bar{b}$. Тогда по определению $\langle a, c\rangle \in \rho$ и $\langle b, c\rangle \in \rho$. Следовательно, $\langle c, a\rangle \in \rho$ и $\langle b, c\rangle \in \rho$. По свойству транзитивности $\langle b, a\rangle \in \rho$. Пусть $d \in \bar{a}$, т.е. $\langle a, d\rangle \in \rho$. Тогда по свойству транзитивности $\langle b, d\rangle \in \rho$, что означает, что $d \in \bar{b}$. Аналогично доказывается, что если $d \in \bar{b}$, то $d \in \bar{a}$. Таким образом, $\bar{a} = \bar{b}$. □

Следствие. $\bar{a} = \bar{b} \iff a \rho\, b$.

Теорема 4. *Пусть I — некоторое множество индексов, $\{A_i \mid i \in I\}$ — разбиение множества A, т.е. $\bigcup\limits_{i\in I} A_i = A$ и $A_i \cap A_j = \varnothing$ для любых различных $i, j \in I$. Тогда отношение $\rho = \{\langle x, y\rangle \mid \exists\, i \in I\,(x, y \in A_i)\}$ является отношением эквивалентности на A.*

Домашнее задание. Докажите следствие и теорему 4.

В теореме 4 мы представили множество A в виде объединения непересекающихся подмножеств. В случае, если $A = A_1 \cup A_2$ и $A_1 \cap A_2 = \varnothing$, вместо $A = A_1 \cup A_2$ будем писать $A = A_1 \sqcup A_2$.

Определение. Множество всех классов эквивалентности по отношению эквивалентности ρ на множестве A называется *фактор-множеством* множества A по отношению ρ (обозначение: A/ρ).

Рассмотрим пример. Пусть ρ — отношение сравнимости по модулю 5 на множестве $\mathbb{Z}$, т.е.

$$a \rho\, b \iff a \text{ и } b \text{ имеют одинаковый остаток при делении на } 5.$$

Тогда, например,

$$\bar{3} = \{x \in \mathbb{Z} \mid 3 \text{ и } x \text{ имеют одинаковый остаток при делении на } 5\} =$$

$$= \{x \in \mathbb{Z} \mid x \text{ даёт остаток } 3 \text{ при делении на } 5\} = \{\ldots, -7, -2, 3, 8, \ldots\}.$$

Очевидно, всего существует пять классов эквивалентности по ρ:

$$\mathbb{Z}/\rho = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}.$$

Упражнение 8. Придумайте отношение эквивалентности на множестве студентов Вашей группы. Чему равно фактор-множество по этому отношению?

§6. Отношение порядка

Определение. Антисимметричное транзитивное бинарное отношение на множестве A называется *отношением частичного порядка*, или просто *порядком*, на A. Множество A при этом называется *частично упорядоченным*. Порядок ρ на множестве A называется *строгим*, если ρ — антирефлексивное отношение, и *нестрогим*, если ρ — рефлексивное отношение.

Определение. Связное отношение частичного порядка на множестве A называется *отношением линейного порядка* на A. Множество A при этом называется *линейно упорядоченным*, или *цепью*.

Например, обычные отношения порядка (как строгие, так и нестрогие) на числовых множествах $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ — линейные порядки, а отношение включения на $\mathcal{P}(A)$, где A содержит более одного элемента, — частичный нелинейный порядок (почему?).

В случае с указанными примерами отношения порядка становится понятным сокращение записи $\langle x, y\rangle \in \rho$ до $x \rho\, y$. Согласитесь, куда удобнее использовать привычную ещё со школы запись $2 \leqslant 5$ вместо $\langle 2, 5\rangle \in \leqslant$, хотя обе записи верны.

Определение. Пусть ρ — отношение порядка на A, $B \subseteq A$, $e \in A$.

e — *минимальный* $\overset{df}{\iff} \forall\, x \in A\,(x \rho\, e \Rightarrow x = e)$.

e — *максимальный* $\overset{df}{\iff} \forall\, x \in A\,(e \rho\, x \Rightarrow e = x)$.

e — *наименьший* $\overset{df}{\iff} \forall\, x \in A\,(e \rho\, x$ или $e = x)$.

e — *наибольший* $\overset{df}{\iff} \forall\, x \in A\,(x \rho\, e$ или $x = e)$.

e — *нижняя грань* $B \overset{df}{\iff} \forall\, x \in B\,(e \rho\, x$ или $e = x)$.

e — *верхняя грань* $B \overset{df}{\iff} \forall\, x \in B\,(x \rho\, e$ или $x = e)$.

Наименьший элемент из множества всех верхних граней B, если он существует, называется *точной верхней гранью* B (обозначение: $\sup B$).

Наибольший элемент из множества всех нижних граней B, если он существует, называется *точной нижней гранью* B (обозначение: $\inf B$).

Рассмотрим пример. Пусть $\rho = \left\{\langle x, y\rangle \;\middle|\; y \vdots x\right\}$ — отношение делимости на множестве $A = \mathbb{N}$, $B = \{2, 3, 8\}$. Легко проверить, что ρ — отношение нестрогого нелинейного порядка. Единственным минимальным и наименьшим элементом в A будет 1, максимальных и наибольшего элементов нет, $\sup B = 24$, $\inf B = 1$. Пусть теперь $A = \mathbb{N} \setminus \{1\}$. Тогда наименьший элемент отсутствует — в A не существует числа, на которое бы поделилось любое натуральное число, отличное от 1. Минимальными элементами теперь являются все простые числа. Наибольшего и максимальных по-прежнему нет. $\sup B = 24$, а вот $\inf B$ не существует.

Определение. Порядок ρ на множестве A называется *плотным*, если

$$\forall\, x, y \in A\,(x \rho\, y \wedge x \neq y \Rightarrow \exists\, z \in A\,(z \neq x \wedge z \neq y \wedge x \rho\, z \wedge z \rho\, y)).$$

Символ $\wedge$ в определении читается как «и» и означает логическую операцию *конъюнкция*, с которой мы познакомимся с Вами в следующей главе. Наряду с символом конъюнкции используют символ *дизъюнкции* $\vee$, который читается как «или». Часто в формулировке определения или утверждения будем использовать эти обозначения.

Определение. Порядок ρ на множестве A называется *полным*, если любое непустое подмножество множества A содержит наименьший элемент.

Упражнение 9. Являются ли плотными и полными следующие отношения порядка:

— $<$ на $\mathbb{N}$,

— $\leqslant$ на $\mathbb{Z}$,

— $<$ на $\mathbb{Q}$,

— $\vdots$ на $\mathbb{N}$?

§7. Отображения

Определение. Бинарное отношение $\varphi \subseteq A \times B$ называется *отображением* из множества A во множество B, если

1) $\forall x \in A\, \exists y \in B\, (\langle x, y\rangle \in \varphi)$,

2) $\forall x \in A,\ y_1, y_2 \in B\, (\langle x, y_1\rangle, \langle x, y_2\rangle \in \varphi \Longrightarrow y_1 = y_2)$.

Обратите внимание на второе условие в этом определении. Оно означает, что в отображении не может существовать двух различных пар с одинаковыми первыми элементами. Сократим запись определения:

$$\varphi \subseteq A \times B \text{ — отображение } \overset{df}{\Longleftrightarrow} \forall\, x \in A\, \exists!\, y \in B\, (\langle x, y\rangle \in \varphi).$$

Символ ! после квантора существования означает, что такой элемент единственен. Отображение $\varphi \subseteq A \times B$ будем обозначать через $\varphi : A \to B$, вместо $\langle a, b\rangle \in \varphi$ будем писать $\varphi(a) = b$.

Например, отношение $\rho_1 = \left\{\langle x, y\rangle \mid x = y^2\right\} \subseteq \mathbb{R}^2$ не является отображением, так как содержит пары $\langle 1, 1\rangle$ и $\langle 1, -1\rangle$, что не соответствует условию 2. Отношение $\rho_2 = \left\{\langle x, y\rangle \mid x = y^2\right\} \subseteq \mathbb{R} \times \mathbb{R}_0^+$ по-прежнему не является отображением — например, не существует такого $y \in \mathbb{R}_0^+$, чтобы $\langle -1, y\rangle \in \rho_2$ (не выполняется условие 1). Наконец, отношение $\rho_3 = \left\{\langle x, y\rangle \mid x = y^2\right\} \subseteq \mathbb{R}_0^+ \times \mathbb{R}_0^+$ является отображением.

Определение. Пусть $\varphi : A \to B$ — отображение, $A' \subseteq A$, $B' \subseteq B$, $a \in A$, $b \in B$, $\varphi(a) = b$.

Элемент b называется *образом* элемента a при отображении φ.

Элемент a называется *прообразом* элемента b при отображении φ.

Множество $\varphi(A') \overset{df}{=} \{\varphi(x) \mid x \in A'\}$ называется *образом* множества A' при отображении φ.

Множество $\varphi^{-1}(B') \overset{df}{=} \{x \in A \mid \varphi(x) \in B'\}$ называется *полным прообразом* множества B' при отображении φ.

Рассмотрим пример. Пусть отображение $f : A \to B$ определяется следующим образом:

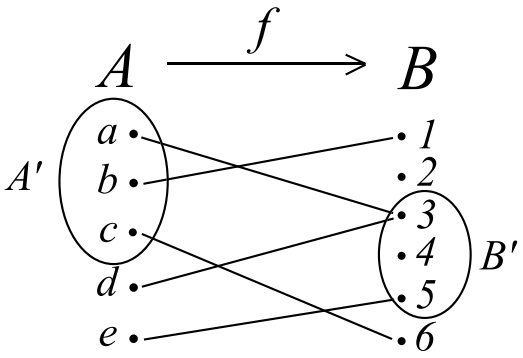

Рисунок 6

Элемент 1 является образом элемента b, а элемент c — прообразом элемента 6. Элемент 3 имеет два прообраза — a и d, а у элементов 2 и 4 прообразов нет вовсе. $f(A') = \{1, 3, 6\}$, $f^{-1}(B') = \{a, d, e\}$.

Определение. Пусть $\varphi : A \to B$ — отображение. Если φ^{-1} является отображением, то оно называется *обратным к* φ, а отображение φ — *обратимым*.

Определение. Отображение $\varphi : A \to B$ называется *инъективным*, если

$$\forall\, x, y \in A \big(\varphi(x) = \varphi(y) \Longrightarrow x = y\big).$$

Отображение $\varphi : A \to B$ называется *сюръективным*, если

$$\forall\, y \in B\, \exists\, x \in A \big(\varphi(x) = y\big).$$

Инъективное сюръективное отображение называется *биективным*.

Например, отображение $\varphi : \mathbb{R} \to \mathbb{R}$ такое, что $\varphi(x) = x^2$, не инъективно и не сюръективно: у числа 4 есть два прообраза — 2 и -2, а для числа -1 прообраза нет вовсе. Отображение $\varphi : \mathbb{R}_0^+ \to \mathbb{R}$ с тем же определяющим равенством инъективно, но не сюръективно. Отображение $\varphi : \mathbb{R}_0^+ \to \mathbb{R}_0^+$ является биективным.

Упражнение 10. Является ли отображение из примера выше (рисунок 6) инъективным? сюръективным? биективным?

Теорема 5. *Отображение φ биективно тогда и только тогда, когда φ обратимо.*

Как Вы помните со школы, теоремы, содержащие слова «тогда и только тогда, когда», «если и только если» и им подобные, состоят из двух утверждений. Условно такие теоремы можно представить в виде

$$\mathcal{A} \Longleftrightarrow \mathcal{B},$$

что на самом деле содержит в себе утверждения

$$\mathcal{A} \Longrightarrow \mathcal{B} \text{ и } \mathcal{B} \Longrightarrow \mathcal{A}.$$

Естественно, доказательство таких теорем состоит так же из двух частей — доказательств каждого из составляющих её утверждений. Напомним, что если $\mathcal{A} \Longrightarrow \mathcal{B}$, то условие $\mathcal{B}$ называется *необходимым* условием для $\mathcal{A}$, а условие $\mathcal{A}$ — *достаточным* для $\mathcal{B}$. Например, если на улице идёт дождь, то асфальт мокрый (естественно, ничем не прикрытый асфальт). Наличие дождя является достаточным условием для того, чтобы асфальт был мокрым. В то время как мокрый асфальт — одно из необходимых условий наличия дождя. Заметим, что мокрого асфальта недостаточно для того, чтобы был дождь. Равно как и дождь — вовсе не необходимое условие мокрого асфальта. Вернёмся с улицы на лекцию и разберём

Доказательство (теорема 5).

Необходимость. Пусть $\varphi : A \to B$ — биективное отображение. Докажем, что φ^{-1} является отображением. Для этого проверим два условия определения. Так как φ сюръективно, то для каждого $b \in B$ найдётся $a \in A$ такой, что $\varphi(a) = b$, т.е. $\varphi^{-1}(b) = a$. В силу инъективности отображения φ он единственен. По определению φ является обратимым отображением.

Достаточность. Пусть $\varphi : A \to B$ обратимо. Тогда $\varphi^{-1} : B \to A$ является отображением. Следовательно, для каждого $b \in B$ найдется $a \in A$ такой, что $\varphi^{-1}(b) = a$, т.е. $b = \varphi(a)$. Значит, φ сюръективно. Предположим, что $\varphi(a_1) = \varphi(a_2) = b$. Тогда $a_1 = \varphi^{-1}(b)$ и $a_2 = \varphi^{-1}(b)$. Так как φ^{-1} — отображение, то $a_1 = a_2$, т.е. φ инъективно. □

Определение. Пусть $\varphi : A \to B$ и $f : B \to C$ — отображения. Отображение $\psi : A \to C$ называется *композицией* отображений φ и f, если

$$\psi(x) = z \Longleftrightarrow \exists\, y \in B \big(\varphi(x) = y \wedge f(y) = z\big).$$

Композицию отображений φ и f будем обозначать через $\varphi \circ f$ или φf.

Теорема 6. *Если $\varphi : A \to B$ и $f : B \to C$ инъективны (сюръективны, биективны), то φf инъективно (сюръективно, биективно).*

Доказательство.

Предположим, что $\varphi : A \to B$ и $f : B \to C$ инъективны. Тогда

$$f(\varphi(a_1)) = f(\varphi(a_2)) \overset{f\text{ — ин}}{\Longrightarrow} \varphi(a_1) = \varphi(a_2) \overset{\varphi\text{ — ин}}{\Longrightarrow} a_1 = a_2.$$

Пусть теперь $\varphi : A \to B$ и $f : B \to C$ сюръективны, $c \in C$. В силу сюръективности отображения f существует $b \in B$ такой, что $f(b) = c$. В силу сюръективности отображения φ существует $a \in A$ такой, что $\varphi(a) = b$. Следовательно, для любого $c \in C$ существует $a \in A$ такой, что $f(\varphi(a)) = f(b) = c$, т.е. φf сюръективно.

Доказательство третьей части теоремы очевидно. □

Теорема 7. *Пусть $\varphi : A \to B$ сюръективно. Тогда для любых отображений $f_1 : B \to A$ и $f_2 : B \to A$*

$$\varphi f_1 = \varphi f_2 \Longrightarrow f_1 = f_2.$$

Теорема 8. *Пусть $\varphi : A \to B$ и $f : B \to C$ биективны. Тогда*

$$(\varphi f)^{-1} = f^{-1}\varphi^{-1}.$$

Теорема 9. *Пусть $\varphi : A \to B$, $A_1, A_2 \subseteq A$, $B_1, B_2 \subseteq B$. Тогда*

1. $\varphi(A_1 \cup A_2) = \varphi(A_1) \cup \varphi(A_2)$.
2. $\varphi^{-1}(B_1 \cup B_2) = \varphi^{-1}(B_1) \cup \varphi^{-1}(B_2)$.
3. $\varphi(A_1 \cap A_2) \subseteq \varphi(A_1) \cap \varphi(A_2)$.
4. $\varphi^{-1}(B_1 \cap B_2) = \varphi^{-1}(B_1) \cap \varphi^{-1}(B_2)$.

Доказательство.

Докажем пункт 3. Пусть $b \in \varphi(A_1 \cap A_2)$. Следовательно, существует $a \in A_1 \cap A_2$ такой, что $\varphi(a) = b$. Так как $a \in A_1 \cap A_2$, то $a \in A_1$ и $a \in A_2$. Поэтому $b \in \varphi(A_1)$ и $b \in \varphi(A_2)$, т.е. $b \in \varphi(A_1) \cap \varphi(A_2)$. Обратное включение, вообще говоря, неверно (приведите пример). □

Домашнее задание. Докажите теоремы 7 – 9.

§8. Алгебраические операции

В этом параграфе мы повторим в основном определения и свойства, которые Вы изучали в курсе алгебры, а также вспоминали в предыдущих параграфах. Иногда наряду с натуральными числами удобно использовать число 0.

Поэтому в некоторых случаях 0 также считают натуральным числом. Множество всех натуральных чисел с нулём будем обозначать через ω.

Определение. Отображение $f : A^n \to A$, где $n \in \omega$, называется *n-местной операцией* на множестве A. В случае, когда $n = 0$, множество A^n состоит из единственного элемента — $\varnothing$. Следовательно, при отображении f во множестве A зафиксируется единственный элемент, в связи с чем такую операцию называют *константой*. Если $n = 1$, то операцию f называют *унарной*. Если $n = 2$, то операцию f называют *бинарной*.

Например, отображение $f : \mathbb{R} \to \mathbb{R}$ такое, что $f(x) = x^2$, является унарной операцией. Отображение $g : \mathbb{R}_0^+ \to \mathbb{R}$, определяемое равенством $g(x) = \sqrt{x}$, не является операцией, а $g : \mathbb{R}_0^+ \to \mathbb{R}_0^+$ такое, что $g(x) = \sqrt{x}$, является унарной операцией. Бинарными операциями будут обычные операции сложения и умножения на множествах $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, а вычитание и деление — не для всех множеств (почему?).

Всюду далее в этой лекции речь будет идти о бинарных операциях. Если $\circ$ — операция на A, то вместо $\circ(x, y) = z$ будем писать $x \circ y = z$.

Определение. Определим свойства операции $\circ$ на множестве A:

$\circ$ — *коммутативная* $\overset{df}{\iff} \forall\, x, y \in A \big(x \circ y = y \circ x\big)$,

$\circ$ — *ассоциативная* $\overset{df}{\iff} \forall\, x, y, z \in A \big(x \circ (y \circ z) = (x \circ y) \circ z\big)$,

$\circ$ — *сократимая слева* $\overset{df}{\iff} \forall\, x, y, z \in A \big(z \circ x = z \circ y \Longrightarrow x = y\big)$,

$\circ$ — *сократимая справа* $\overset{df}{\iff} \forall\, x, y, z \in A \big(x \circ z = y \circ z \Longrightarrow x = y\big)$,

$\circ$ — *сократимая* $\overset{df}{\iff}$ $\circ$ сократима слева и справа,

$\circ$ — *обратимая слева* $\overset{df}{\iff} \forall\, x, y \in A\, \exists\, z \in A \big(z \circ x = y\big)$,

$\circ$ — *обратимая справа* $\overset{df}{\iff} \forall\, x, y \in A\, \exists\, z \in A \big(x \circ z = y\big)$,

$\circ$ — *обратимая* $\overset{df}{\iff}$ $\circ$ обратима слева и справа,

$e \in A$ — *нейтральный* $\overset{df}{\iff} \forall\, x \in A \big(x \circ e = e \circ x = x\big)$,

$y \in A$ — *симметричный для* $x \in A \overset{df}{\iff} x \circ y = y \circ x = e$, где e — нейтральный для $\circ$,

$\theta \in A$ — *нулевой* $\overset{df}{\iff} \forall\, x \in A \big(x \circ \theta = \theta \circ x = \theta\big)$,

$a \in A$ — *идемпотент* $\overset{df}{\iff} a \circ a = a$,

$\circ$ — *идемпотентная* $\overset{df}{\iff} \forall\, x \in A \big(x \circ x = x\big)$.

Рассмотрим операцию $\cap$ на множестве $\mathcal{P}(A)$, где $A \neq \varnothing$. Согласно теореме 2, эта операция обладает свойствами коммутативности, ассоциативности, идемпотентности, а также существованием нейтрального элемента A и нулевого элемента $\varnothing$. Легко убедиться, что существование для каждого элемента симметричного ему элемента, сократимость слева и справа, обратимость слева и справа

не выполняются.

Упражнение 11. Будет ли операцией обычное сложение, умножение, вычитание, деление на множестве $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q} \setminus \{0\}$? Если да, то какими свойствами она обладает?

Определение. Подмножество B множества A, на котором определена операция $\circ$, называется *замкнутым относительно* $\circ$, если

$$\forall\, x, y \in B \big(x \circ y \in B\big).$$

Определение. Если на множестве A заданы две операции $\circ$ и $*$, для которых выполняется условие

$$\forall\, x, y, z \in A \big(x * (y \circ z) = (x * y) \circ (x * z)\big),$$

то операция $*$ называется *дистрибутивной слева относительно* $\circ$. Аналогично определяется *дистрибутивность справа* и *дистрибутивность* (двухсторонняя).

§9. Основные алгебраические системы

В этом параграфе напомним основные алгебраические системы — полугруппы, группы, кольца, поля. Мы не ставим перед собой задачу изучить подробно свойства этих алгебраических систем, это вопрос алгебры. Ограничимся в рамках курса математической логики определениями этих алгебраических систем и примерами.

Определение. Пусть на множестве A заданы операции $f_1, f_2, \ldots, f_n$ и отношения $\rho_1, \rho_2, \ldots, \rho_m$. Набор $\langle A; f_1, f_2, \ldots, f_n, \rho_1, \rho_2, \ldots, \rho_m\rangle$ называется *алгебраической системой*.

Определение. Алгебраическая система $\langle S; \circ\rangle$, где $\circ$ — ассоциативная операция, называется *полугруппой*.

Примеров полугрупп можно привести достаточно много. Некоторые из них:

— Пусть $A^A \stackrel{df}{=} \{\varphi : A \to A\}$ для некоторого множества $A \neq \varnothing$, $\circ$ — композиция отображений. Алгебраическая система $\langle A^A; \circ\rangle$ является полугруппой.

— Пусть $A \neq \varnothing$. Через B обозначим множество всех *слов* алфавита A, то есть конечных последовательностей символов из A. Определим на B операцию *конкатенации* — приписывания справа второго слова к первому:

$$u \circ v \stackrel{df}{=} uv.$$

Алгебраическая система $\langle B; \circ\rangle$ является полугруппой.

— Множества $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$ со стандартными операциями сложения или умножения образуют полугруппы.

Определение. Если $\mathcal{S} = \langle S; \circ \rangle$ — полугруппа, множество $T \subseteq S$ замкнуто относительно $\circ$, то $\langle T; \circ \rangle$ называется *подполугруппой* $\mathcal{S}$.

Например, $\langle \mathbb{N}; + \rangle$ — подполугруппа полугруппы $\langle \mathbb{Z}; + \rangle$, $\langle 2\mathbb{N} - 1; \cdot \rangle$ — подполугруппа полугруппы $\langle \mathbb{N}; \cdot \rangle$, $\langle \{2a + 3b \mid a, b \in \mathbb{N}\}; + \rangle$ — подполугруппа полугруппы $\langle \mathbb{N}; + \rangle$.

Определение. *Группой* называется алгебраическая система $\langle G; \circ \rangle$, где $\circ$ — ассоциативная операция, относительно которой в G существует нейтральный элемент и каждый элемент G имеет симметричный.

Группами являются, например, полугруппы целых, рациональных, действительных, комплексных чисел по сложению. Множество матриц заданного размера с целыми коэффициентами также является группой относительно операции сложения матриц.

Упражнение 12. Групповая операция сократима.

Определение. Если $\mathcal{G} = \langle G; \circ \rangle$ — группа, множество $H \subseteq G$ замкнуто относительно $\circ$ и каждый элемент в H имеет симметричный, который тоже принадлежит H, то $\langle H; \circ \rangle$ называется *подгруппой* $\mathcal{G}$.

Например,

— $\langle 2\mathbb{Z}; + \rangle$ — подгруппа $\langle \mathbb{Z}; + \rangle$,

— $\langle \{e\}; \circ \rangle$ — подгруппа группы $\langle G; \circ \rangle$, где e — нейтральный элемент в G,

— множество всех поворотов плоскости является подгруппой группы всех движений плоскости.

Определение. Если групповая операция коммутативна, то группа называется *коммутативной*, или *абелевой* (в честь математика Нильса Абеля).

Определение. *Кольцом* называется алгебраическая система $\langle K; \circ, * \rangle$, удовлетворяющая следующим условиям:

1) $\circ$ — ассоциативная операция,

2) $\circ$ — коммутативная операция,

3) существует нейтральный элемент $e \in K$ относительно операции $\circ$,

4) для каждого элемента из K существует симметричный относительно операции $\circ$,

5) $*$ дистрибутивна относительно $\circ$.

Если при этом $*$ ассоциативна (коммутативна), то кольцо называется *ассоциативным* (*коммутативным*). Если в K существует нейтральный элемент относительно $*$, то такое кольцо называется *кольцом с единицей*.

Упражнение 13. Какие из следующих алгебраических систем являются кольцами?

1. $\langle \mathbb{Z}; +, \cdot \rangle$.

2. $\langle k\mathbb{Z}; +, \cdot \rangle$, где $k \in \mathbb{Z}$.

3. $\langle \mathbb{Z}/\rho; +, \cdot \rangle$, где

$$a \rho b \iff a \text{ и } b \text{ имеют одинаковый остаток при делении на } m,$$

$\bar{a} + \bar{b} \stackrel{df}{=} \overline{a+b}$, $\bar{a} \cdot \bar{b} \stackrel{df}{=} \overline{a \cdot b}$. Такое кольцо называется *кольцом классов вычетов по модулю* m.

4. $\langle \mathbb{Z}^2; +, \cdot \rangle$, где $\langle a, b \rangle + \langle c, d \rangle \stackrel{df}{=} \langle a + c, b + d \rangle$, $\langle a, b \rangle \cdot \langle c, d \rangle \stackrel{df}{=} \langle ad, bc \rangle$.

Определение. Коммутативное кольцо $\langle P; \circ, * \rangle$ с единицей называется *полем*, если для всякого ненулевого элемента из P найдётся симметричный относительно $*$ элемент.

В качестве примеров укажем следующие поля:

— кольцо классов вычетов по простому модулю,

— кольца рациональных, действительных, комплексных чисел с обычными операциями сложения и умножения чисел,

— множество $\mathbb{Q}(\sqrt{2}) \stackrel{df}{=} \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ с обычными операциями сложения и умножения чисел,

— множество рациональных дробей, в числителе и знаменателе которых стоят многочлены от одной переменной с целыми коэффициентами и знаменатель которых — не нулевой многочлен.

§10. Мощность множеств

На первой лекции мы уже затрагивали понятие количества элементов в конечном множестве. Естественным кажется вопрос: а как быть с бесконечными множествами? Например, нам кажется очевидным, что чётных натуральных чисел ровно столько, сколько и нечётных. А если сравнивать натуральные числа и, например, целые — каких больше? В случае бесконечных множеств понятие «количество элементов» становится бессмысленным.

С другой стороны, нам вовсе не обязательно считать количество элементов. Вернёмся на несколько веков назад и вспомним историю появления чисел как универсального способа записи количества. Как, например, подсчитывать овец в стаде, если счёт и числа ещё не придуманы? В жаркие периоды необходимо было уводить стада в более прохладные регионы, а с уходом жары возвращать назад. А стада насчитывали тысячи голов. Естественно, владельцы не могли отпустить свой скот, не предприняв каких-либо мер предосторожности. Поначалу подсчёт вёлся следующим образом. У владельца был сосуд с небольшими глиняными жетонами, количество которых равно количеству овец. Каждый раз, когда стадо возвращалось домой, владелец подсчитывал овец, сопоставляя один жетон одной голове. Позже стали задаваться вопросом сохранности жетонов, а

именно — их количества. Было предпринято решение запечатывать сосуд, ставить на него подписи. Но и это не исключало взломов и подмены количества жетонов. Тогда на сосуде стали делать специальные засечки: по одной засечке на один жетон. И только спустя время людям пришла в голову гениальная идея: настолько гениальная, что удивительно, как она не появилась раньше. Зачем вообще запечатывать сосуд с жетонами, когда количество овец можно фиксировать с помощью этих же засечек? Позже эта система стала распространяться на другие сферы жизни, система засечек потерпела множество модификаций, группы по несколько засечек стали заменять на засечки специального вида...

Что же примечательного в этой истории? Будучи знакомыми с отображениями, Вы уже наверняка поняли, что фактически было установлено биективное отображение из множества овец во множество жетонов. Аналогичная ситуация с множеством жетонов и множеством засечек. А если бы овец было бесконечное множество? С помощью бесконечного множества жетонов можно было бы так же посчитать их «количество», поставив в соответствие один жетон одной овце, т.е. установив биекцию.

Идея биективного отображения одного множества в другое служит для обобщения понятия количества элементов на случай бесконечного множества. Так, например, мы можем с уверенностью утверждать, что чётных натуральных чисел ровно столько, сколько и нечётных: каждому нечётному натуральному числу поставим следующее за ним чётное, установив тем самым биективное отображение. Сказать, что эти два множества имеют одно и то же количество элементов, мы не можем. Но в чём-то эти множества всё-таки похожи. Вот это «что-то» и есть то, что в математике называют *мощностью* множества.

Определение. Множества A и B называются *равномощными* (обозначение: $|A| = |B|$), если существует биективное отображение из A в B.

Упражнение 14. Отношение равномощности является отношением эквивалентности.

Определение. Класс эквивалентности множества A по отношению равномощности называется *мощностью* множества A. Мощность множества A будем обозначать через $|A|$.

Теорема 10 (Кантора–Бернштейна). *Если существуют инъективные отображения $f : A \to B$ и $g : B \to A$, то $|A| = |B|$.*

Доказательство.

Пусть $a \in A$. Построим *цепь* с концом a следующим образом. Если существует такой элемент $b \in B$, что $g(b) = a$, то запишем

$$b \overset{g}{\mapsto} a;$$

если же такого элемента b нет, то построение закончено и цепь *имеет длину* 1. Далее, если найдётся такой элемент $a' \in A$, что $f(a') = b$, то запишем

$$a' \overset{f}{\mapsto} b \overset{g}{\mapsto} a$$

(рисунок 7); если же такого элемента a' нет, то построение закончено и цепь *имеет длину* 2. Продолжая этот процесс далее, мы либо остановимся на каком-то шаге и получим цепь, длина которой равна натуральному числу, либо никогда не остановимся. Длину цепи с концом a обозначим через l_a. Если цепь с концом a бесконечна, то будем писать $l_a = \infty$.

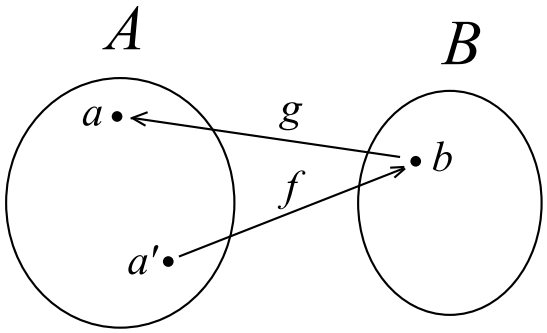

Рисунок 7

Таким образом, для каждого элемента $a \in A$ мы определили величину l_a. Представим множество A в виде объединения трёх непересекающихся подмножеств:

$$A = A_1 \sqcup A_2 \sqcup A_\infty,$$

где

$$A_1 = \{x \in A \mid l_x - \text{нечётное}\},$$
$$A_2 = \{x \in A \mid l_x - \text{чётное}\},$$
$$A_\infty = \{x \in A \mid l_x = \infty\}.$$

Построив аналогичным образом цепи для элементов из множества B, мы можем разбить его также на три непересекающихся подмножества:

$$B = B_1 \sqcup B_2 \sqcup B_\infty,$$

где

$$B_1 = \{x \in B \mid l_x - \text{нечётное}\},$$
$$B_2 = \{x \in B \mid l_x - \text{чётное}\},$$
$$B_\infty = \{x \in B \mid l_x = \infty\}.$$

Если $b \in B_2$, то в силу инъективности отображения f найдётся единственный элемент $a \in A$, для которого $f(a) = b$, причём $l_a = l_b - 1$, а значит, $a \in A_1$. С другой стороны, если $a \in A_1$ и $f(a) = b \in B$, то $l_b = l_a + 1$, поэтому $b \in B_2$. Следовательно, отображение $f : A_1 \to B_2$ является биективным. Аналогичным образом можно показать, что $g : B_1 \to A_2$ — биективное отображение. Наконец, легко понять, что если $a \in A_\infty$, то $f(a) = b \in B_\infty$, и наоборот, для каждого $b \in B_\infty$ найдётся единственный элемент $a \in A_\infty$ такой, что $f(a) = b$.

Построим отображение $h : A \to B$ следующим образом:

$$h(x) = \begin{cases} f(x), & \text{если } x \in A_1, \\ g^{-1}(x), & \text{если } x \in A_2, \\ f(x), & \text{если } x \in A_\infty. \end{cases}$$

Нетрудно понять, что h является биекцией, поэтому $|A| = |B|$. □

Пусть A и B — два бесконечных множества. Рассмотрим все возможные случаи, опираясь на условие теоремы 10.

Случай 1. Существуют инъективные отображения из A в B и из B в A. По теореме 10 $|A| = |B|$.

Случай 2. Существует инъективное отображение из A в B, и не существует инъективного отображения из B в A. В таком случае говорят, что *мощность множества A меньше мощности множества B*, и пишут $|A| < |B|$.

Случай 3. Не существует инъективного отображения из A в B, и существует инъективное отображение из B в A. В таком случае говорят, что *мощность множества A больше мощности множества B*, и пишут $|A| > |B|$.

Случай 4. Не существует инъективных отображений из A в B и из B в A. Возможна ли такая ситуация?

Так как для любого конечного множества $A = \{a_1, \ldots, a_n\}$, где $n \in \omega$, существует биекция $\varphi : A \to \{1, \ldots, n\}$, то под мощностью конечного множества будем понимать количество элементов в нём. Тогда указанные в случаях 1–3 соотношения также имеют место.

Сравнивать мощности бесконечных множеств имеет смысл только в том случае, когда существуют множества разных мощностей. Любой школьник 7 класса или даже младше с радостью Вам скажет, что есть конечные множества, а есть бесконечные, и что бесконечные множества в смысле «количества элементов» все одинаковы. Следующая теорема разрушает это представление о бесконечных множествах.

Теорема 11 (Кантора). $|A| < |\mathcal{P}(A)|$.

Доказательство проведём методом *от противного*. Этот метод доказательства известен Вам ещё со школьного курса геометрии. Мы будем часто пользоваться им при доказательстве теорем математической логики. Метод основан на так называемом *законе контрапозиции*, который кратко можно сформулировать следующим образом:

$$(\mathcal{A} \Longrightarrow \mathcal{B}) \Longleftrightarrow (\text{не } \mathcal{B} \Longrightarrow \text{не } \mathcal{A}).$$

Например, если на улице идёт дождь, то асфальт мокрый. Но если асфальт сухой, то дождя на улице уж точно нет.

Ход доказательства следующий. Допустим, нам нужно доказать утверждение $\mathcal{A} \Longrightarrow \mathcal{B}$. Предположим, что утверждение $\mathcal{A}$ истинно. Так как утверждение $\mathcal{B}$ либо истинно, либо ложно, то предположение о том, что $\mathcal{B}$ ложно, приведёт нас (согласно закону контрапозиции) к тому, что утверждение $\mathcal{A}$ ложно, что не так. Значит, наше предположение неверно и утверждение $\mathcal{B}$ истинно.

Доказательство (теорема 11).
Очевидно, если $A = \varnothing$, то

$$|A| = 0 < 1 = |\{\varnothing\}| = |\mathcal{P}(A)|.$$

Пусть $A \neq \varnothing$. Предположим, что существует биективное отображение $f : A \to \mathcal{P}(A)$. Рассмотрим множество

$$M = \{x \in A \mid x \notin f(x)\}.$$

Можество M не пусто: так как f — биекция, то найдётся $a \in A$ такой, что $f(a) = \varnothing \not\ni a$. В силу биективности f существует $m \in A$ такой, что $f(m) = M$. Тогда

$$m \in M \Longleftrightarrow m \notin f(m) \Longleftrightarrow m \notin M$$

— противоречие. Так как отображение $g : A \to \mathcal{P}(A)$ такое, что $g(a) = \{a\}$, является инъективным, то $|A| < |\mathcal{P}(A)|$. □

Познакомившись подробно с понятием мощности, дадим строгие определения конечных и бесконечных множеств.

Определение. Множество, не равномощное никакому своему собственному подмножеству, называется *конечным*. В противном случае множество называется *бесконечным*.

Так как бесконечные множества тоже можно сравнивать по мощности, то естественными кажутся вопросы: существует ли бесконечное множество с наименьшей мощностью? с наибольшей? Теорема 11 даёт отрицательный ответ на вопрос о существовании наибольшей мощности. Наименьшей бесконечной мощностью является мощность множества натуральных чисел.

Определение. Множество, равномощное ω, называется *счётным*. Мощность счётного множества будем обозначать через ω. Биекцию $f : \omega \to A$ иногда будем называть *нумерацией* счётного множества A, а $n \in \omega$ — номером элемента $f(n) \in A$ при нумерации f.

Следующая теорема даёт представление о структуре конечных и бесконечных множеств.

Теорема 12. *Имеют место следующие свойства:*

1. Всякое множество, содержащее бесконечное подмножество, само бесконечно.

2. Множество $\bar{n} \stackrel{df}{=} \{x \in \omega \mid x < n\}$, *где* $n \in \omega$, *конечно. Такое множество называется отрезком натурального ряда.*

3. Множество, равномощное бесконечному множеству, бесконечно.

4. Множество, равномощное конечному множеству, конечно.

5. Счётное множество бесконечно.

6. Множество конечно тогда и только тогда, когда оно равномощно отрезку натурального ряда.

7. Объединение конечного множества конечных множеств конечно.

8. Объединение счётного множества конечных множеств не более чем счётно.

9. Объединение конечного множества счётных множеств счётно.

10. Объединение счётного множества счётных множеств счётно.

11. Всякое подмножество счётного множества конечно или счётно.

12. Во всяком бесконечном множестве есть счётное подмножество.

13. Если A *бесконечно,* B *конечно, то* $|A \cup B| = |A| = |A \setminus B|$.

14. Если A *бесконечно,* B *счётно, то* $|A \cup B| = |A|$.

15. Если A *более чем счётно,* B *счётно, то* $|A \setminus B| = |A|$.

16. Декартово произведение двух счётных множеств счётно.

Домашнее задание. Докажите теорему 12. При доказательстве можно воспользоваться следующими указаниями:

1. Пусть $B \subset A$, B бесконечно, $C \subset B$, $|C| = |B|$. Построить биективное отображение из A в $(A \setminus B) \cup C$.

2. Индукцией по n.

3. По определению для бесконечного множества A существует биективное отображение $f : A \to B$ в собственное подмножество $B \subset A$. Пусть $|A| = |C|$. Нужно в C найти такое подмножество, которое будет равномощно B.

4. Воспользоваться п. 3.

5. Занумеровать элементы и построить биекцию на собственное подмножество, используя номера.

6. *Необходимость.* Показать, что если A конечно, то $A \setminus \{a\}$, где $a \in A$, тоже конечно. Построить отрезок $\bar{n}$, перебирая элементы конечного множества. *Достаточность.* Воспользоваться пп. 2 и 4.

7–10. Нарисовать обход.

11. Достаточно показать для ω. Взять бесконечное подмножество $A \subseteq \omega$ и построить биекцию $f : \omega \to A$.

12. Выбирать элементы из бесконечного множества по одному. Показать, что бесконечность множества при этом не исчезает. Для этого использовать п. 7.

13. $A \cup B = (A \setminus C) \cup C \cup B$, где $C \subseteq A$ счётно. Показать, что $|C \cup B| = |C|$. Построить биекцию между $A \cup B$ и A. Показать, что $A \setminus B$ бесконечно. Тогда $|A \setminus B| = |(A \setminus B) \cup B| = |A|$ (по доказанному ранее).

14. Аналогично п. 13, используя п. 9.

15. Аналогично п. 13.

16. Нарисовать обход.

Теорема 13. *Множество $\mathbb{R}$ несчётно.*

Доказательство.

Рассмотрим множество всех действительных чисел из отрезка $[0;1]$. Все такие числа в десятичной форме записи имеют вид $0,\ldots$ (из двух представлений числа 1 ($0,999\ldots$ и 1) выберем первое[1]). Предположим, что $[0;1]$ — счётное множество и f — его нумерация. Тогда каждая дробь из $[0;1]$ имеет номер при нумерации f. Пусть

$$q = 0, q_0 q_1 q_2 \ldots q_n \ldots,$$

где q_i отличается от i-ой цифры числа $f(i)$. Дробь q не имеет номера, что противоречит тому, что $[0;1]$ занумеровано с помощью f. Следовательно, $[0;1]$ — несчётное множество. По теореме 12 (п. 8) множество всех действительных чисел несчётно. □

Определение. Говорят, что множество имеет *мощность континуума*, если оно равномощно $\mathbb{R}$. Мощность континуума будем обозначать через $\mathfrak{c}$.

[1] Возможно, этот факт для некоторых читателей покажется удивительным, но числа $0,9999999\ldots$ и 1 есть разные записи числа 1. Существует много доказательств этого факта, в интернете полно различных шуток на тему равенства $0,9999999\ldots = 1$. Самое простое, которое мне нравится, заключается в том, что между числами $0,9999999\ldots$ и 1 нет действительных чисел, в то время как отношение $<$ на множестве $\mathbb{R}$ является плотным порядком.

Теорема 14. *Имеют место следующие свойства:*

1. Объединение конечного или счётного множества множеств мощности континуума имеет мощность континуума.

2. Декартово произведение двух множеств, имеющих мощность континуума, имеет мощность континуума.

Домашнее задание. Докажите теорему 14.

В 1877 году Георг Кантор выдвинул гипотезу о том, что любое бесконечное подмножество множества мощности континуума является либо счётным, либо само имеет мощность континуума. Другими словами, гипотеза предполагает, что мощность континуума — наименьшая, превосходящая мощность счётного множества, и между счётной и континуумом нет мощностей. Эта гипотеза получила название

Континуум-гипотеза. Не существует множества A такого, что

$$\omega < |A| < c.$$

Эту гипотезу можно распространить на общий случай: невозможно

$$|A| < |B| < |\mathcal{P}(A)|.$$

Это утверждение носит название **обобщённая континуум-гипотеза**. Безуспешные попытки доказать континуум-гипотезу предпринимались до тех пор, пока в трудах Гёделя и Коэна не было показано, что средствами аксиоматической теории множеств её невозможно ни доказать, ни опровергнуть.

§11. Парадоксы теории множеств

Парадокс Рассела

В 1901 году британский философ, логик и математик Бертран Рассел открыл теоретико-множественный парадокс, демонстрирующий противоречивость логической системы Фреге, которая являлась ранней попыткой формализации наивной теории множеств Георга Кантора, создателя теории множеств. Этот парадокс довольно известен, и у него есть много версий. Приведём одну из них.

В одном полку жил-был полковой парикмахер, которого по историческим причинам называют брадобреем (отсюда и другое название этого парадокса: *Парадокс брадобрея*). Однажды командир полка приказал ему брить тех и только тех, кто сам не бреется. Вполне разумный приказ — зачем тратить время

брадобрея на тех, кто в состоянии побриться сам? Брадобрей, получив приказ, сначала обрадовался, так как многие солдаты умели бриться сами. Он побрил тех, кто бриться сам не умел, а потом сел на пенёк и задумался: а что ему с собой-то делать? Ведь если он будет брить себя, то нарушит приказ командира не брить тех, кто бреется сам. А если он сам себя брить не будет, то окажется, что он по приказу командира должен всё-таки себя побрить...

Что стало с несчастным брадобреем, история умалчивает.

Казалось бы, при чём здесь теория множеств? Попробуем разобраться, в чём же проблема приказа командира полка. Командир пытался определить множество людей, которых брадобрей должен брить, используя описательный способ, а именно

$$\{x \mid x \text{ сам не бреется}\}.$$

На первый взгляд, в этом множестве нет ничего необычного. Но возникает вопрос: принадлежит ли этому множеству брадобрей?

Приведём другую версию парадокса Рассела. Назовём прилагательное русского языка *рефлексивным*, если оно обладает свойством, которое определяет. Например, «русский» — рефлексивное прилагательное, так как является русским словом, а «английский» — нет; «трёхсложный» — рефлексивное, а «пятисложный» — нет (придумайте ещё примеры). Но что мы можем сказать про слово «нерефлексивный»? «Нерефлексивный» рефлексивно или нерефлексивно? Если оно рефлексивно, то оно нерефлексивно. Если оно нерефлексивно, то оно не нерефлексивно, то есть рефлексивно...

Наконец, дадим более строгую формулировку парадокса. Пусть

$$M = \{A \mid A \notin A\}.$$

Верно ли, что $M \in M$? Или же $M \notin M$?

Парадокс Кантора

Этот парадокс был открыт раньше парадокса Рассела, в 1899 году, самим Кантором и стимулировал разработку строгой аксиоматики теории множеств.

Как мы уже отмечали ранее, согласно теореме 11 не существует самого «мощного» множества, то есть множества, обладающего наибольшей мощностью. Не существует потому, что для любого сколь угодно мощного множества можно указать ещё более мощное. Это с одной стороны. А с другой — интуитивно очевидно, что множество всех множеств должно быть самым мощным, ведь оно представляет совокупность всех множеств, какие только могут существовать, и вообще включает все мыслимые множества.

Дадим более строгую формулировку. Предположим, что множество всех множеств существует: $\mathcal{U} = \{x \mid x = x\}$. Так как $\mathcal{P}(\mathcal{U})$ — множество множеств, то $\mathcal{P}(\mathcal{U})$ является подмножеством $\mathcal{U}$. Но тогда $|\mathcal{P}(\mathcal{U})| \leqslant |\mathcal{U}|$. По теореме 11 $|\mathcal{P}(\mathcal{U})| > |\mathcal{U}|$. Получили противоречие. Значит, наше предположение неверно и не существует множества всех множеств.

Фиксация мощности множества всех множеств представляется очень сложной задачей. И как бы близко мы ни подбирались к определению мощности множества всех множеств, в следующий момент времени наш результат может оказаться уже не соответствующим действительности.

Это рассуждение иллюстрирует невозможность получения истинного непротиворечивого логического вывода на основе зыбких, ошибочных, ложных оснований, посылок. Как следствие, теория множеств получила определённую аксиоматику, в рамках которой вопрос о существовании множества всех множеств не ставится.

Парадокс Берри

Существует лишь конечное число слогов в русском языке. Следовательно, имеется лишь конечное число таких фраз русского языка, которые содержат не более пятидесяти слогов. Поэтому с помощью таких фраз можно охарактеризовать только конечное число натуральных чисел. Пусть k есть *наименьшее из натуральных чисел, которые не характеризуются никакой фразой русского языка, содержащей не более пятидесяти слогов*. Напечатанная курсивом фраза характеризует число k и содержит не более пятидесяти слогов.

Парадоксы Рассела, Кантора и Берри приводят нас к тому, что не всякое синтаксически корректное логическое условие P может определять множество. Схема аксиом

$$\forall x \big(x \in A \iff P(x)\big),$$

описывающая множество A, была отвергнута как противоречивая. Вместо этого была разработана система ограничений, накладываемых на условие P.

Ещё пример

Назовите наименьшее натуральное число, не упомянутое на протяжении всех лекций первой главы.

Казалось бы, что тут сложного? С одной стороны, это можно сделать, так как множество натуральных чисел вполне упорядочено и можно найти наибольшее упомянутое число. Но парадокс в том, что если бы мы могли определить

это число, оно автоматически бы перешло из класса не упомянутых в лекциях в класс упомянутых.

Парадокс Тристрама Шенди

В романе Стерна «Жизнь и мнения Тристрама Шенди, джентльмена» герой обнаруживает, что ему потребовался целый год, чтобы изложить события первого дня его жизни, и ещё один год, чтобы описать второй день. В связи с этим герой сетует, что материал его биографии будет накапливаться быстрее, чем он сможет его обработать, и он никогда не сможет её завершить.

— Теперь я утверждаю, — возражает на это Рассел, — что если бы он жил вечно и его работа не стала бы ему в тягость, даже если бы его жизнь продолжала быть столь же богатой событиями, как вначале, то ни одна из частей его биографии не осталась бы ненаписанной.

Действительно, события n-го дня Шенди мог бы описать за n-й год, и, таким образом, в его автобиографии каждый день оказался бы запечатлённым.

Иначе говоря, если бы жизнь длилась бесконечно, то она насчитывала бы столько же лет, сколько дней.

По мнению Рассела, решение лежит в том, что целое эквивалентно его части в бесконечности. Однако же разрешение проблемы лежит в области чистой математики. Очевидно, что есть два множества — года и дни, между элементами которых установлено биективное отображение. Тогда при условии бесконечной жизни главного героя имеется два бесконечных равномощных множества, что, если рассматривать мощность как обобщение понятия количества элементов в множестве, разрешает парадокс.

Данное рассуждение демонстрирует нарушение принципа «часть меньше целого», которое характерно для бесконечных множеств и даже используется нами для отличия их от конечных. Критерий бесконечности множества, предложенный Дедекиндом, формулируется следующим образом: *множество является бесконечным тогда и только тогда, когда оно равномощно некоторой своей части*. Можно доказать, что критерий Дедекинда в аксиоматической теории множеств эквивалентен определению бесконечного множества как множества, содержащего счётное подмножество элементов.

Дед Мороз и конфеты

Рассмотрим следующую историю.

На Новый год к детишкам пришёл Дед Мороз и принёс с собой огромный мешок конфет. Конфет в мешке бесконечно много, и все они занумерованы

натуральными числами: на каждой конфете написан её номер, а для каждого натурального числа есть конфета с таким номером. За одну минуту до полуночи Дед Мороз взял конфету с номером 1 и подарил детям. Через полминуты Дед Мороз понял, что дал мало конфет, и дал детям конфеты с номерами 2 и 3, а конфету с номером 1 забрал. Ещё через четверть минуты он дал детям конфеты с номерами 4, 5, 6 и 7, а конфеты с номерами 2 и 3 забрал. И так далее: щедрый Дед Мороз каждый раз по истечении половины оставшегося времени даёт вдвое больше конфет, чем давал в предыдущий раз, забирая при этом отданные ранее конфеты.

Сколько же конфет будет у детей в полночь?

С одной стороны, количество конфет у детей стремительно растёт. С приближением полуночи Дед Мороз со скоростью света выдаёт детям огромное количество конфет, не помещающихся дома и во всём городе! Но давайте подумаем: у кого в полночь будет конфета с номером 1? У Деда Мороза, так как он её забрал, отдавая конфеты с номерами 2 и 3. А у кого будет конфета под номером 2? 3? Также у Деда Мороза — он их тоже забрал. Дед Мороз забрал и конфеты с номерами 100 и 150, и конфету с номером 10000000000000000000...

На самом деле никакого парадокса тут нет. Всё дело в том, что бесконечные множества устроены существенно сложнее конечных, и интуиция тут не всегда срабатывает.

Математики довольно долго боялись столь абстрактного понятия *множество*. Понятно, почему: возникали парадоксы и множества с непонятными свойствами, примеры которых Вы прочитали в этом параграфе.