Элементы математической логики и дискретной математики

Драч Константин Дмитриевич*

Частичные цели курса:

1. Организовать плавный переход между школьной и реальной математикой.
2. На элементарном и доступном языке ввести основные математические объекты дискретной математики и математической логики и научиться с ними работать.
3. Обсудить некоторые фундаментальные математические идеи (например, доказуемость, измеримость).
4. Преодолеть страх перед обозначениями, формулировками, доказательствами, логическими высказываниями, импликациями, вычислениями... и всем остальным, что может на начальных этапах вызвать неконтролируемую панику.

(!) Внимание! Возможно наличие очепаток. Все замеченные опечатки и ошибки просьба присылать автору.

Motto: Keep calm and do math

*http://geometry.karazin.ua/~drach, e-mail: drach@karazin.ua

1 *Лекция 1*

1.1 Что такое множество? “Наивная” теория множеств

Стая птиц, табун лошадей, косяк рыб, прайд львов, выводок поросят, группа людей... – такое большое количество разных названий для, по сути, одного и того же понятия *совокупности* объектов (птиц, лошадей, etc). В математике такие совокупности принято называть *множествами.*

Определение 1.1. Множество – это совокупность объектов (*элементов множества*), которые объединены по некоторому *свойству.*

Так, множество (стая) птиц на крыше – это все те птицы, которые сидят на конкретной крыше. Множество (группа) людей в аудитории – люди, сидящие в данный момент в данной аудитории, etc. Самые “математические” множества, которые появлялись в школе и первыми приходят на ум, это множества чисел: натуральных $\mathbb{N}$, целых $\mathbb{Z}$, рациональных $\mathbb{Q}$, иррациональных, действительных (вещественных) $\mathbb{R}$, возможно, комплексных $\mathbb{C}$. Но множества могут быть разной природы!

В математике, для обозначения множеств принято использовать заглавные латинские буквы $A, B, F, M \dots$ Если a – какой-то элемент множества A, то пишут

$$a \in A$$

(читается, “a принадлежит A”). Если же a не лежит в множестве A, то пишут $a \notin A$(“a не принадлежит A”). Обычно, элементы A берутся из некоторого большого множества I, которое называется *универсальным множеством.* Множество, в котором нет ни одного элемента, называется *пустым множеством* и обозначается $\emptyset$[1]. Множество B, все элементы которого являются одновременно и элементами множества A, называется *подмножеством* A. Этот факт обозначается

$$B \subset A.$$

Заметим, что

$$A \subset A, \quad \emptyset \subset A, \quad A \subset I$$

для любого множества A и универсального множества I. Если B не является подмножеством A, то пишут $B \not\subset A$.

Множества, состоящие из конечного числа элементов называются *конечными.* Множество *бесконечно*, если оно состоит из бесконечного числа элементов.

Множества (конечные и бесконечные) называются *равными* $A = B$, если они состоят из одних и тех же элементов.

[1] Этот символ представляет собой перечеркнутый кружек.

Определения выше, вместе с основами "наивной" теории множеств, предложил **Георг Кантор** в середине XIX века. Почему его теория называется "наивной"? Проблема в том, что определение 1.1 в таком его виде может вести к парадоксам. Вот два классических примера.

Пример 1.1 (Парадокс брадобрея)**.** *Армейскому брадобрею приказали брить тех и только тех людей в гарнизоне, которые не бреют себя сами*[2]*. Брил ли брадобрей себя?*

Другими словами: пусть B – множество всех людей в гарнизоне, которые бреют себя, HB – множество тех людей в гарнизоне, которые себя не бреют (т.е. B и HB вместе составляют весь гарнизон и при этом не имеют общих элементов), а b – это брадобрей. Вопрос выше можно переформулировать: что верно,

$$b \in B \quad \text{или} \quad b \in HB?$$

Правильный ответ: ни то, ни другое. Такие множества определить нельзя.

Пример 1.2 (Список списков)**.** *Должен ли список всех списков, которые не включают себя, включать себя?*

Другими словами: Пусть в некотором городе решили сделать ревизию библиотек. Главная бибилиотека попросила все меньшие библиотеки составить списки книг в наличии. Каждый из таких списков – это отдельная книга. Некоторые библиотеки включили ее в список наличных книг, а некоторые нет. Собрав списки, главная библиотека составила мастер-список тех списков, *которые не включали себя.* Должна ли главная библиотека включить получившийся мастер-список[3] в перечень самого себя?

Если C – множество (по сути, список) списков от меньших библиотек, которые себя не содержат, то верно ли, что

$$C \in C \text{ (считая в первом случае } C \text{ – списком)?}$$

Ответить на этот вопрос невозможно. Действительно, если $C \in C$, но тогда это уже не будет список списков, которые себя не содержат. Если $C \notin C$, то мастер-список не будет содержать себя, а значит, как и любой другой список себя не содержащий, должен быть включен в мастер-список, что противоречит $C \notin C$.

Итак, ни один из возможных вариантов ($C \in C$ и $C \notin C$) не возможен.

Разрешение этих парадоксов невозможно без строгого построения теории множеств. Это можно сделать выбрав правильную систему аксиом (бездоказательных утверждений). Такая система аксиом называется *системой аксиом*

[2] Отметим, что брадобрей – мужчина, бреет он мужчин, в гарнизоне только мужчины.

[3] Мастер-список тоже список; слово "мастер" добавлено для того, чтобы отличать этот список от списков меньших библиотек.

Цермело – Френкеля. В дальнейшем мы поговорим о некоторых аспектах этой системы и ее связью с логикой. Но в рамках этого курса мы не будем вдаваться в детали построения системы Цермело – Фрункеля и останемся в рамках "наивного" подхода, который совершенно непротиворечив в большинстве случаев.

1.2 Способы задания множеств

Существует несколько способов задания множеств. Множество можно задать просто перечислив его элементы, если их конечное число. Для этого элементы записывают в $\{\}$ скобках через запятую. Например:

1. $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ – множество всех десятичных цифр; заметим $\{1, 5, 9\} \subset A$, $\{-2, 3, 0\} \not\subset A$.

2. $B = \{2\}$ – множество всех четных простых чисел.

3. $C = \{\text{Север, Юг, Запад, Восток}\}$ – множество всех направлений света.

4. $M = \emptyset$ – множество всех ныне живущих мамонтов. Отметим, что $\{\emptyset\}$ содержит один элемент – $\emptyset$.

5. $T = \{\{\text{Даша, Паша}\}, \{\text{Света, Дима}\}, \{\text{Катя, Алена, Инна, Николай}\}\}$ – множество всех танцующих групп на дискотеке. Заметим, что Катя $\notin T$, хотя $\{\text{Даша, Паша}\} \in T$ так как $\{\text{Даша, Паша}\}$ является элементом (а не подмножеством!) T.

6. $Z = \{z_1, z_2, \dots, z_n\}$ – абстрактное множество, состоящее из n элементов z_1, z_2 и так далее, z_n.

Для записи элементов множества не важен порядок и количество раз, сколько записан элемент. Например,

$$A_1 = \{1, 1, 2, 5, 5, 5\} = \{1, 2, 5\}.$$

В тоже время,

$$A_2 = \{1, \{1, 2, 5\}, \{5\}\} \neq A_1.$$

Задание множества явно (перечислением его элементов) возможно лишь в некоторых случаях. Чаще всего множество выделяется согласно некоторому признаку (см. определение 1.1; *а что за признак фигурирует в заданиях 1 – 6 выше?*). Для этого использую обозначение $\{* : \star\}$, где на месте $*$ указывают, какого вида элементы должны быть в множестве. Иногда тут же указывают, из какого универсального множества берутся эти элементы. На месте $\star$ указывают все свойства, которыми должны обладать выбираемые в множество элементы. Двоеточие : при таком задании читается "такие, что". Приведем несколько примеров:

0. $\mathbb{Q} = \left\{\dfrac{m}{n} : m \in \mathbb{Z} \text{ и } n \in \mathbb{N}\right\}$ – "$\mathbb{Q}$ *это множество всех элементов (чисел) вида* $\dfrac{m}{n}$ *таких, что* m *– целое число,* n *– натуральное*" – задание множества рациональных чисел.

1. Для множества A, $2^A = \{B\colon B \subset A\}$ – "2^A *– это множество всех* B *таких, что* B *является подмножеством* A" – множество всех подмножеств. Откуда такое обозначение? Заметим, что элементами 2^A являются множества. Если $A = \{1, 2, 3\}$, то

$$2^A = \{\emptyset, \{1, 2, 3\}, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}$$

 – всего $8 = 2^3$ элементов.

2. $S = \{x \in \mathbb{R}\colon x^2 + x - 2 = 0\}$ (читается *"множество всех тех вещественных* x*, что* $x^2 + x - 2 = 0$*"*) – множество корней квадратного уравнения. Из школьного курса известно, что S совпадает с множеством $\{-2, 1\}$.

3. $S' = \{x \in \mathbb{N}\colon x^2+x-2 = 0\}$ – множество натуральных корней уравнения. В этом примере мы поменяли универсальное множество для x. Имеем, $S' = \{1\}$.

4. Для множеств M, N определим $M \times N = \{(m, n)\colon m \in M, n \in N\}$ – декартово произведение двух множеств. Например, декартова плоскость – это декартово произведение $\mathbb{R} \times \mathbb{R}$ (часто пишут $\mathbb{R}^2$).

5. $R = \{(n, m)$ – пар целых чисел : $3n - 2m = 1\}$ – множество решений так называемого *диофантового уравнения* $3n - 2m = 1$. Можно показать (*как?*), что $R = \{(1 + 2k, 1 + 3k)\colon k \in \mathbb{Z}\}$. R – бесконечное множество.

6. Для данных точек A и B на плоскости положим

$$SP_{A,B} = \{X \text{ – точка плоскости } : AX = XB\}$$

 – геометрическое место точек (множество точек), находящихся на одинаковом расстоянии от двух данных. Это – серединный перпендикуляр! *Как определить окружность?*

7. $C = \{(x, y) \in \mathbb{R}^2\colon x^2 + y^2 \leqslant 4\}$ – круг радиуса 2. *Как определить множество точек над параболой* $y = 5x^2$ (так называемый, *надграфик*)?

К бесконечным множествам мы еще вернемся в последующих лекциях (обсудим отображения бесконечных множеств, счетность, мощность, etc)

Бывает так, что множество задается просто, но его подмножества или свойства определить очень сложно. Такие исследования порой составляют содержания целых областей математики. Например:

1. Пусть $M = \{1, 2, 3\}$, а b – цифра, стоящая на стотысячном месте в десятичной записи числа $\pi = 3,141592\ldots$. Можно ли сходу сказать, что $b \in M$, или что $b \notin M$? Скорее всего нет. Принципиально же (с помощью компьютера) это можно выяснить.

2. Пусть P – множество всех простых чисел. Конечно ли P? Нет (доказательство опирается на основную теорему арифметики).

3. Пусть $Tw = \{p \in \mathbb{N} \colon p$ и $p + 2$ – простые числа$\}$ – множество простых чисел-близнецов[4]. Легко видеть, что $3 \in Tw$, $5 \in Tw$, $11 \in Tw$ и т.д. Конечно ли Tw? Гипотеза чисел-близнецов (открытая!) состоит в том, что Tw – бесконечное множество.

   Недавний прорыв (2013 год, **Итан Чжан**): для заданного (но фиксированного!) числа $N = 246$ множество

   $$Tw_N = \{p \in \mathbb{N} \colon \text{среди } p, p + 1, \ldots, p + N \text{ есть два простых числа}\}$$

   – бесконечно. Осталось уменьшить N до 2.

4. $F_2 = \{(a, b, c)$ – тройка натуральных чисел: $a^2 + b^2 = c^2\}$. Как велико это множество? Оказывается, F_2 – бесконечно (пифагоровы тройки). Пусть теперь

   $$F_n = \{(a, b, c) \text{ – тройка натуральных чисел: } a^n + b^n = c^n\}$$

   для натурального $n > 2$. Как велико F_n? Оказывается, $F_n = \emptyset$ для всех $n > 2$. Это – великая теорема Ферма, доказанная в 1994 сэром **Эндрю Вайлсом**.

5*. P – множество проблем, которые можно *решить* за полиномиальное время на машине Тьюринга[5] (быстро решаемые). NP – множество проблем, которые можно *проверить* за полиномиальное время на машине

[4]Название множества Tw от англ. **tw**eens – близнецы.

[5]В очень-очень грубом смысле можно думать об этом, как о решении задачи на своем домашнем ПК. Машина Тьюринга является абстрактной вычислительной машиной (компьютером), придуманная **Аланом Тьюрингом** для формализации понятия “алгоритм”.

Тьюринга (быстро проверяемые). Например, существует ли в множестве $\{-2, -3, 15, 14, 7, -10\}$ подмножество с суммой 0. Да, например, $\{-2, -3, -10, 15\}$. Это легко проверить (NP сложная задача). Но все известные алгоритмы нахождения таких сумм – экспоненциальны (количество операций порядка 2^n, где n – количество элементов). Известно, что $P \subset NP$. Верно ли, что $P = NP$? Нерешенная задача на миллион долларов (millennium prize problem).

1.3 Операции над множествами и диаграммы Эйлера(– Венна)

Над множествами можно проводить операции, похожие, в некотором смысле, на арифметические операции над числами. Для простоты, рассмотрим два подопытных множества, на которых мы будем иллюстрировать наши определения.

$$A_0 = \{1, 3, 4, 7, 15\}, \quad B_0 = \{-8, 3, 7, 15, 23\}.$$

Определение 1.2. *Объединением* множеств A и B (обозначение $A \cup B$[6]) называется множество, состоящие из всех элементов множеств A и B.

Другими словами,

$$A \cup B = \{e \in I\,^7 \colon e \in A \textbf{ или } e \in B\}.$$

Пример 1.3. Для подопытных множеств $A_0 \cup B_0 = \{-8, 1, 3, 4, 7, 15, 23\}$.

Определение 1.3. *Пересечением* множеств A и B (обозначение $A \cap B$[8]) называется множество, состоящее из общих элементов множеств A и B.

Другими словами

$$A \cap B = \{e \in I \colon e \in A \textbf{ и } e \in B\}.$$

Пример 1.4. Для подопытных множеств $A_0 \cap B_0 = \{3, 7, 15\}$.

Определение 1.4. *Разностью* множества A и множества B (обозначение $A \backslash B$[9]) называется множество, состоящее из всех элементов A, которые не являются элементами B.

Другими словами

$$A \backslash B = \{e \in I \colon e \in A \textbf{ и } e \notin B\}.$$

[6] Легко запомнить, если выучить слово **U**nate - (*англ.*) объединять.

[7] Напомним, I – это универсальное множество.

[8] $\cap$ напоминает букву П – **П**ересечение.

[9] Обратите внимание на направление косой линии.

Пример 1.5. Для подопытных множеств $A_0 \backslash B_0 = \{1, 4\}$ и $B_0 \backslash A_0 = \{-8, 23\}$. Заметим, что порядок множеств имеет значение!

Мы уже встречались с операцией разности, когда говорили об иррациональных числах как о всех действительных числах, которые не являются рациональными ($\mathbb{R} \backslash \mathbb{Q}$).

Определение 1.5. *Дополнением* множества A в множестве I (обозначение $\complement A$[10]) называется множество, состоящее из всех элементов I, которые не входят в A.

Другими словами

$$\complement A = \{e \in I \colon e \notin A\}.$$

Пример 1.6. Для подопытных множеств, если $I = \{1, 2, \ldots, 14, 15\}$ – первые 15 натуральных чисел, то $A \subset I$ и $\complement A = \{2, 5, 6, 8, 9, 10, 11, 12, 13, 14\}$.

Операции над множествами удобно визуализировать при помощи *диаграмм (кругов)* **Эйлера(– Венна)**, изображая множества кругами (см. рис. 1.1)[11].

Подробнее о свойствах операций над множествами и использованием диаграмм Эйлера мы поговорим на следующей лекции, а пока рассмотрим некоторые примеры операций с множествами.

1. Если A, B и C – три точки на плоскости, а $SP_{A,B}$, $SP_{B,C}$ – два серединных перпендикуляра (см. пример выше), то $SP_{A,B} \cap SP_{B,C} = \{\mathrm{O}\}$ – одна точка – центр описанной окружности $\triangle ABC$.

2. Если A и B – две бесконечные непараллельные полосы на плоскости, то $A \cap B$ – параллелограмм. Если A, B, C – три полуплоскости, границы которых не параллельны, то $A \cap B \cap C$ – треугольник.

3. Если $A = \{x \in \mathbb{R} \colon x + 1 = 0\}$, $B = \{x \in \mathbb{R} \colon x^2 - 3 = 0\}$ и $C = \{x \in \mathbb{R} \colon (x+1)(x^2-3) = 0\}$, то $C = A \cup B$ (совокупность уравнений). *Что будет для системы уравнений?*.

4. Если $A = \{x \colon f(x)/g(x) = 0\}$, $B = \{x \colon f(x) = 0\}$ и $C = \{x \colon g(x) = 0\}$, то $A = B \backslash C$.

[10] От *англ.* **C**omplement – дополнение.

[11] Отметим, что хоть “круги” есть ограниченные фигуры на плоскости, множества, изображаемые этими кругами, могут быть бесконечны.

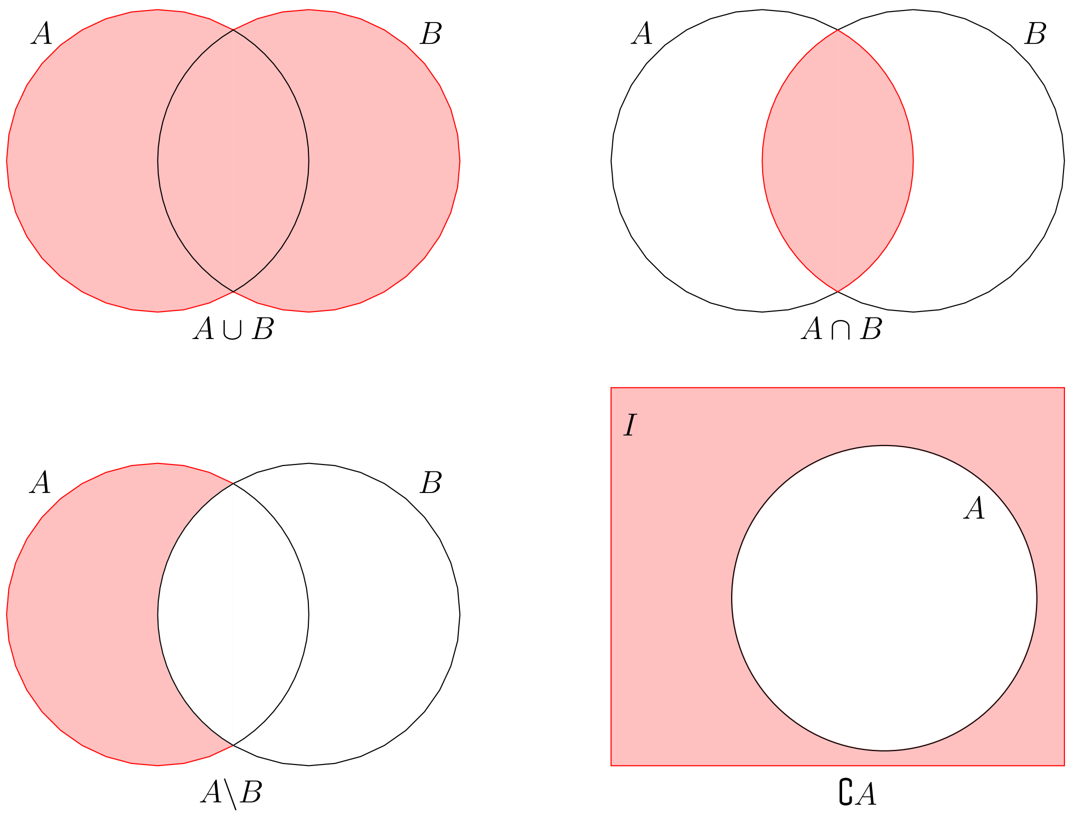

Рис. 1.1: Интерпретация операций над множествами при помощи диаграмм Эйлера. Результат соответствующей операции закрашен цветом.

Список литературы

[1] Н.Я. Виленкин, Рассказы о множествах, МЦНМО, 2005.

[2] Энциклопедия для детей. Т.11. Математика / Глав. ред. М.Д. Аксенова, М.: Аванта+, 1999.

[3] К. Куратовский, А. Мостовский. Теория множеств / Перевод с английского М. И. Кратко под редакцией А. Д. Тайманова. – М.: Мир, 1970.

2 *Лекция 2*

2.1 Доказательство равенства двух множеств

Как мы говорили в прошлой лекции, два множества называются равными, если они состоят из одинаковых элементов. Иначе, это можно сформулировать так:

$$A = B \text{ тогда и только тогда, когда } A \subset B \textbf{ и } B \subset A^{12}$$

$$(A = B \Leftrightarrow A \subset B \textbf{ и } B \subset A)$$

Другими словами, $A = B$ тогда и только тогда, когда *какой бы ни был* элемент $a \in A$, для него верно $a \in B$, и *какой бы ни был* элемент $b \in B$, для него верно $b \in A$.

Рассмотрим два примера, иллюстрирующих схему доказательства равенства множеств:

1. Зададим два множества $E = \{x \in \mathbb{R} \colon \sqrt{3x-2} = x\}$ и $S = \{2, 1\}$. Докажем, что $E = S$.

   Для доказательства, проверим два включения:

$E \subset S$. Действительно, пусть $x \in E$ – *произвольный элемент*[13]. Тогда,

$$\sqrt{3x-2} = x \ \Rightarrow^{14} \ 3x-2 = x^2 \ \Rightarrow \ x^2-3x+2 = 0 \ \Rightarrow x = 2 \text{ или } x = 1.$$

То есть, $x \in S$. Так как x был произвольным элементом, то значит *все* элементы E лежат в S, что и означает $E \subset S$.

$S \subset E$. Это следует из того, что выбирая по очереди 2 и 1 и подставляя в уравнение $\sqrt{3x-2} = x$, мы получим верное равенство. Такая операция вам уже встречалась в школе и называлась она *проверка*.

Из двух включений следует, что $S = L$.

---

[12] Таким образом, для проверки равенства множеств необходимо проверить *два включения*!

[13] Когда мы говорим "произвольный элемент" мы не знаем, какой конкретно элемент из множества нам попадется. Можно считать, что этот элемент дают со стороны, и на его выбор мы влиять не можем. Например, произвольный элемент множества $\{1, 2, 3\}$ – это какое-то из чисел 1, 2 или 3. Нельзя говорить "*возьмем произвольный элемент множества* $\{1, 2, 3\}$*, например,* 2". 2 – это не произвольный, а заданный элемент.

[14] Заметим, что в этом месте мы возводим в квадрат, что может вести к появлению дополнительных корней уравнения (как, например, в уравнении $\sqrt{-x} = x$). В математике говорят, что такой переход не является *равносильным*. Поэтому стрелочка только в одну сторону. Все остальные переходы в этой цепочке, в действительности, равносильны. О логическом следовании и равносильности мы поговорим в одной из последующих лекций.

2. Аналогичная схема работает для доказательства равенств бесконечных множеств. Докажем, что множества $E = \{n \in \mathbb{Z} \colon n \ -\ $ нечетное число$\}$ и $F = \{2k+1 \colon k \in \mathbb{Z}\}$ – равны.

$F \subset E$. Возьмем произвольный элемент из множества F. Он имеет вид $2k+1$ (так как *каждый* элемент F имеет такой вид). Число $2k+1$ не делится на 2 (при целочисленном делении имеем $(2k+1) : 2 = k\,(\text{ост } 1)$), т.е. является нечетным. Значит, $2k+1 \in E$. Так как элемент был выбран произвольно, $F \subset E$.

$E \subset F$. Пусть $n \in E$ – произвольный элемент. Тогда, n – нечетное число. Но тогда $n-1$ – четное число, а значит мы можем записать

$$n = 2 \cdot \frac{n-1}{2} + 1, \text{ где } \frac{n-1}{2} \in \mathbb{Z}.$$

Итого, мы представили n в виде $2k+1$ для некоторого целого k (в частности, $k = \frac{n-1}{2}$). Следовательно, $n \in F$, так как в F лежат *все* числа такого вида. Заключение стандартное: элемент был выбран произвольно, значит $E \subset F$.

Из двух доказанных включений следует равенство $F = E$.

2.2 Свойства операций над множествами

Мы определили четыре базовые операции над множествами: $\cap$, $\cup$, $\setminus$, $\complement$. Посмотрим, какими свойствами они обладают. Начнем с операций объединения и пересечения.

Утверждение 2.1. *Для любых*[15] *множеств A, B, C из I справедливо:*

1. *(коммутативность* = “можно переставлять местами”*)*

$$A \cup B = B \cup A, \qquad A \cap B = B \cap A;$$

2. *(ассоциативность* = “можно не ставить скобки”*)*

$$A \cup (B \cup C) = (A \cup B) \cup C, \qquad A \cap (B \cap C) = (A \cap B) \cap C,$$

а значит имеют смысл выражения $A \cup B \cup C$, $A \cap B \cap C$.

[15]“Любых” значит произвольных. О произвольности см. сноску 13.

3. (дистрибутивность[16] = “правило раскрытия скобок”*)*

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C), \qquad A \cap (B \cup C) = (A \cap B) \cup (A \cap C);$$

*4. (*правила работы с “особыми” множествами*)*

$$A \cup \emptyset = A, \qquad A \cap \emptyset = \emptyset;$$

$$A \cup I = I, \qquad A \cap I = A;$$

Перед тем, как доказывать эти свойства, заметим, что имеют смысл выражения $A \cup B \cup C$, $A \cap B \cap C$, так как ассоциативность операций $\cup$, $\cap$ позволяет не задумываться о порядке выполнения операций.

В тоже время, выражения $A \cap B \cup C$ и $A \cup B \cap C$ без расстановки скобок *однозначного смысла не имеют.* Например, в первой записи не понятно, сначала надо пересечь A и B, и результат объединить с C (то есть найти $(A \cap B) \cup C$), или сперва объединить B и C, а потом пересечь результат с A (т.е. найти $(B \cup C) \cap A = A \cap (B \cup C)$)? Из свойства дистрибутивности следует, что $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, что, *вообще говоря*[17], не равно $(A \cap B) \cup C$.

Доказательство утверждения 2.1. **1.** Свойства коммутативности $\cup, \cap$ следуют из определения соответствующей операции.

2. Докажем ассоциативность $\cup$. Для доказательства ассоциативности операции пересечения надо провести аналогичные рассуждения.

Как мы отмечали в начале лекции, для доказательства равенства множеств необходимо проверить два включения. Пусть $x \in A \cup (B \cup C)$ – произвольный

---

[16]Свойства коммутативности, ассоциативности и дистрибутивности вам уже встречались, когда вы в школе говорили о свойствах операций *сложения* $(+)$ и *умножения* $(\cdot, *)$. Точно так же, как алгебра чисел (алгебра) – это все операции и их свойства, которые связаны с числами, иногда говорят про *алгебру множеств*, так как при работе с множествами выполняются похожие правила.

[17]В математике словосочетание “вообще говоря” относится к ситуациям, когда какое-то свойство, равенство, включение,... может выполнятся, но это происходит не всегда. Например, некорректно утверждать, что *произвольный треугольник не является прямоугольным*, так как может случиться, что наугад выбранный треугольник как раз окажется с углом в 90°. Правильней говорить *произвольный треугольник, вообще говоря, не является прямоугольным*, ведь, скорее всего, наугад выбранный треугольник не окажется прямоугольным. В случае с множествами, $A \cap (B \cup C)$ и $(A \cap B) \cup C$, вообще говоря, различны. Например, для $A = \{1, 2, 3\}$, $B = \{2, 5\}$, $C = \{1, 6\}$ имеем

$$A \cap (B \cup C) = \{1, 2\}, \qquad (A \cap B) \cup C = \{1, 2, 6\}.$$

В тоже время, если в этом примере взять $C = \{1\}$, то множества $A \cap (B \cup C)$ и $(A \cap B) \cup C$ окажутся равными (*проверьте!*).

элемент. Имеем такую логическую цепочку:

$$\begin{aligned}
&x \in A \cup (B \cup C) \Rightarrow [\text{ по определению операции } \cup\,]\, x \in A \text{ или } x \in B \cup C\\
&\ \Rightarrow [\text{ по определению операции } \cup\,]\, x \in A \text{ или } x \in B \text{ или } x \in C\\
&\ \Rightarrow x \in A \cup B \text{ или } x \in C \Rightarrow x \in (A \cup B) \cup C,
\end{aligned}$$

где последние два следования выполняются вновь по определению операции объединения, но прочитанном в *обратном* порядке. Таким образом, $x \in (A \cup B) \cup C$. И так как x был произвольным элементом множества $A \cup (B \cup C)$, то мы получаем $A \cup (B \cup C) \subset (A \cup B) \cup C$. Для доказательства обратного включения, надо вновь взглянуть на цепочку выше и прочитать ее в обратном порядке. Таким образом, $(A\cup B)\cup C \subset A\cup(B\cup C)$. Два включения доказаны, значит $(A \cup B) \cup C = A \cup (B \cup C)$.

3. По прежнему, докажем левую формулу. Правая доказывается по такой же схеме.

Проделаем доказательство равенства $A\cup(B\cap C) = (A\cup B)\cap(A\cup C)$ двумя способами. Начнем с более формального доказательства, как это было при доказательстве ассоциативности выше.

Пусть $x \in A \cup (B \cap C)$ – произвольный элемент. Имеет такая цепочка рассуждений:

$$\begin{aligned}
&x \in A \cup (B \cap C) \Rightarrow [\text{ по определению операции } \cup\,]\, x \in A \text{ или } x \in B \cap C;\\
&\text{если } x \in A \Rightarrow x \in A \cup B \text{ и } x \in A \cup C\ [\text{ в } A \cup B \text{ и в } A \cup C \text{ есть все эл-ты } A\,]\\
&\qquad\qquad \Rightarrow [\text{ по определению операции } \cap\,]\, x \in (A \cup B) \cap (A \cup C);\\
&\text{если } x \in B \cap C \Rightarrow [\text{ по определению операции } \cap\,]\, x \in B \text{ и } x \in C\\
&\qquad\qquad\qquad \Rightarrow\ x \in A \cup B \text{ и } x \in A \cup C\\
&\qquad\qquad\qquad \Rightarrow [\text{ по определению операции } \cap\,]\, x \in (A \cup B) \cap (A \cup C).
\end{aligned}$$

Таким образом, в обоих случаях $x \in (A \cup B) \cap (A \cup C)$. Элемент был выбран произвольно. Значит, $A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C)$.

Докажем включение в обратную сторону. Пусть $y \in (A \cup B) \cap (A \cup C)$ – произвольный элемент. В этом случае, цепочка рассуждений такая:

$$\begin{aligned}
&y \in (A \cup B) \cap (A \cup C) \Rightarrow\ y \in A \cup B \text{ и } y \in A \cup C;\\
&\text{возможны 2 случая: } y \in A \text{ или } y \notin A;\\
&\text{пусть } y \in A \Rightarrow y \in A \cup (B \cap C);\\
&\text{пусть } y \notin A \Rightarrow y \in B \textbf{ и } y \in C\ [\text{ если бы } y \text{ не попадал в какое-то из}\\
&\qquad\qquad\qquad \text{множеств } B \text{ или } C, \text{ то он должен был бы попасть в}\\
&\qquad\qquad\qquad A, \text{ что в этом случае не выполнено }]\\
&\qquad\qquad\qquad \Rightarrow\ y \in B \cap C \Rightarrow\ y \in A \cup (B \cap C).
\end{aligned}$$

Таким образом, в обоих случаях $y \in A \cup (B \cap C)$. В силу произвольности y, имеем включение $(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)$. Два включения доказывают равенство множеств.

Второй, более наглядный, способ доказательства такого рода формул состоит в применении диаграмм Эйлера. Для этого, нужно построить диаграмму Эйлера для множеств, стоящих в правой и левой части предполагаемого равенства, и убедиться, что эти диаграммы совпадают. Проделаем это для множеств $A \cup (B \cap C)$ и $(A \cup B) \cap (A \cup C)$ (см. рис. 2.1).

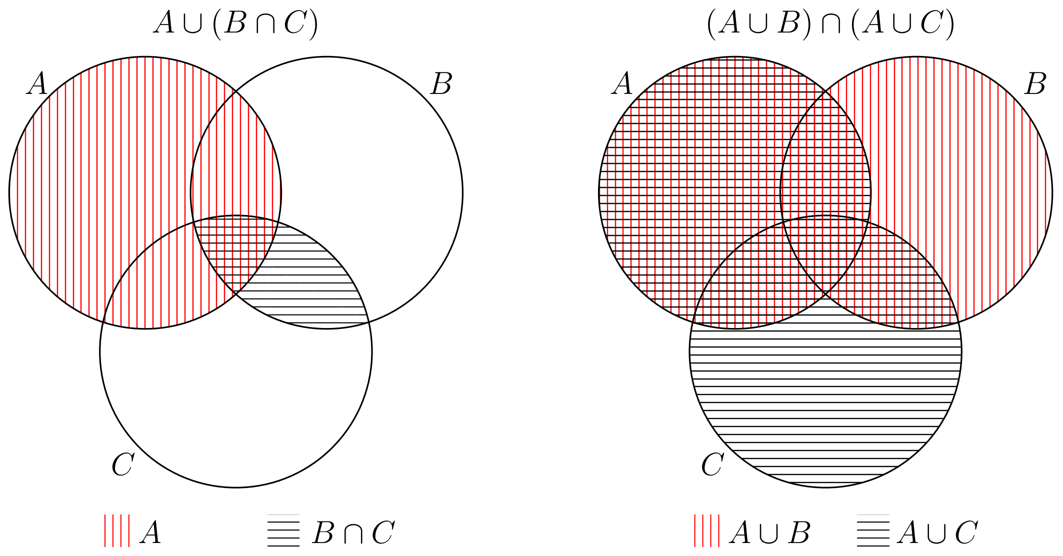

Рис. 2.1: В первом случае, в множестве $A \cup (B \cap C)$ лежат те части на диаграмме, которые содержат хоть какую-то штриховку; во втором случае, в множестве $(A \cup B) \cap (A \cup C)$ лежат только те части диаграммы, которые содержат оба вида штриховки. Как видно, получившиеся множества совпадают, что и доказывает $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

4. Доказательства правил работы с пустым множеством $\emptyset$ и универсальным множеством I следуют из определений этих множеств и операций $\cap$, $\cup$. Например, $A \cup \emptyset$ – по определению, это множество элементов, которые лежат в A или в $\emptyset$. Но т.к. в $\emptyset$ ничего не лежит, остаются только элементы A. Поэтому $A \cup \emptyset = A$. Аналогично в остальных случаях.

□

Как выглядят доказательства всех оставшихся равенств из утверждения 2.1 на языке диаграмм Эйлера, кроме доказанного первого равенства свойства дистрибутивности? Нарисуйте их.

Перейдем к свойствам операции дополнения. Все они сформулированы в следующем утверждении (в котором мы продолжим нумерацию из предыдущего утверждения).

Утверждение 2.2. *Для произвольных множеств A, B из I справедливо:*

5. *(множество и его дополнение)*
$$A \cup \complement A = I, \qquad A \cap \complement A = \emptyset;$$

6. *(дополнения "особых" множеств)*
$$\complement\emptyset = I, \qquad \complement I = \emptyset;$$

7. *(правило двойного дополнения)*
$$\complement\complement A = A;$$

8. *(законы **де Моргана**[18] = дополнения объединений и пересечений)*
$$\complement\,(A \cup B) = \complement A \cap \complement B, \qquad \complement\,(A \cap B) = \complement A \cup \complement B.$$

Доказательство утверждения 2.2. **5.** Докажем первое равенство. Оно следует из того, что если $x \in I$ – произвольный элемент, то либо $x \in A$, либо $x \notin A$. Но во втором случае, по определению дополнения, получаем, что $x \in \complement A$. Таким образом, $x \subset A \cup \complement A$. Элемент был произвольным, значит $I \subset A \cup \complement A$. Обратное включение выполняется всегда, ведь I – универсальное множество. Итого, $A \cup \complement A = I$.

Если еще раз перечитать абзац выше, то можно увидеть, что в нем доказано и второе равенство. Действительно, любой элемент x лежит либо в A, либо в дополнении к A, и не может лежать и там, и там! Значит, $A \cap \complement A = \emptyset$.

6. Следуют из определения операции дополнения.

7. Правило двойного дополнения следует из аккуратного переписывания определения $\complement\complement A$, а именно:
$$\begin{aligned}\complement\complement A &= \{e \in I \colon e \notin \complement A\} = [\text{ т.к. } A \cap \complement A = \emptyset \text{ из } e \notin \complement A \text{ следует } e \in A\ ] \\ &= \{e \in I \colon e \in A\} = A.\end{aligned}$$

8. По традиции, докажем левое равенство. Для произвольного элемента x имеем следующую логическую цепочку, которая справедлива в обе стороны:
$$\begin{aligned}x \in \complement(A \cup B) &\Leftrightarrow x \notin A \cup B \Leftrightarrow x \notin A \textbf{ и } x \notin B \\ &\Leftrightarrow x \in \complement A \textbf{ и } x \in \complement B \Leftrightarrow x \in \complement A \cap \complement B,\end{aligned}$$

---

[18] Названы в честь **Августуса де Моргана** – шотландского математика и логика XIX столетия. Был одним из учителей **Ады Лавлейс** – первой женщины-программиста.

где мы использовали то, что элемент не лежит в объединении множеств, если он не лежит ни в одном, ни в другом множестве. Таким образом, $\complement(A \cup B) = \complement A \cap \complement B$.

Проделаем доказательство этого же равенства на языке диаграмм Эйлера (см. рис. 2.2).

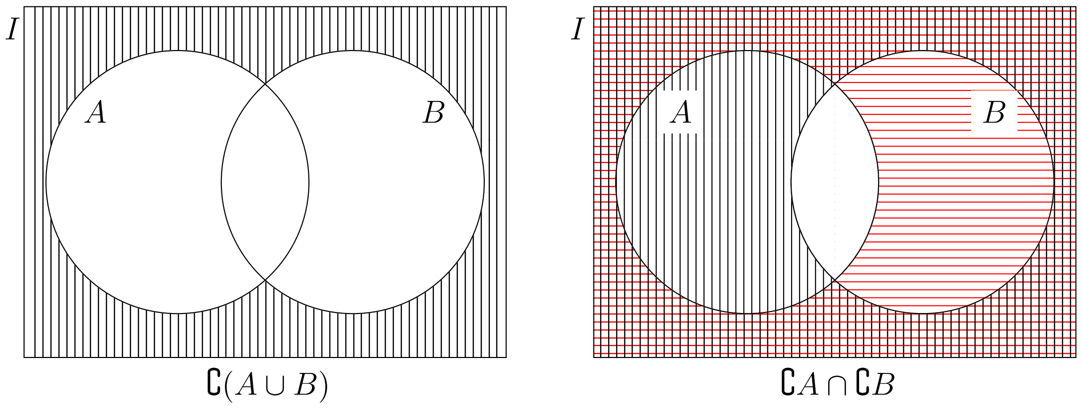

Рис. 2.2: В первом случае заштрихована та часть диаграммы Эйлера, которая не содержит элементов $A \cup B$, то есть $\complement(A \cup B)$; во втором случае горизонтальной (красной) штриховкой обозначено множество $\complement A$ (все без A), вертикальной (черной) штриховкой – множество $\complement B$ (все без B), множество $\complement A \cap \complement B$ есть та часть диаграммы, которая содержит оба типа штриховки. Из диаграмм видно, что $\complement(A \cup B) = \complement A \cap \complement B$.

Доказательство оставшейся формулы де Моргана аналогично только что проделанному. *Проведите его двумя способами!* $\square$

Список литературы

[1] К. Куратовский, А. Мостовский. Теория множеств / Перевод с английского М. И. Кратко под редакцией А. Д. Тайманова. – М.: Мир, 1970.

[2] Р. Курант, Г. Робинс. Что такое математика? – 3-е изд., испр. и доп. – М.: МЦНМО, 2004.

3 *Лекция 3*

3.1 А что с операцией вычитания?

На прошлой лекции мы обсудили правила работы с операциями объединения $\cup$, вычитания $\cap$ и дополнения $\complement$. Но перед этим были введены 4 операции: так что же делать с вычитанием $\setminus$?

Оказывается, эту операцию можно определить через уже упомянутые три операции:

$$A\setminus B = A\cap\left(\complement B\right) \quad \text{или} \quad A\setminus B = \complement\left(\complement A\cup B\right).$$

Доказательство. Действительно, по определению[19]

$$\begin{aligned} x\in A\setminus B &\Leftrightarrow x\in A \text{ и } x\notin B \\ &\Leftrightarrow x\in A \text{ и } x\in\complement B \Leftrightarrow x\in A\cap\complement B. \end{aligned}$$

Значит, $A\setminus B = A\cap\left(\complement B\right)$. Докажем второе равенство:

$$\begin{aligned} x\in A\setminus B &\Leftrightarrow x\in A \text{ и } x\notin B \\ &\Leftrightarrow x\notin\complement A \text{ и } x\notin B \Leftrightarrow x\notin\complement A\cup B \Leftrightarrow x\in\complement\left(\complement A\cup B\right), \end{aligned}$$

значит, $A\setminus B = \complement\left(\complement A\cup B\right)$.

Приведите два доказательства при помощи диаграмм Эйлера.

□

Из-за того, что вычитание множеств можно выполнить, зная только операции объединения, пересечения и дополнения, то все свойства операции вычитания получаются из уже доказанных свойств $\cup, \cap, \setminus$.

Например[20],

$$\begin{aligned} A\setminus(B\cap C) &= A\cap\left(\overline{B\cap C}\right) = A\cap\left(\overline{B}\cup\overline{C}\right) \\ &= \left(A\cap\overline{B}\right)\cup\left(A\cap\overline{C}\right) = (A\setminus B)\cup(A\setminus C). \end{aligned}$$

По аналогии, найдите $A\setminus(B\cup C)$ и докажите соответствующее равенство. А чему равно $\complement\left(A\setminus B\right)$?

Пусть A, B, C – три множества. Имеет ли смысл $A\setminus B\setminus C$?

[19] Заметим, что как и во всех доказательствах, где участвовало только определение, цепочка справедлива в обе стороны.

[20] Иногда, дополнение множества обозначают чертой над множеством:

$$\overline{A} = \complement A.$$

В некоторых выкладках такая запись упрощает изложение, и мы время от времени будем ей пользоваться.

3.2 (*) Пару слов об избыточности операций над множествами

Как мы уже видели, операция вычитания может быть выражена через операции объединения и дополнения, или пересечения или дополнения.

А достаточно ли каких-то **двух** операций, чтобы определить **все** остальные?

Оказывается, достаточно. А именно, зная операции $\cup$ и $\complement$, можно выразить операции $\setminus$ (см. выше) и $\cap$:

$$A \cap B = \complement \left(\complement A \cup \complement B\right).$$

(*проверьте это равенство!*)

Но можно пойти дальше! Определим новую операцию $\star$ следующим образом: для *любых* двух множеств A и B из I

$$A \star B = \{e \in I \colon e \notin A \text{ и } e \notin B\}.$$

Другими словами, на языке "обычных" операций $A \star B = \complement A \cap \complement B = \complement A \cup \complement B$. Но определение выше не подразумевает, что мы знаем "обычные" операции.

Задача 3.1. Пусть $\mathcal{U} \subset 2^I$ – некоторый заданный набор подмножеств I[21]. Известно, что для любых двух множеств $A, B \in \mathcal{U}$, справедливо $A \star B \in \mathcal{U}$. Докажите, что для любых $A, B \in \mathcal{U}$:

1. $A \cup B \in \mathcal{U}$;
2. $A \cap B \in \mathcal{U}$;
3. $A \backslash B \in \mathcal{U}$;
4. $\complement A \in \mathcal{U}$ (дополнение считается в I);
5. $\{\emptyset\} \in \mathcal{U}$, $I \in \mathcal{U}$ [22].

[21] Напомним, что 2^I – это множество всех подмножеств множества I.

[22] Множество называется *замкнутым относительно операции*, если для любых двух элементов из множества, результат выполнения операции над этими элементами также лежит в множестве. Например, множество натуральных чисел $\mathbb{N}$ замкнуто относительно операции сложения $+$, так как сумма натуральных чисел есть натуральное число. В тоже время, $\mathbb{N}$ не замкнуто относительно операции вычитания $-$, например, для натуральных чисел $3, 5$, $3 - 5 \notin \mathbb{N}$. Таким образом в нашей задаче, при выполнении условия $A \star B \in \mathcal{U}$, множество $\mathcal{U}$ оказывается замкнутым относительно стандартных операций.

Таким образом, задача 3.1 показывает, что все стандартные операции над множествами ($\cap$, $\cup$, $\setminus$, $\complement$) могут быть получены посредством **одной** операции $\star$.

Можно ли определить все стандартные операции посредством одной *стандартной операции? Придумайте операцию, отличную от $\star$, при помощи которой можно получить все стандартные операции. Можно ли определить все стандартные операции при помощи $\complement$ и $\cup$? А при помощи $\complement$ и $\setminus$? $\cup$ и $\cap$? $\cap$ и $\setminus$?*

3.3 Мощность множества и формула включений – исключений

Пусть $A \subset I$ – конечное множество.

Определение 3.1. *Мощностью* множества A (обозначение $|A|$[23]) называется количество элементов в A.

Например, для $A = \{1, 5, 8, 2000\}$, $|A| = 4$. В то же время, $|\emptyset| = 0$.

А что такое мощность бесконечного множества? Оказывается, этому понятию можно придать точное значение. Об этом мы поговорим в одной из следующих лекций.

Как узнать мощность объединения множеств, если известны мощности каждого из входящих в объединение множеств? Очевидно, что если два множества A и B *не пересекаются*, то есть $A \cap B = \emptyset$, то

$$|A \cup B| = |A| + |B|.$$

В общем случае справедливо

Утверждение 3.1. *Для любых $A, B \subset I$,*

$$\begin{aligned} |A \cup B| = |A| &+ |B| \\ &- |A \cap B|. \end{aligned}$$

Доказательство. Следует из диаграммы Эйлера. □

А что будет для объединения трех множеств (см. рис. 3.1)?

Утверждение 3.2. *Для любых $A, B, C \subset I$,*

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| \\ &- (|A \cap B| + |A \cap C| + |B \cup C|) \\ &+ |A \cap B \cap C|. \end{aligned}$$

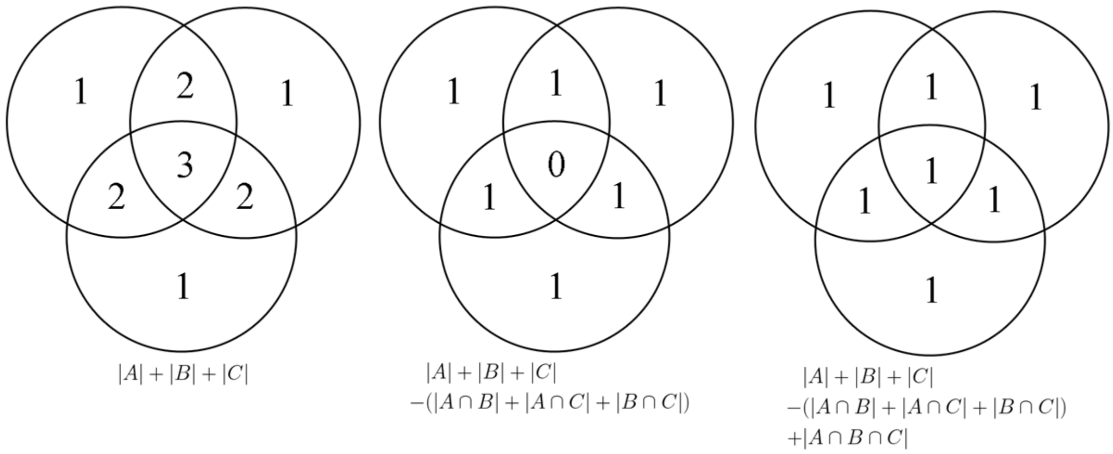

Рис. 3.1: Количество раз, сколько каждый элемент на диаграмме Эйлера учтен в соответствующей сумме.

Доказательство. Смотри рисунок 3.1. $\square$

Формулы утверждений 3.1, 3.2 называются *формулами включений – исключений.* Название обусловлено тем, что для того, чтобы найти количество элементов в объединении надо сначала включить все элементы всех множеств ($|A|+|B|$, $|A|+|B|+|C|$), потом выключить все повторяющиеся элементы в попарных пересечениях ($-|A\cap B|$, $-(|A\cap B|+|A\cap C|+|B\cap C|)$), потом включить неучтенные элементы из пересечений по три, если есть ($|A\cap B\cap C|$) и т.д.

Таким образом получается общий вид формулы включений-исключений для n множеств[24].

Теорема 1 (Формула включений-исключений)**.** [25] *Для произвольных мно-*

[23]Иногда используют обозначение $\sharp A$, но мы не будем этого делать.

[24]Как это принято в математике, когда речь идет о произвольном количестве, это количество обозначают буквой n, считая n произвольным числом. В таком случае, удобней нумеровать множеств, а не называть их разными буквами (не понятно, сколько нужно букв!).

[25]Первая теорема в нашем курсе!

жеств $A_1, A_2, \ldots, A_n \subset I$[26]

$$
\begin{aligned}
\left|\bigcup_{i=1}^{n} A_i\right| = &\sum_{i=1}^{n} |A_i| \\
&- \sum_{i<j}^{n} |A_i \cap A_j| \\
&+ \sum_{i<j<k}^{n} |A_i \cap A_j \cap A_k| \\
&- \ldots \\
&+ (-1)^{n-1} \left|\bigcap_{i=1}^{n} A_i\right|.
\end{aligned}
\tag{3.1}
$$

Что значат все эти значки? Перед тем, как читать доказательство распишите формулу (3.1) для $n = 4$, $n = 5$.

Доказательство. Как и многие утверждения в математике, в которых фигурируют произвольные количества элементов (n штук), мы будем доказывать формулу 3.1 *методом математической индукции (ММИ)*[27].

1) *База*: при $n = 2$ и $n = 3$ формула (3.1) доказана (см. утверждения 3.1, 3.2).

2) *Индукционный переход*: пусть формула (3.1) верна для произвольных $n-1$ множества. Докажем, что она верна для n множеств $A_1, A_2, \ldots, A_n$.

Рассмотрим множества $B_1 = A_1 \cap A_n$, $B_2 = A_2 \cap A_n$ и так далее до $B_{n-1} = A_{n-1} \cap A_n$. Таких множеств $n-1$ штука. Значит, по предположению индукции, для них верна формула включений-исключений. Запишем ее:

$$
\begin{aligned}
\left|\bigcup_{i=1}^{n-1} B_i\right| &= \sum_{i=1}^{n-1} |B_i| - \sum_{i<j}^{n-1} |B_i \cap B_j| + \ldots + (-1)^{n-2} \left|\bigcap_{i=1}^{n-1} B_i\right| \\
&= \sum_{i=1}^{n-1} |A_i \cap A_n| - \sum_{i<j}^{n-1} |A_i \cap A_j \cap A_n| + \ldots + (-1)^{n-2} \left|\bigcap_{i=1}^{n} A_i\right|,
\end{aligned}
\tag{3.2}
$$

где мы подставили выражение множеств B через A и воспользовались ассо-

[26]Такая запись не означает, что у нас три множества. Она означает, что множеств n штук (5, 10, 200, 20000 и т.п.), и вместо точек стоят множества с номерами от 3 до $n-1$. Например, для $n = 100$, в записи $A_1, A_2, \ldots, A_n$ троеточие скрывает 97 множеств с номерами от 3 до 99 включительно.

[27]Это пример утверждения про множества, которых бесперспективно пытаться доказывать при помощи диаграмм Эйлера.

циативностью операции $\cap$. С другой стороны,

$$\left|\bigcup_{i=1}^{n-1} B_i\right| = \left|\bigcup_{i=1}^{n-1} (A_i \cap A_n)\right| = \left|A_n \cap \bigcup_{i=1}^{n-1} A_i\right|, \tag{3.3}$$

по свойству дистрибутивности операций $\cap$ и $\cup$.

Таким образом, из (3.2) и (3.3) мы получаем

$$\left|A_n \cap \bigcup_{i=1}^{n-1} A_i\right| = \sum_{i=1}^{n-1} |A_i \cap A_n| - \sum_{i<j}^{n-1} |A_i \cap A_j \cap A_n| + \ldots + (-1)^{n-2} \left|\bigcap_{i=1}^{n} A_i\right|. \tag{3.4}$$

Заметим, что в правой части формулы выше все пересечения содержат множество A_n. Нам нужны пересечения без A_n. Откуда их взять? Но предположение индукции верно и для $n-1$ множества $A_1, A_2, \ldots, A_{n-1}$. Запишем формулу включений-исключений для них:

$$\left|\bigcup_{i=1}^{n-1} A_i\right| = \sum_{i=1}^{n-1} |A_i| - \sum_{i<j}^{n-1} |A_i \cap A_j| + \ldots + (-1)^{n-2} \left|\bigcap_{i=1}^{n-1} A_i\right|, \tag{3.5}$$

и правой части стоят пересечения без A_n!

Вычтем из равенства (3.5) равенство (3.4). В левой части разности получим:

$$\left|\bigcup_{i=1}^{n-1} A_i\right| - \left|A_n \cap \bigcup_{i=1}^{n-1} A_i\right| = \left|\bigcup_{i=1}^{n} A_i\right| - |A_n|$$

(легко видно из диаграммы Эйлера). В правой части равенства получим (в равенстве (3.5) мы дописали еще одно, третье, слагаемое):

$$\sum_{i=1}^{n-1}|A_i| - \sum_{i<j}^{n-1}|A_i\cap A_j| + \sum_{i<j<k}^{n-1}|A_i\cap A_j\cap A_k| - \ldots + (-1)^{n-2}\left|\bigcap_{i=1}^{n-1}A_i\right|$$

$$-\left(\sum_{i=1}^{n-1}|A_i\cap A_n| - \sum_{i<j}^{n-1}|A_i\cap A_j\cap A_n| + \ldots + (-1)^{n-2}\left|\bigcap_{i=1}^{n}A_i\right|\right)$$

$$= \sum_{i=1}^{n-1}|A_i| - \left(\sum_{i<j}^{n-1}|A_i\cap A_j| + \sum_{i=1}^{n-1}|A_i\cap A_n|\right)$$

$$+\left(\sum_{i<j<k}^{n-1}|A_i\cap A_j\cap A_k| + \sum_{i<j}^{n-1}|A_i\cap A_j\cap A_n|\right) + \ldots +$$

$$+(-1)^{n-1}\left|\bigcap_{i=1}^{n}A_i\right|$$

$$= \sum_{i=1}^{n-1}|A_i| - \sum_{i<j}^{n}|A_i\cap A_j| + \sum_{i<j<k}^{n}|A_i\cap A_j\cap A_k| + \ldots + (-1)^{n-1}\left|\bigcap_{i=1}^{n}A_i\right|.$$

Сопоставляя полученные правую и левую части нашей разности, перенося недостающее слагаемое $|A_n|$ из левой части в правую, получим формулу (3.1). □

3.4 Применение формулы включений-исключений

Формула включений-исключений имеет огромное число различных применений в разных областях математики. Вы еще встретитесь с ней в курсе теории вероятностей. Но мы продемонстрируем ее применение на двух примерах из теории чисел.

0. (Хрестоматийный пример) *В классе 50 школьников, из них 25 – девочки. На "отлично" учатся 30 школьников, из них 16 – девочки. Спортом занимаются 28 учеников, среди которых 18 девочек и 17 отличников. Девочек-отличников, занимающихся спортом, 15 человек. Сколько в этом классе мальчиков, которые учатся плохо и не занимаются спортом?*

   Обозначим через O – множество отличников, D – множество девочек, C – множество спортсменов. Имеем $|D| = 25$, $|O| = 30$, $|C| = 28$, $|O\cap D| = 16$, $|C\cap D| = 18$, $|C\cap O| = 17$, $|D\cap O\cap C| = 15$.

По формуле включений-исключений, $|O\cup D\cup C| = 25+30+28-16-18-17+15 = 47$ – количество людей, которые есть либо отличниками, либо девочками, либо спортсменами. А значит, мальчиков, которые плохо учатся и не занимаются спортом 50 - 47 = 3 человека.

1. *Сколько существует целых чисел от 1 до 500, которые не делятся ни на 3, ни на 5, ни на 11?*

   Эта задача тяжело решается "в лоб". Намного проще найти количество чисел, которые на что-то *делятся*, чем не делятся.

   Пусть $I = \{1, 2, 3, \ldots, 500\}$ – универсальное множество. Обозначим через U_3, U_5 и U_{11} множества тех чисел из I, которые делятся, соответственно, на 3, 5 и 11. Тогда множество $U_3 \cup U_5 \cup U_{11}$ составляют числа, которые делятся на 3, или на 5, или на 11. Значит, искомое количество чисел, которые ни на что не делятся, равно $|I| - |U_3 \cup U_5 \cup U_{11}| = 500 - |U_3 \cup U_5 \cup U_{11}|$.

   Найдем $|U_3 \cup U_5 \cup U_{11}|$ по формуле включений-исключений!

   Сколько чисел в множестве U_3? Это легко – каждое третье число из I делится на 3. Значит, $|U_3| = [500 : 3] = 166$ (целочисленное деление!). Аналогично,

   $$|U_5| = [500 : 5] = 100, \quad |U_{11}| = [500 : 11] = 45.$$

   Множество $U_3 \cap U_5$ составляют числа, которые делятся и на 3, и на 5, т.е. делятся на 15. Значит,

   $$|U_3 \cap U_5| = [500 : 15] = 33.$$

   Аналогично,

   $$|U_3 \cap U_{11}| = [500 : 33] = 15, \quad |U_5 \cap U_{11}| = [500 : 55] = 9.$$

   И наконец, в $U_3 \cap U_5 \cap U_{11}$ лежат числа, которые делятся на 165. Таких в I имеется $[500 : 165] = 3$.

   Таким образом, по формуле включений-исключений:

   $$\begin{aligned} |U_3 \cup U_5 \cup U_{11}| &= |U_3| + |U_5| + |U_{11}| \\ &\quad - (|U_3 \cap U_5| + |U_3 \cap U_{11}| + |U_5 \cap U_{11}|) \\ &\quad + |U_3 \cap U_5 \cap U_{11}| \\ &= 166 + 100 + 45 - (33 + 15 + 9) + 3 = 257. \end{aligned}$$

   Значит, чисел, которые не делятся ни на 3, ни на 5, ни на 11 имеется $500 - 257 = 243$ штуки.

2. *Функция Эйлера* $\varphi(n)$ для натурального числа n определяется как количество чисел от 1 до n, взаимно простых с n.

   Например, $\varphi(4) = 3$, $\varphi(5) = 4$, $\varphi(10) = 4$, $\varphi(20) = 8$, $\varphi(p) = p - 1$, если p – простое число.

   Пусть $n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$ *– разложение числа* n *на различные простые множители. Доказать, что*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_s}\right).$$

   Например, так как $20 = 2^2 \cdot 5$, то $\varphi(20) = 20(1 - 1/2)(1 - 1/5) = 8$, что верно.

   На первый взгляд, задача не имеет отношения к формуле включений исключений. Но, как мы видели в предыдущем примере, количество чисел, которые делятся или не делятся на что-то, удобно считается при помощи формулы включений-исключений.

   Для произвольного индекса $i \in \{1, \dots, s\}$ обозначим через U_{p_i} множество чисел среди первых n натуральных чисел, которые делятся на p_i. Число взаимно просто с n если оно не делится ни на один из простых делителей n. Тогда, как и в предыдущем примере,

$$\varphi(n) = n - \left|\bigcup_{i=1}^{s} U_{p_i}\right|.$$

   В то же время, $|U_{p_i}| = n/p_i$ (заметим, что это целое число), $|U_{p_i} \cap U_{p_j}| = n/(p_i p_j)$, $|U_{p_i} \cap U_{p_j} \cap U_{p_k}| = n/(p_i p_j p_k)$ и т.д. Значит, по формуле включений-исключений,

$$\begin{aligned} \varphi(n) &= n - \sum_{i=1}^{s} \frac{n}{p_i} + \sum_{i<j}^{s} \frac{n}{p_i p_j} - \sum_{i<j<k}^{s} \frac{n}{p_i p_j p_k} \dots + (-1)^s \frac{n}{p_1 p_2 \dots p_s} \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_s}\right). \end{aligned} \tag{3.6}$$

   Как при помощи функции Эйлера и найденной для нее формулы получить ответ примера 1?

Список литературы

[1] К. Куратовский, А. Мостовский. Теория множеств / Перевод с английского М. И. Кратко под редакцией А. Д. Тайманова. – М.: Мир, 1970.

[2] Н.Я. Виленкин, А.Н. Виленкин, П.А. Виленкин. Комбинаторика. – М.: ФИМА, МЦНМО, 2006.

[3] Р. Курант, Г. Робинс. Что такое математика? – 3-е изд., испр. и доп. – М.: МЦНМО, 2004.

4 *Лекция 4*

План лекции[28]:

1. Высказывания: неоднозначность высказываний в обычной жизни, математические высказывания.
2. Логические связки ИЛИ ($\vee$), И ($\wedge$):
   (a) Таблицы истинности (в том числе, для исключающего или (XOR)).
   (b) Примеры.
3. Логическая импликация (следование) ($\Rightarrow$), равносильность ($\Leftrightarrow$):
   (a) Связь с причинно-следственной связью.
   (b) Таблица истинности.
   (c) Примеры.
4. Отрицание ($\neg$):
   (a) Таблица истинности.

Список литературы

[1] K. Devlin, Introduction to Mathematical Thinking, 2012

[2] Энциклопедия для детей. Т.11. Математика / Глав. ред. М.Д. Аксенова, М.: Аванта+, 1999.

[28]Отражает то, что было реально рассказано на лекции.

5 *Лекция 5*

5.1 Еще пару слов о логическом следовании.

В прошлый раз мы определили понятие *логического следования* или *импликации* $A \Rightarrow B$ = “из утверждения A следует утверждение B”. Кроме этого, мы построили следующую таблицу истинности.

A	B	$A \Rightarrow B$
И	И	И
И	**Л**	**Л**
Л	И	И
Л	Л	И

Таким образом, единственный случай, когда импликация целиком ЛОЖНА, если из ИСТИНЫ следует ЛОЖЬ.

Три замечания: почему такая таблица?

1. Первые две строчки совпадают с нашим интуитивным восприятием в случае наличия *причинно-следственной связи*. А что с последними двумя? Пусть есть причинно-следственная связь между A и B. Посмотрим что будет, если импликация НЕ верна. Т.е. “не верно то, что из A следует B”. Когда такое может быть? Когда “A – верно, а B, в тоже время, неверно”. А значит, если A – ЛОЖЬ, то “A – верно, а B, в тоже время, неверно” всегда ЛОЖЬ (союз “а” имеет смысл логической связки И в данном случае). Так как мы смотрели на *отрицание*, то прямое[29] высказывание всегда ИСТИНА, вне зависимости от значений B.

2. Дадим еще одну мотивацию правильности определения таблицы истинности для логического следования. Рассмотрим высказывание A = “Если $4|n$, то $2|n$”. Если ввести два высказывания: $B = 4|n$ (т.е. 4 делит n) и $C = 2|n$ (2 делит n), то высказывание A будет иметь вид $B \Rightarrow C$ и будет, очевидно, истинным для любого значения n. Подставим сюда $n = 5$: тогда B – ложно, C – ложно, но высказывание A *в целом*, по прежнему, истинно. При $n = 6$, B – ложно, но C – истинно, и все высказывание A (по прежнему) истинно. Наконец, при $n = 8$, все утверждения (A, B, C) – истинны. Эти три рассуждения мотивируют 1-ю, 3-ю и 4-ю строки таблицы истинности для $\Rightarrow$. С другой стороны, обратное утверждение (“если $2|n$, то $4|n$”) неверно, и число 2 является контрпримером. При этом, $2|2$, $4 \nmid 2$, и вся импликация “если $2|n$, то $4|n$” – ложна. Это обосновывает 2-ю строчку таблицы истинности для $\Rightarrow$.

[29] Т.е. до отрицания.

3. “Житейский пример”. Хороший пример, помогающий запомнить таблицу истинности для следования, следующий. Пусть есть преподаватель и студент. Преподаватель может говорить “Пиши!” или “Делай, что хочешь!”[30]. Студент может писать или не писать. И тогда логическое следование из того, что говорит преподаватель и что делает студент, это не что иное, как послушание или нет. Сравните следующую таблицу с таблицей истинности для импликации:

Преподаватель	Студент	Послушание
Пиши!	Пишет	(есть) И
Пиши!	**Не пишет**	**(нет) Л**
Делай, что хочешь!	Пишет	(есть) И
Делай, что хочешь!	Не пишет	(есть) И

Вернемся к утверждению о связи отрицания с другими операциями.

Утверждение 5.1. *Для высказываний A и B справедливо:*

1. $\neg(A \vee B) = \neg A \wedge \neg B$ [31]*;*

[30]Заметим, что “Пиши!” и “Делай, что хочешь!” это не высказывания с точки зрения математической логики. В тоже время, приводимая интерпретация действительно помогает запомнить таблицу.

[31]Заметим, что “равенство” высказываний подразумевает, что таблицы истинности для левой и правой частей высказывания совпадают. С другой стороны, для высказываний A и B равенство $A = B$ само по себе является *высказыванием*. Для такого высказывания справедлива таблица истинности (ИСТИНА, когда истинности высказываний A и B равны; иначе – ложь):

A	B	$A = B$
И	И	И
И	Л	Л
Л	И	Л
Л	Л	И

Высказывание $A = B$ это тоже самое, что и высказывание $(A \Leftrightarrow B) = (A \Rightarrow B) \wedge (B \Rightarrow A)$:

A	B	$A \Rightarrow B$	$B \Rightarrow A$	$A \Leftrightarrow B$
И	И	И	И	И
И	Л	Л	И	Л
Л	И	И	Л	Л
Л	Л	И	И	И

Для значка $\Leftrightarrow$ в математике используют выражение *тогда и только тогда*.

2. $\neg(A \wedge B) = \neg A \vee \neg B$ [32]*;*

3. $\neg(A \Rightarrow B) = A \wedge \neg B$*;*

4. $\neg(\neg A) = A$ [33]*.*

Доказательство. Доказательство можно провести двумя способами – рассуждением или при помощи таблиц истинности. [34]

□

Заметим, что из пунктов 2, 3 и 4 выше следует, что $(A \Rightarrow B) = (\neg A \vee B)$. Как это было в теории множеств, логические операции также *не являются* независимыми между собой (см. следующий пункт лекции).

А как связаны оставшиеся операции?

Утверждение 5.2. *Для высказываний A, B и C справедливо:*

(дистрибутивность для $\wedge$ и $\vee$)

1. $(A \wedge (B \vee C)) = ((A \wedge B) \vee (A \wedge C))$ [35]*;*

2. $(A \vee (B \wedge C)) = ((A \vee B) \wedge (A \wedge C))$ [36]*;*

(из сложного высказывание следует)

3. $((A \wedge B) \Rightarrow C) = ((A \Rightarrow C) \vee (B \Rightarrow C))$*;*

4. $((A \vee B) \Rightarrow C) = ((A \Rightarrow C) \wedge (B \Rightarrow C))$ [37]

(сложное высказывание следует из)

5. $(A \Rightarrow (B \wedge C)) = ((A \Rightarrow B) \wedge (A \Rightarrow C))$ [38]*;*

6. $(A \Rightarrow (B \vee C)) = ((A \Rightarrow B) \vee (A \Rightarrow C))$ [39]*.*

---

[32] Пункты 1 и 2 вместе составляют **законы логики де Моргана**, того самого, что и в теории множеств. Через одну лекцию мы обсудим связь множеств и логических операций более подробно.

[33] Закон двойного отрицания.

[34] Тут доказательство опущено, на лекциях приводилось.

[35] “Я пойду на лекцию и буду слушать или играть на телефоне” = “Я пойду на лекцию и буду слушать” или “Я пойду на лекцию и буду играть на телефоне”.

[36] “Я пойду на лекцию или останусь дома и поиграю на телефоне” = “Я пойду на лекцию или останусь дома” и “Я пойду на лекцию или поиграю на телефоне”

[37] Если утверждение “Если $6|n$ или $10|n$, то n – составное число” – верно, то оба утверждения – “Если $6|n$, то n – составное число” и “Если $10|n$, то n – составное число” – также верны. *Что-нибудь похожее в предыдущем пункте?*

[38] $A = ((a \cdot b)|n), B = (a|n), C = (b|n)$.

[39] $A = (a \cdot b = 0), B = (a = 0), C = (b = 0)$.

Доказательство. Доказательство можно провести двумя способами – рассуждением или при помощи таблиц истинности. [40]

□

5.2 Булева логика

Вернемся к замечаниям про импликацию $\Rightarrow$. Добавим еще одно:

4. Если результатом последних двух строк сделать ЛОЖЬ, то получим, что так определенная операция логического следования совпадет с $\wedge$. Как мы это поняли? Совпали таблицы истинности для них. Таким образом, логические операции определяются своей таблицей истинности.

Всего имеется $16 = 2^4$ различных таблиц истинности для возможных операций над двумя высказываниями A и B (*почему?*). Каждая такая таблица задает так называемую *булеву*[41] *функцию* (от двух переменных). Примерами булевых функций являются $\vee$, $\wedge$, $\Rightarrow$, $\Leftarrow$, $\Leftrightarrow$, XOR, $\neg$. Булевы функции принимают значения ИСТИНА или ЛОЖЬ.

Как мы уже говорили, всего существует 16 булевых функций двух аргументов[42]. Две особые функции: *штрих Шеффера* $|$ и *стрелка Пирса* $\downarrow$. Эти две функции задаются таблицами истинности:

A	B	$A\|B$	$A \downarrow B$
И	И	Л	Л
И	Л	И	Л
Л	И	И	Л
Л	Л	И	И

Упражнение 5.1. Покажите, что при помощи *любой* из двух особых операций (штриха Шеффера или стрелки Пирса) можно выразить любую из определенных ранее логических операций.

[40] Тут доказательство опущено, на лекциях приводилось.

[41] Джордж Буль – английский математик

[42] В математике принято обозначать функции как $y = f(x)$ или $z = f(x, y)$. В математической логике такие обозначения не используют. Так $A \wedge B$ уже есть обозначение для булевой функции И. Подставляя различные значения *аргументов* A и B, мы будем получать (используя соответствующую таблицу истинности) значения этой функции. На традиционном "языке" у нас есть функция $f(A, B) = A \wedge B$.

Список литературы

[1] K. Devlin, Introduction to Mathematical Thinking, 2012

[2] Энциклопедия для детей. Т.11. Математика / Глав. ред. М.Д. Аксенова, М.: Аванта+, 1999.

[3] Верещагин Н. К., Шень А., Лекции по математической логике и теории алгоритмов. Часть 2. Языки и исчисления. — 4-е изд., испр. – М.: МЦНМО, 2012. – 240 с.

6 *Лекция 6*

6.1 Кванторы, высказывания с кванторами

В предыдущих лекциях мы говорили о логических высказываниях, то есть предложениях, истинность или ложность которых можно установить однозначно. При этом, пока мы могли однозначно определить ИСТИНУ или ЛОЖЬ, нас не очень заботило, как эти высказывания устроены внутри.

В тоже время, в математике структура самих высказываний очень важна. Большинство теорем[43] – в той или иной перефразировке – устроены одним из следующих образов:

А. *Существует* объект x, который обладает свойством P.

Б. *Для всех* объектов x свойство P выполняется.

Слова *существует* и *для всех* называются (математическими) *кванторами* и обозначаются, соответственно,

$$\exists \quad \text{и} \quad \forall.$$

Сделаем несколько лингвистических замечаний.

1. Квантор $\exists$ называется *квантором существования* (отсюда и обозначение – перевернутая первая буква в Exists – (*англ.*) Существует). Квантор $\forall$ называется *квантором всеобщности* (обозначение – перевернутая первая буква в All – (*англ.*) Все).

2. Само название "квантор" происходит от QUANTify – (*англ.*) определять количество. Таким образом, кванторы показывают, для какого количества объектов выполняется то или иное свойство. Квантор существования показывает, что найдется *как минимум один* такой объект. Квантор всеобщности показывает, что свойство верно *для любого* объекта, какой бы мы только не взяли.

3. Символ $\exists$ может заменять на письме слова "существует", "найдется", "хотя бы один", "как минимум один", "какой-то" и т.д. Все эти словосочетания несут один и тот же логический смысл.

   Символ $\forall$ может заменять слова "для всех", "для любого", "для каждого", "какой бы ни был", "для произвольного", "для всякого" и т.д. Все эти словосочетания логически не отличаются[44].

[43] В рамках этой лекции все математические утверждения, вне зависимости от их степени важности, будут называться теоремами.

[44] Хотя, как гласит известная шутка, *в запорожец может залезть любой, но поместится не каждый.* Это шутка. К курсу отношения не имеет.

Теоремы вида A называются *теоремами существования.* Пример такой теоремы:

Теорема 1: *Уравнение* $x^2 + 2x + 1 = 0$ *имеет вещественное решение.*

Чтобы увидеть структуру вида A, перепишем последнее высказывание в эквивалентном виде:

Теорема 1: *Существует вещественное число* x *такое, что* $x^2 + 2x + 1 = 0$.

Используя обозначения, мы получим:

Теорема 1: $\exists x \in \mathbb{R}\colon x^2 + 2x + 1 = 0.$ [45]

Свойство P, про которое в данном случае идет речь, есть свойство быть корнем уравнения $y^2 + 2y + 1 = 0$. Понятно, что об истинности или ложности P можно судить только зная значение x. Поэтому пишут, что $P(x) = (x^2 + 2x + 1 = 0)$, подразумевая, что $P(x) =$ ИСТИНА, если $x^2 + 2x + 1 = 0$, и $P(x) =$ ЛОЖЬ, если $x^2 + 2x + 1 \neq 0$.

Таким образом, $P(x)$ играет роль логической функции, аргументами которой являются вещественные x, а значениями – **И** или **Л**. В таких обозначениях:

Теорема 1: $\exists x \in \mathbb{R}\colon P(x)$.

(*) Высказывание вида $P(x)$, об истинности которого можно сказать, зная значения x, называется *логическим одноместным предикатом.* Множество, откуда мы можем брать x, называется *предметной областью* для предиката $P(x)$. Предметная область выполняет роль своеобразной "области определения" "функции" $P(x)$.

Приведем несколько примеров:

1. Для предиката в Теореме 1, $P(1) =$ **Л**, $P(-1) =$ **И**.
2. $P(x) = (x > 3)$ – одноместный предикат, выражающий свойство числа быть больше 3, $P(5) =$ **И**, $P(0) =$ **Л**.
3. Если считать предметной областью для предиката $P(x) = (x > 10) \wedge (5 \mid x)$ все натуральные числа, то $P(x)$ выражает свойство числа быть больше 10 и делиться на 5. $P(15) =$ **И**, $P(23) =$ **Л**.

[45] Иногда используют обозначение $\exists x \in \mathbb{R}(x^2 + 2x + 1 = 0)$, а иногда не ставят скобок вообще: $\exists x \in \mathbb{R}\ x^2 + 2x + 1 = 0$. Мы все же советуем ставить двоеточие, заменяющее словосочетание "такой(такие), что".

4. $P(x) = (x -$ фруктовое дерево) – одноместный предикат, предметной областью которого естественно считать все деревья[46]. Тогда P(груша) = **И**, P(клен) = **Л**.
5. $P(x) = (x > y)$ – не предикат, так как по значению x мы не можем сказать, не зная y, верен ли $P(x)$. Тут мы имеем дело с *двухместным предикатом* $P(x, y) = (x > y)$. И тогда $P(2, 3) =$ **Л**, $P(100, 1) =$ **И**.

Аналогично последнему пункту можно определить n-местный предикат. Существует целая теория исчисления предикатов. В нашем курсе мы на ней более подробно останавливаться не будем.

Вернемся к Теореме 1. Верна ли эта теорема и как она доказывается? Очевидно, что верна, и для ее доказательства достаточно предъявить конкретное знание x. Например, $x = -1$. Не все теоремы существования можно доказать явным образом предъявив искомый объект. Например, для

$$\underline{\text{Теорема 2}}\colon \exists x \in \mathbb{R}\colon x^{33} + 3x^{17} + 1 = 0.$$

так сделать нельзя. Тем не менее, Теорема 2 верна, и мы можем ее доказать (*идея непрерывности*). В следующих двух лекциях мы детальней поговорим о разных видах доказательств.

Еще одним примером теоремы существования (теоремы вида А) является (ложное! (*докажите*)) утверждение:

$$\sqrt{2} \text{ – \textit{рациональное число.}}$$

Это действительно теорема существования, так как мы можем переписать ее:

$$\textit{Существуют такие натуральные числа } p \textit{ и } q\textit{, что } \sqrt{2} = p/q.$$

Или, используя обозначения:

$$\exists p \in \mathbb{N}\, \exists q \in \mathbb{N}\colon \sqrt{2} = p/q.^{47}$$

Посмотрим на теоремы (утверждения) вида Б. Аналогично только что рассмотренному случаю А, теоремы вида Б имеют вид

$$\forall x\colon P(x),$$

утверждение $P(x)$ зависит от объекта x. Например, (истинное утверждение)

[46] Расплывчатое понятие "все деревья" показывает, почему не совсем корректно считать предметную область множеством. Но для наших целей это определение вполне подходит.

[47] Имеем двухместный предикат $P(p, q) = (\sqrt{2} = p/q)$.

квадрат любого вещественного числа – неотрицателен

в обозначениях запишется

$$\forall x \in \mathbb{R}\colon x^2 \geqslant 0.$$

В этом примере $P(x) = (x^2 \geqslant 0)$.

Еще один квантор, который часто встречается, это

$$\exists!.$$

(читается “существует и единственный”). Таким образом, высказывание

$$\exists!\, x\colon P(x)$$

означает, что *найдется* ***и*** *ровно один* (существует и единственный) объект x, который обладает свойством $P(x)$.

Этот квантор может быть выражен посредством кванторов существования и единственности. А именно:

$$(\exists!\, x\colon P(x)) = (\exists x\colon P(x) \wedge (\forall y\colon P(y) \Rightarrow x = y)).$$

6.2 Что нельзя делать с кванторами

При использовании кванторов, нужно помнить о нескольких правилах:

1. Большая часть математических утверждений и теорем задействует комбинации кванторов обоих типов. Нужно помнить, **перестановка кванторов, вообще говоря, меняет смысл высказывания!** Например, рассмотрим следующие два высказывания:

   $$\underline{\text{Утв. 1}}\colon \forall m \in \mathbb{N}\ \exists n \in \mathbb{N}\colon n > m.$$
   $$\underline{\text{Утв. 2}}\colon \exists n \in \mathbb{N}\ \forall m \in \mathbb{N}\colon n > m.$$

   Утв. 1 равносильно утверждению о том, что для любого натурального числа (m) можно найти натуральное число (n) большее m. Другими словами, не существует максимального натурального числа. Это, безусловно, верно. Более того, мы всегда можем выбрать $n = m + 1$ (предъявить n явно!)

   В тоже время, Утв. 2 говорит, что я могу найти (подобрать) такое натуральное число (n), что все натуральные числа m будут меньше n. Это (ложное) утверждение о том, что найдется максимальное натуральное число.

Таким образом, порядок кванторов играет существенную роль.

Привести пример такого высказывания с кванторами, что при перестановке этих кванторов смысл высказывания не поменяется.

Что вы можете сказать про следующие два утверждения?

Утв. 3: $\exists m \in \mathbb{N}\ \forall n \in \mathbb{N}\colon n > m.$

Утв. 4: $\forall n \in \mathbb{N}\ \exists m \in \mathbb{N}\colon n > m.$

2. **Кванторы нельзя вносить в "скобки"**. Рассмотрим два примера, которые иллюстрируют, что при внесении смысл может кардинально поменяться:

   Утв. 5 : $\forall x \in \mathbb{N}\colon (2 \mid x) \vee (2 \nmid x).$

   Утв. 6 : $(\forall x \in \mathbb{N}\colon (2 \mid x)) \vee (\forall x \in \mathbb{N}\colon (2 \nmid x)).$

   Утв. 5, очевидно, истинно, а Утв. 6 – ложно.

   Приведите аналогичный пример с квантором существования.

6.3 Отрицания высказываний с кванторами

В предыдущей части лекции мы увидели, что высказывания с кванторами имеют вид

$$\exists x\colon P(x) \quad \text{или} \quad \forall x\colon P(x).$$

Давайте научимся строить отрицания к этим высказываниям.
Начнем с двух примеров:

- $\neg$(*Найдется* студент, который спал этой ночью) $=$ *Все* студенты не спали этой ночью.
- $\neg$(*Все* украинские дороги в ужасном состоянии) $=$ *Есть* как минимум одна дорога в Украине в хорошем состоянии.

Утверждение 6.1. *Отрицания высказываний с кванторами строятся по правилу (*"кванторы заменить на противоположные, предикат заменить на его отрицание"*):*

1. $\neg\,(\exists x\colon P(x)) = (\forall x\colon \neg P(x))$[48];
2. $\neg\,(\forall x\colon P(x)) = (\exists x\colon \neg P(x)).$

[48] Часто используют символ $\nexists$. При таком обозначении, $\nexists x\colon P(x)$ есть тоже самое, что и $\neg\,(\exists x\colon P(x))$. Иногда также пишут $\overline{\exists}$ вместо $\nexists$.

Доказательство. 1. $\neg(\exists x\colon P(x)) \Longrightarrow$ (Неверно, что существует x такой, что он обладает свойством $P(x)$) $\Longrightarrow$ (Для любого x свойство $P(x)$ не выполнятся) $\Longrightarrow$ (Для любого x выполняется $\neg P(x)$) $\Longrightarrow$ $(\forall x\colon \neg P(x))$. И в обратную сторону: $(\forall x\colon \neg P(x)) \Longrightarrow$ (Для всех значений x не выполняется $P(x)$) $\Longrightarrow$ (Неверно, что найдется такой x, что $P(x)$ верно) $\Longrightarrow \neg(\exists x\colon P(x))$. Первый пункт доказан.

Второй пункт доказывается аналогично. □

Пример 6.1. Построим отрицание к тому, что число A есть пределом последовательности a_n. Имеем по определению:

$$\left(\lim_{n\to\infty} a_n = A\right) \Leftrightarrow \forall\varepsilon > 0\ \exists N \in \mathbb{N}\ \forall n > N\colon |a_n - A| < \varepsilon.$$

Тогда (три раза используя утверждение 6.1)

$$\left(\lim_{n\to\infty} a_n \neq A\right) \Leftrightarrow \exists\varepsilon > 0\ \forall N \in \mathbb{N}\ \exists n > N\colon |a_n - A| \geqslant \varepsilon.$$

Список литературы

[1] K. Devlin, Introduction to Mathematical Thinking, 2012

[2] Энциклопедия для детей. Т.11. Математика / Глав. ред. М.Д. Аксенова, М.: Аванта+, 1999.

[3] П.С. Новиков, Элементы математической логики, М.: Наука, 1973, 400 с.

[4] Р.Р. Столл, Множества. Логика. Аксиоматические теории, М.: Просвещение, 1968.

7 *Лекция 7*

7.1 Связь операций над множествами и логических операций

Мы уже не раз замечали, что логические операции над высказываниями и операции над множествами связаны друг с другом каким-то образом. Давайте поймем, каким именно.

Пусть у нас есть одноместный предикат $P(x)$[49], истинный только для значений x из множества A_P[50]. Будем считать, что $A_P \subset I$, где I – некоторое универсальное множество. Таким образом, имеет место истинное высказывание

$$\forall x \in A_P \colon P(x).$$

В тоже время, для произвольного подмножества $A \subset I$, мы можем построить предикат $P(x)$, определенный на универсальном множестве I и такой, что $A = A_P$. Действительно, определим P так:

$$P(x) = \begin{cases} \textbf{И}, \text{ если элемент } x \text{ лежит в множестве } A, \\ \textbf{Л}, \text{ если элемент } x \text{ не лежит в множестве } A. \end{cases}$$

Таким образом, мы получаем взаимно однозначное соответствие между всеми подмножествами I и предикатами, заданными на I.

Имеет место следующее утверждение

Утверждение 7.1. *Пусть $P(x)$ и $Q(x)$ – два предиката, заданных на множестве I.*

1. *Если $R(x) = P(x) \wedge Q(x)$, то $A_R = A_P \cap A_Q$ (связка "и" соответствует операции пересечения).*

2. *Если $R(x) = P(x) \vee Q(x)$, то $A_R = A_P \cup A_Q$ (связка "или" соответствует операции объединения).*

3. *Если $R(x) = \neg P(c)$, то $A_R = \complement A_P$ (отрицание соответствует операции дополнения).*

4. *Если $\forall x \in I \ (P(x) \Rightarrow Q(x))$ – истинное высказывание, то $A_P \subset A_Q$.*

---

[49]То есть высказывание, истинность или ложность которого зависит от значения величины x. При этом природа x, как мы уже отмечали, может быть совершенно произвольной.

[50]Название продиктовано тем, что множество должно зависеть от предиката P. Поэтому мы добавили индекс P.

Доказательство. Непосредственной проверкой. [51]

□

Утверждение дает связь между формулами для операций со множествами и их аналогами – формулами для логических операций.

Упражнение 7.1. 1. Какой логической операции отвечает операция вычитания множеств? 2. Как сформулировать обратное утверждение к утверждению 7.1?

7.2 Математический словарь: необходимые и достаточные условия, равносильность и эквивалентность, обратные и противоположные утверждения

В логической импликации $A \Rightarrow B$, в которой присутствует причинно - следственная связь, A называется *посылкой*, B – *заключением*. Большинство математических утверждений (теорем, лемм,...) имеют такую структуру и состоят из посылки и заключения.

Определение 7.1. Условие A называется *достаточным* для выполнения условия B, если $A \Rightarrow B$ или другими словами, *как только A выполнилось, условие B также становится верным*

Определение 7.2. Условие B называется *необходимым* для выполнения условия A, если $\neg B \Rightarrow \neg A$ или другими словами, *если B* ***не*** *выполняется, то не выполняется и A.*

Так как $(\neg B \Rightarrow \neg A) = (A \Rightarrow B)$ (*проверьте!*), то в импликации с причинно-следственной связью

$$A \Rightarrow B$$

- A – достаточное условие для B;
- B – необходимое условие для A.[52]

Пример: "Если последовательность вещественных чисел имеет конечный предел, то она ограничена". *Что является необходимым, что достаточным условием? Верно ли наоборот?*

Определение 7.3. Утверждение $B \Rightarrow A$ является *обратным* к утверждению $A \Rightarrow B$. В таком случае $A \Rightarrow B$ называется *прямым утверждением.*

[51] Тут доказательство опущено, на лекциях приводилось.

[52] Правило для запоминания ДОН (река): в последовательности $A \Rightarrow B$ идет **ДО**статочное (А достаточно для В), а потом **Н**еобходимое (В необходимо для А) условие.

Пример: *прямая и обратная теорема Пифагора.*

Определение 7.4. Условие A *равносильно (или эквивалентно)* условию B, если $A \Leftrightarrow B$. Другими словами, A равносильно B, если A является необходимым и достаточным условием для B (и наоборот).[53]

Пример: *теорема Пифагора.*

Пример: *три вектора линейно зависимы тогда и только тогда, когда они компланарны.*

7.3 Доказательства, методы доказательств

Что такое доказательство? Рассуждение, которое убеждает нас настолько, что мы готовы убеждать других, используя то же рассуждение. Рассуждение, которое убеждает экспертов.

Классификации доказательств не существует.

Отметим, что для доказательства логического следования $\varphi \Rightarrow \psi$ нужно проверять только выполнение одной из первых двух строк таблицы истинности для импликации. Другими словами, для проверки истинности или ложности $\varphi \Rightarrow \psi$ мы предполагаем, что φ – ИСТИНА. Тогда из первых двух строк таблицы истинности для импликации получим, что истинность/ложность всего следования совпадает с истинностью/ложностью утверждения ψ. Если же φ – ЛОЖЬ, то из двух последних строк таблицы истинности следует, что вся импликация – ИСТИНА, вне зависимости от значений ψ. Таким образом, проверка импликации с точки зрения формальной логики *совпадает* с тем, как мы привыкли доказывать логические следования при наличии причинно-следственной связи.

Какие из следующих утверждений являются истинными, а какие – ложными?[54]

<u>Утв. 0:</u> (x и y – рациональные числа) $\Rightarrow$ ($x + y$ – рациональное число).
<u>Утв. 1:</u> (r и s – иррациональные числа) $\Rightarrow$ ($r + s$ – иррациональное число).
<u>Утв. 2:</u> (r и s – иррациональные числа) $\Rightarrow$ (rs – иррациональное число).
<u>Утв. 3:</u> (r – иррациональное число) $\Rightarrow$ ($\sqrt{r}$ – иррациональное число).
<u>Утв. 4:</u> (r и s – иррациональные числа) $\Rightarrow$ (r^s – иррациональное число).

Последнее утверждение – ЛОЖЬ. Мы докажем это на следующей лекции.

[53] Очень часто в формулировках математических утверждений (теорем, лемм, ...) как раз используют выражение “необходимо и достаточно”. Выражение “тогда и только тогда” означает тоже самое.

[54] На лекции были даны ответы и соответствующие доказательства. Здесь это опущено.

Список литературы

[1] K. Devlin, Introduction to Mathematical Thinking, 2012

[2] Энциклопедия для детей. Т.11. Математика / Глав. ред. М.Д. Аксенова, М.: Аванта+, 1999.

[3] П.С. Новиков, Элементы математической логики, М.: Наука, 1973, 400 с.

8 *Лекция 8*

8.1 Методы и приемы доказательств утверждений

Теорема. *Существуют иррациональные числа r и s такие, что r^s – рационально. Иначе:*

$$\exists r, s \in \mathbb{R}\backslash\mathbb{Q} \colon r^s \in \mathbb{Q}.$$

Доказательство. Рассмотрим два случая, один из которых точно реализуется:

1) Пусть $\sqrt{2}^{\sqrt{2}}$ – рационально. Тогда положим $r = s = \sqrt{2}$, после чего $r^s = \sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$.

2) Пусть $\sqrt{2}^{\sqrt{2}}$ – иррационально. Тогда положим $r = \sqrt{2}^{\sqrt{2}}$, $s = \sqrt{2}$, после чего $r^s = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = 2$.[55] $\square$

8.1.1 Доказательство, используя прием контрапозиции

Прием *контрапозиции* заключается в следующем (*проверьте!*)

$$(\varphi \Rightarrow \psi) = (\neg\psi \Rightarrow \neg\varphi).$$

Другими словами, для доказательство логического следования равносильно доказательству того, что из отрицания заключения следует отрицание посылки.

Пример: утверждение $(\sin\alpha \neq 0) \Rightarrow \forall n \in \mathbb{N} \colon \alpha \neq n\pi$.

Пример: утверждение из геометрии *если в треугольнике никакая медиана и высота не совпадают, то треугольник не равнобедренный.*

8.1.2 Доказательство методом “от противного”

Суть доказательства “*от противного*” заключается в следующем: нужно доказать φ. Предположим $\neg\varphi$. Дальше есть два варианта:

1. Получим одновременно истинными являются ψ и $\neg\psi$, что и даст требуемое противоречие.

   Пример: доказательство иррациональности $\sqrt{2}$.

[55] Заметим, что мы не знаем, какое из допущений верно! Но в обоих случаях мы предъявили два иррациональных числа дающие, после возведение одного в степень другого, рациональное число.

2. Получим, что ($\neg\varphi \Rightarrow$ **Л**) – ИСТИНА. Тогда будет верной импликация $\neg$**Л** $\Rightarrow \varphi$, или **И** $\Rightarrow \varphi$. Прием *modus ponens*

$$((A \wedge (A \Rightarrow B)) \Rightarrow B) \text{ всегда ИСТИНА}$$

(*проверьте!*) дает, что (**И** $\wedge$ (**И** $\Rightarrow \varphi$)) $\Rightarrow \varphi$ – ИСТИНА, а значит φ – истина.

Пример: **Принцип Дирихле**[56]: *Если имеется k клеток и $k+1$ кроликов в этих клетках, то найдется клетка, в которой сидит как минимум 2 кролика.*

Докажем, используя принцип Дирихле следующее утверждение: *Если в клетках таблицы 3x3 расставлены числа 1, 2, 3, то среди сумм по строчкам, столбцам и двум диагоналям как минимум две будут совпадут.*

Доказательство. Имеется 8 сумм, 7 вариантов значений (от минимального $1 + 1 + 1 = 3$ до максимального $3 + 3 + 3 = 9$). Значит, по принципу Дирихле, найдется клетка (значение), в которой сидит как минимум два кролика (сумма). Это и требовалось доказать.[57] □

8.2 Индукция

Индукция – переход от частного к общему.

8.2.1 Полная индукция

Полная индукция, или метод полного перебора, часто встречается доказательствах, где количество возможных состояний объектов (значений) конечно **и** их можно перебрать (вручную или при помощи компьютера).

Пример: Доказать, что среди трехзначных натуральных чисел нет числа, которое можно разделить на 7, 11 и 13.

Полная индукция не всегда работает. Например, до сих пор открытой является гипотеза Гольдбаха[58]: *всякое $n \geqslant 6$ есть сумма трех простых.* Легко проверить справедливость этой гипотезы для первых 100 чисел. **Иван Матвеевич Виноградов** показал, что эта гипотеза верна для всех $n > 3^{3^{15}}$ [59]. Дальше перебирать?? Этот перебор, по сути, неосуществим.

[56] **Петер Густав Дирихле** (1805-1859); в англоязычной литературе называется pingeonhole principle.

[57] Заметим, что это прямое доказательство, а не "от противного".

[58] **Христиан Гольдбах** сформулировал ее в 1742 году.

[59] На сегодняшний день известно, что гипотеза верна для $n > e^{e^{11,5}}$, что в разы лучше оценки Виноградова, но все же невозможно перебрать.

8.2.2 Метод (принцип) математической индукции

Метод математической индукции применяется к доказательству утверждений, зависящих от какого-то натурального числа, т.е. представляющих из себя бесконечный набор случаев (для 1, для 2, для 3...). Например:

Утв. А: Сумма внутренних углов в выпуклом n-угольнике равна $\pi(n-2)$. (утверждение $A(n)$, $n = 3, 4, 5, \ldots$)

Утв. В: n прямых разбивает плоскость не более чем на 2^n частей. (утверждение $B(n)$, $n = 2, 3, 4, \ldots$) [60]

Принцип математической индукции. *Пусть есть набор утверждений $A(n)$, зависящих от номера $n = 1, 2, \ldots$*[61]*. Предположим, что выполнены следующие условия:*

(1) База индукции: *утверждение $A(1)$ – ИСТИНА (верно).*

(2) Индукционный переход $n \rightsquigarrow n+1$: *Если утверждение $A(n)$ – ИСТИНА (верно), то утверждение $A(n+1)$ также ИСТИНА (верно).*

Тогда, для любого $n = 1, 2, \ldots$ утверждения $A(n)$ – ИСТИННЫ (верны).

При помощи принципа математической индукции можно *доказать* утверждения А и В. (доказательства опущены, на лекции приводились.)

Список литературы

[1] K. Devlin, Introduction to Mathematical Thinking, 2012

[2] Энциклопедия для детей. Т.11. Математика / Глав. ред. М.Д. Аксенова, М.: Аванта+, 1999.

[3] П.С. Новиков, Элементы математической логики, М.: Наука, 1973, 400 с.

[60] На лекции утверждения А и В обсуждались и доказывались для начальных значений n.

[61] Заметим, что нумерацию можно начинать с любого натурального числа r. В таком случае, везде ниже все рассуждения, вместо 1, стартуют с r.

9 *Лекция 9*

9.1 Метод математической индукции: доказательство

На прошлой лекции мы сформулировали следующий принцип (метод) математической индукции[62].

Принцип математической индукции. *Пусть есть набор утверждений $A(n)$, зависящих от номера $n = 1, 2, \ldots$*[63]*. Предположим, что выполнены следующие условия:*

(1) База индукции: *утверждение $A(1)$ – ИСТИНА (верно).*

(2) Индукционный переход $n \rightsquigarrow n+1$: *Если утверждение $A(n)$ – ИСТИНА (верно), то утверждение $A(n+1)$ также ИСТИНА (верно).*

Тогда, для любого $n = 1, 2, \ldots$ утверждения $A(n)$ – ИСТИННЫ (верны).

Доказательство основано на следующем принципе:

Принцип наименьшего числа: *В любом непустом подмножестве натуральных чисел есть наименьшее число.* Формально:

$$\forall C \subset \mathbb{N}, C \neq \emptyset, \exists n_0 \in C \, \forall n \in C \colon n_0 \leqslant n.$$

Этот принцип является, по сути, одной из аксиом теории построения натуральных чисел (иногда, его доказывают исходя их других аксиом, например, полноты множества вещественных чисел). Поэтому, мы принимаем его без доказательства.

Доказательство принципа математической индукции. Рассмотрим множество

$$C = \{n \in \mathbb{N} \colon A(n) - \text{ЛОЖЬ}\}.$$

C – множество всех номеров ложных утверждений. Это подмножество натуральных чисел, причем $1 \notin C$ (исходя из базы индукции). По принципу наименьшего числа, в этом множестве есть наименьшее число $n_0 \in \mathbb{N}$, $n_0 \neq 1$. По определению C, утверждение $A(n_0)$ – ЛОЖЬ, а $A(n_0 - 1)$ – ИСТИНА (т.к. $n_0 - 1 \in \mathbb{N}$ и число n_0 – наименьший номер, для которого утверждения $A(n)$ – ложные). В тоже время, по индукционному переходу, если $A(n_0 - 1)$ – ИСТИНА, то и $A(n_0 - 1 + 1) = A(n_0)$ – тоже ИСТИНА. Полученное противоречие доказывает принцип математической индукции.

□

[62] Сокращенно, ММИ.

[63] Заметим, что нумерацию можно начинать с любого натурального числа r. В таком случае, везде ниже все рассуждения, вместо 1, стартуют с r.

Используя принцип математической индукции, нужно всегда тщательно следить за тем, чтобы условия (1) и (2) были действительно выполнены. Иначе можно прийти к абсурду. Приведем несколько "доказательств" методом математической индукции[64]:

Пример 9.1. Утверждение: *Все лошади одного цвета.* Проведём доказательство по индукции.

(1) База индукции: Одна лошадь, очевидно, одного (одинакового) цвета.

(2) Шаг индукции: Пусть доказано, что любые K лошадей всегда одного цвета. Рассмотрим $K+1$ каких-то лошадей. Уберём одну лошадь. Оставшиеся K лошадей одного цвета по предположению индукции. Возвратим убранную лошадь и уберём какую-то другую. Оставшиеся K лошадей снова будут одного цвета. Значит, все $K+1$ лошадей одного цвета.

Отсюда, по принципу математической индукции, следует, что все лошади одного цвета. Утверждение "доказано".

Что не так?

Пример 9.2. Утверждение: $A(n) =$"Если a и b – два таких натуральных числа, что $\max(a, b) = n$, то $a = b$".

(1) База индукции: утверждение $A(1)$ выполняется, так как в таком случае $a = b = n = 1$.

(2) Индукционный переход: Пусть $A(n)$ – верно. Рассмотрим утверждение $A(n+1)$. Введем в рассмотрение два числа $\alpha = a-1$, $\beta = b-1$. $\max(\alpha, \beta) = n$. Следовательно, $\alpha = \beta$, а значит и $a = b$.

По принципу математической индукции, заключаем, что утверждение верно.

Что не так?

Упражнение 9.1. Выведите принцип наименьшего числа из принципа математической индукции, взяв последний в качестве аксиомы.

9.2 Метод наименьшего числа и метод бесконечного спуска

Упражнение 9.2. На плоскости проведено n прямых, $n \geqslant 3$ общего положения (все пересекаются со всеми, и нет трех прямых, проходящих через одну точку). Они делят плоскость на области. Используя принцип наименьшего числа докажите, что среди этих областей есть треугольная.

В основе метода бесконечного спуска лежит следующее утверждение.

[64] Такие, на первый взгляд, верные доказательства утверждений называются *софизмами.*

Утверждение 9.1. *Не существует бесконечной последовательности убывающих натуральных чисел.*

Доказательство. Доказывается, используя принцип наименьшего числа.[65] □

Пример: Диагональ квадрата не соизмерима с его стороной.

Пример: Уравнение $8x^4 + 4y^4 + 2z^4 = t^4$ не имеет целых решений.

Пример: Доказать, что не существует правильного пятиугольника с вершинами в узлах клетчатой бумаги. *Как это сделать для произвольного правильного многоугольника?*

Список литературы

[1] K. Devlin, Introduction to Mathematical Thinking, 2012

[2] Энциклопедия для детей. Т.11. Математика / Глав. ред. М.Д. Аксенова, М.: Аванта+, 1999.

[3] П.С. Новиков, Элементы математической логики, М.: Наука, 1973, 400 с.

[65] Доказательство опущено, на лекциях приводилось.