

ВВЕДЕНИЕ. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Все математические дисциплины можно условно разделить на *дискретные* и *непрерывные*. Дискретная математика – это та часть математики, главной особенностью которой является изучение отдельных объектов, без привлечения понятия непрерывности, т.е. дискретность – это антипод непрерывности. В дискретной математике отсутствует понятие предельного перехода, присущее классической, «непрерывной» математике. Она занимается изучением дискретных структур, которые возникают как внутри математики, так и в ее приложениях. Однако она зародилась в глубокой древности, раньше, чем непрерывная математика, хотя особую значимость приобрела только в последние десятилетия, в связи с повсеместным внедрением в практику информационных технологий.

Таким образом, в широком смысле дискретная математика включает в себя все разделы математики, в которых не используются топологические методы, в частности понятие непрерывности. Это – все разделы алгебры, математическая логика, почти вся теория чисел (в том числе всевозможные компьютерные арифметики), многие разделы экономико-математических методов, комбинаторика и многие другие дисциплины. В более узком смысле дискретная математика – это те разделы математической логики, алгебры, теории чисел и математической кибернетики, которые непосредственно составляют теоретический фундамент информатики. В этом узком смысле дискретная математика включает в себя теорию булевых функций и их минимизацию, теорию графов и многие разделы теоретической кибернетики, теорию автоматов и формальных грамматик, комбинаторику, теорию алгоритмов (в том числе теорию сложности вычислений), криптографию и теорию кодирования.

Некоторые из вышперечисленных разделов имеют не только многочисленные «внутренние» (с точки зрения специалиста по информационным системам или вычислительной техники) приложения, используемые, к примеру, при построении различных дискретных устройств, в программировании и т.д., но их результаты и методы применяются также при решении многих нужных для практики задач. Например, при рассмотрении транспортных задач, для нахождения оптимальных решений в управлении, для выделения «узких мест» при планировании и разработке проектов, при составлении оптимальных расписаний, а также при моделировании сложных технологий и процессов различной природы.

Целью изучения дисциплины является ознакомление студентов с системой понятий и некоторыми наиболее важными в приложениях методами теории множеств, математической логики, теории булевых функций и теории графов. Знания и навыки, полученные при ее изучении, используются в дисциплинах: «Информатика», «Программирование», «Структуры и алгоритмы обработки данных в ЭВМ», «Базы данных», «Экспертные и интеллектуальные системы» и т.д. Но в особенности знания по дискретной математике пригодятся

при изучении дисциплин, связанных с функциональным и логическим программированием, кодированием и защитой информации.

Основная задача состоит в том, чтобы будущие специалисты чётко освоили основные понятия и приёмы работы с булевыми функциями и графами: построение таблиц значений; поиск и исключение фиктивных переменных; приведение булевых функций к стандартной форме (д.н.ф., к.н.ф., многочлен Жегалкина); основные методы минимизации булевых функций; построение диаграммы (рисунка) графа по его матрицам смежности и инцидентности и обратная задача; установление изоморфизма (одинаковости) графов; определение основных характеристик и свойств графов (векторы степеней, планарность, эйлеровость, гамильтоновость и т.п.); изучение важного частного случая графов – деревьев и их свойств.

За недостатком места о приложениях говорится относительно мало. Однако такие примеры содержатся в литературе.

Данное пособие предназначено в основном для изучения основ именно дискретной математики в узком понимании слова, хотя при этом затронуты основополагающие разделы математической логики – исчисление высказываний и исчисление предикатов. Однако математическую логику настоятельно рекомендуется изучать по более фундаментальным источникам, например, [1, 11,15,16,19,23,29]. В то же время, многие разделы дискретной математики в узком смысле слова в данном пособии никак не отражены, в частности, теория кодирования и криптография, теория алгоритмов и теория сложности вычислений. Это связано, в первую очередь, с ограниченностью отводимого времени для изучения дисциплины в учебных планах у студентов, обучающихся информационным технологиям и использованию вычислительной техники. Курс лекций будет также полезен будущим специалистам по прикладной математике, в частности по математическому и компьютерному моделированию.

Пособие – это существенно поработанный и дополненный вариант пособий [20,21].

ЧАСТЬ ПЕРВАЯ. ЭЛЕМЕНТЫ ТЕОРИИ МНОЖЕСТВ И МАТЕМАТИЧЕСКОЙ ЛОГИКИ

Как уже отмечалось выше во «Введении» это пособие не предназначено для глубокого изучения основ математики, в частности математической логики и теории множеств. Тем не менее, изложенного здесь материала по этим разделам математики вполне достаточно для будущих инженеров почти по всем техническим специальностям, в том числе по математическому и компьютерному моделированию.

1 МНОЖЕСТВА. ОПЕРАЦИИ НАД НИМИ. СВОЙСТВА МНОЖЕСТВ

В этом разделе кратко излагается элементарное введение в так называемую *наивную* теорию множеств. «Наивность» здесь означает то, что разрешается объявлять множеством любую совокупность каких угодно объектов. Это вседозволенность может привести к серьёзным недоразумениям, и даже к парадоксам, таким как парадокс Рассела и другие – см. [11,16,23]. С другой стороны столкнуться с подобными неприятностями в практической инженерной деятельности не реально, и на практике вполне достаточно в меру наглядного представления о множествах, которое даёт «наивная теория». Ввиду этого и запредельной сложности аксиоматической теории множеств, последняя теория здесь только упомянута.

1.1 Основные определения

Понятие *множества* является фундаментальным неопределяемым понятием. Интуитивно под множеством понимают любую совокупность вполне определенных различаемых объектов, рассматриваемых как единое целое.

Природа объектов может быть самой различной. Так, можно говорить о множестве стульев в комнате, людей, живущих в каком-то доме, студентов в группе, о множестве натуральных чисел, букв в алфавите, состояний системы и т.п. Множества могут состоять из элементов совершенно разной природы. Например, можно говорить о множестве, включающем в себя одновременно все живые существа, и все предметы и частицы, находящиеся сейчас на поверхности земли и в воде, и в то же время это же множество может содержать и все слова и символы, которые используются людьми.

Но не совсем корректно, например, говорить о множестве капель в стакане воды, так как невозможно четко и ясно указать каждую отдельную каплю, капли нераздельны между собой, когда находятся в одном сосуде. Другое дело – совокупность капель, выпущенных из пульверизатора за определённое время, это уже опять множество, с интуитивной точки зрения.

Отдельные объекты, из которых состоит множество, называются его *элементами*. Для обозначения конкретных множеств принято

использовать прописные буквы A, S, X, \dots . Для обозначения элементов множества будем использовать строчные буквы a, s, x, \dots . Для указания того, что объект x принадлежит множеству X , т.е. что x является элементом множества X , используется запись $x \in X$. Запись $x \notin X$ означает, что объект x не принадлежит множеству X , т.е. x не является элементом X .

Два множества X и Y равны в том и только в том случае, когда они состоят из одних и тех же элементов, т.е. равенство $X = Y$, равносильно двум утверждениям: 1) если $x \in X$, то $x \in Y$ и 2) если $y \in Y$, то $y \in X$.

Множество A называется подмножеством множества B , если любой элемент множества A принадлежит множеству B . Этот факт записывается как $A \subseteq B$ (иногда, когда точно известно, что эти множества различны, это обозначают как $A \subset B$ или $A \subsetneq B$). Сопоставляя определения равных множеств и подмножества нетрудно увидеть, что

$$A = B \Leftrightarrow A \subseteq B \text{ и } B \subseteq A.$$

Это утверждение иногда называют принципом экстенциональности или аксиомой объёмности.

Множество называется конечным, если оно содержит конечное число элементов, и бесконечным, если число его элементов бесконечно.

Если множество конечно, то иногда бывает можно выписать все его элементы: $A = \{a_1, a_2, \dots, a_n\}$. Это один из способов задания множества – перечисление всех его элементов. Он весьма удобен, когда множество относительно небольшое.

Следует различать сам элемент a и множество $\{a\}$, состоящее из одного этого элемента a . Обратите внимание, что при задании множества совершенно неважно в каком порядке и по сколько раз перечисляются его элементы. Например, $\{a, 2, 3, n\} = \{n, a, 2, 3\} = \{2, n, a, a, 2, 3\}$, т.е. множество не следует путать с упорядоченным набором элементов. Такие наборы мы рассмотрим ниже – в разделе 2.

Другой способ задания множества – описательный, он состоит в том, что указывается характерное свойство, которым обладают все элементы множества. Пусть $P(x)$ – какое-то свойство элемента x (какое-то утверждение об элементе x). Тогда запись

$$\{x \mid P(x)\} \quad (\text{или то же самое } \{x : P(x)\})$$

обозначает множество всех тех x , для которых выполняется свойство $P(x)$ (для которых $P(x)$ верно). Так, если M – множество студентов группы, то множество X отличников этой группы записывается в виде $X = \{x \in M \mid x \text{ – отличник}\}$, что читается следующим образом: множество X состоит из (всех) элементов x множества M таких, что x является отличником. Множество простых чисел записывается как $X = \{x : x \text{ – простое число}\}$.

Множество, не содержащее ни одного элемента, называется пустым.

Лемма 1.1 Пустое множество содержится как подмножество во всяком множестве.

Лемма 1.2 *Пустое множество – единственно.*

Поэтому вполне корректно обозначить пустое множество одним символом \emptyset . Например, если M – множество, живущих на Земле кентавров, то

$$M = \{x \in \mathbf{Z} \mid x^2 + 1 = 0\} = \emptyset,$$

где \mathbf{Z} – множество целых чисел. Пустое множество условно относится к конечным множествам.

Упражнение 1.1 *Обоснуйте или докажите леммы 1.1 и 1.2. Указание. Если у Вас возникли затруднения с доказательством, то воспользуйтесь формальным определением импликации в п. 3.2.2.3.*

1.2 Операции над множествами

Над множествами можно производить действия, которые во многом напоминают действия сложения и умножения в элементарной алгебре. Для графической иллюстрации операций над множествами будем использовать так называемые *диаграммы Эйлера-Венна*, в которых произвольному множеству X ставится в соответствие множество точек на плоскости внутри некоторой замкнутой кривой. На рисунке 1.1 слева изображены (условно!) два множества по отдельности, а справа – эти же множества вместе.

1.2.1 *Объединением* (иногда суммой) множеств X и Y называют множество, состоящее из всех тех и только тех элементов, которые принадлежат хотя бы одному из множеств X или Y .

Их объединению на рисунке 1.1 соответствует та часть плоскости, которая заштрихована хотя бы на один раз, т.е. фигура, изображённая на рисунке 1.2 слева. Объединение двух множеств символически записывают как $X \cup Y$. В обозначениях подраздела 1.1 можно записать:

$$X \cup Y = \{a \mid a \in X \text{ или } a \in Y\}.$$

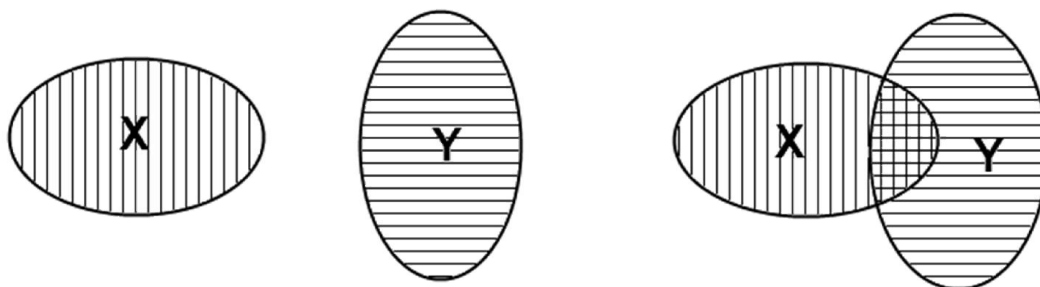


Рисунок. 1.1 – Два множества по отдельности и вместе

Объединение множеств X_i ($i=1,2,\dots,n$) есть множество элементов, каждый из которых принадлежит хотя бы одному из множеств X_i .

Соответствующее обозначение: $\bigcup_{i=1}^n X_i$.

1.2.2 *Пересечением* множеств X и Y называют множество, сос-

тоящее из всех тех и только тех элементов, которые принадлежат как множеству X , так и множеству Y . На рисунке 1.1 пересечению соответствует та часть плоскости, которая заштрихована дважды (в «клеточку»). На рисунке 1.2 эта фигура изображена отдельно (справа). Пересечение множеств обозначается через $X \cap Y$, таким образом,

$$X \cap Y = \{a \mid a \in X \text{ и } a \in Y\}.$$

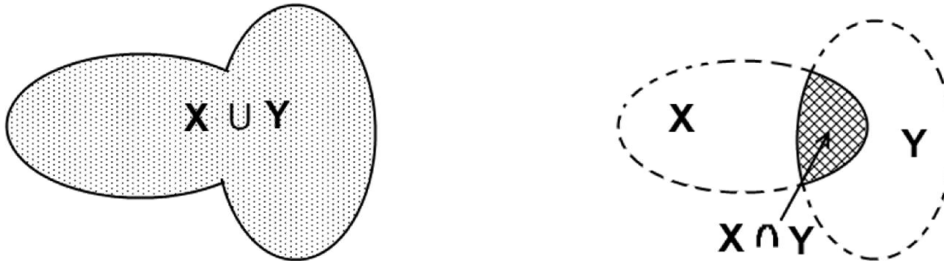


Рисунок 1.2 – Объединение (слева), пересечение (справа)

Множества X и Y называют *непересекающимися*, если они не имеют общих элементов, т.е. если $X \cap Y = \emptyset$.

Пересечением множеств X_i ($i=1,2,\dots,n$) называется множество элементов, принадлежащих всем X_i . Оно обозначается как $\bigcap_{i=1}^n X_i$.

1.2.3 *Разностью* множеств X и Y называют множество, состоящее из всех тех элементов, которые принадлежат X и не принадлежат Y . На рисунке 1.1 этой разности соответствует та часть плоскости, которая заштрихована вертикально, на рисунке 1.3 эта фигура («надкушенная слива») изображена отдельно. Разность множеств обозначается через $X \setminus Y$. Другая форма этого определения:

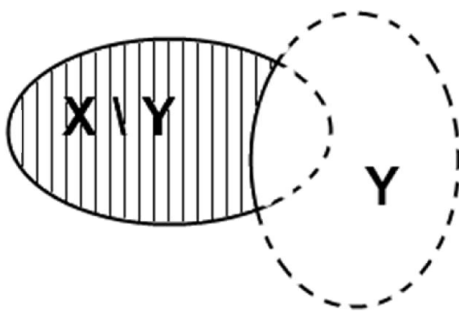


Рисунок 1.3 – Разность множеств X и Y

$$X \setminus Y = \{a \mid a \in X \text{ и } a \notin Y\} = \{a \mid a \in X \text{ и не верно, что } a \in Y\}.$$

1.2.4 *Симметрической разностью* множеств X и Y называют множество, состоящее из всех тех элементов, которые принадлежат в точности одному из множеств и не принадлежат другому. На рисунке 1.1 этой разности соответствует та часть плоскости, которая заштрихована либо только вертикально, либо только горизонтально. На рисунке 1.4 (слева) эта фигура («две слипшиеся надкушенные сливы») изображена отдельно, но уже для других двух множеств – A и B . Симметрическая разность множеств обозначается через $X \div Y$. Другая форма этого определения:

$$X \div Y = \{a \mid \text{либо } a \in X, \text{ либо } a \in Y\} =$$

$\{a \mid a \in X \text{ или } a \in Y \text{ и не верно, что } a \text{ входит в оба множества}\}$.

Пример 1.1 Пусть X – множество отличников в группе, Y – множество студентов, проживающих в общежитии. Тогда $X \cup Y$ – множество студентов, которые учатся на «отлично» или проживают в общежитии; $X \cap Y$ – множество отличников, проживающих в общежитии, $X \setminus Y$ – множество отличников, живущих вне общежития.

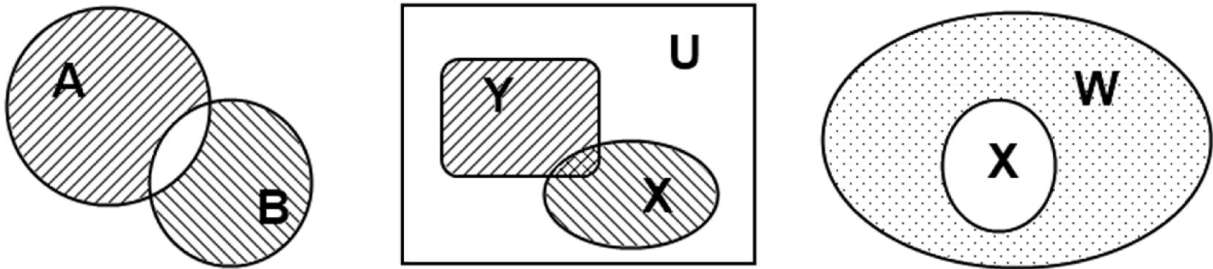


Рисунок 1.4 – Симметрическая разность множеств A и B (слева); универсальное множество U и его подмножества X и Y (в центре); справа – дополнительное к подмножеству X по отношению к множеству W

1.2.5 В некоторых случаях бывает удобно ввести так называемое *универсальное* множество, подмножествами которого являются все остальные множества, рассматриваемые в данной конкретной ситуации. Это множество не всегда однозначно задаётся.

Например, при решении уравнений и неравенств получаются подмножества действительных R или комплексных C чисел, естественно, что здесь в качестве универсального множества удобно взять R или C . В примере 1 на роль универсального годится и множество M всех людей, и множество S всех студентов, а можно ограничиться только множеством S_{EKSTU} – множеством студентов данного ВУЗа или даже множеством студентов в группе.

Универсальное множество удобно изображать на диаграммах Эйлера-Венна в виде множества точек прямоугольника. Отдельные области внутри этого прямоугольника представляют различные подмножества универсального множества – см. рисунок 1.4 (в центре).

Множество \bar{X} , определяемое из соотношения $\bar{X} = U \setminus X$, называют *дополнением* множества X (до универсального множества U). На рисунке 1.4 (по центру) множество \bar{X} представляет собой не закрашенную область и область, включающую в себя почти всё Y (кроме точек из пересечения X и Y).

1.2.6 *Дополнительным* к множеству X по отношению к множеству W , если $X \subset W$, называется множество, состоящее из элементов W , не принадлежащих множеству X . Символически дополнительное множество обозначается как $Z_W(X)$. На рисунке 1.4 (справа) этому множеству соответствует закрашенная часть большого овала.

1.2.7 Если A – множество, то через $P(A)$ обозначается его *множество-степень*, элементами которого являются все подмножества множества A , т.е.

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

Например, 1) $P(\emptyset) = \{\emptyset\}$; 2) если $A = \{0\}$, то $P(A) = \{\emptyset, \{0\}\} = \{\emptyset, A\}$; 3) а если $A = \{0, 1\}$, то $P(A) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\} = \{\emptyset, \{0\}, \{1\}, A\}$.

Упражнение 1.2 Сколько элементов в $P(A)$, если в A : а) 3 элемента; б) 4 элемента; в) 5 элементов; г) n элементов?

Упражнение 1.3 Можно ли в качестве универсального множества взять множество всех множеств? Удобства от такого определения очевидны – этот объект однозначно определён, а какие-нибудь недостатки Вы можете указать?

1.3 Свойства операций над множествами

1.3.1 Основные свойства операций, если существование универсального множества не предполагается, перечислены ниже.

Теорема 1.1 Пусть A, B, C, X, Y, Z – произвольные множества. Тогда имеют место следующие равенства.

1. *Коммутативность пересечения, объединения, симметрической разности:*

$$а) A \cap B = B \cap A; \quad б) A \cup B = B \cup A; \quad в) A \div B = B \div A.$$

2. *Ассоциативность пересечения, объединения, симметрической разности:*

$$а) A \cap (B \cap C) = (A \cap B) \cap C; \quad б) A \cup (B \cup C) = (A \cup B) \cup C; \quad в) A \div (B \div C) = (A \div B) \div C.$$

3. *Дистрибутивность пересечения относительно объединения и симметрической разности:*

$$а) A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \quad б) A \cap (B \div C) = (A \cap B) \div (A \cap C).$$

4. *Дистрибутивность объединения относительно пересечения:*

$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z).$$

5. *Идемпотентность объединения и пересечения:*

$$а) X \cup X = X; \quad б) X \cap X = X.$$

6. *Выражение одной разности через другую:*

$$а) A \div B = (A \setminus B) \cup (B \setminus A) \quad б) A \setminus B = (A \div B) \setminus (B \setminus A) = (A \div B) \cap A.$$

7. *Свойства пустого множества:*

- а) $X \cup \emptyset = X$; – *нейтральность относительно объединения;*
 б) $X \setminus \emptyset = X \div \emptyset = X$ – *нейтральность относительно обеих разностей;*
 в) $X \cap \emptyset = \emptyset$ – *поглощение.*

Доказательство. Свойства 1а), 1б), 5, 6, 7 – очевидны и следуют прямо из определений. Свойство 1в) – следствие 1б) и 6а).

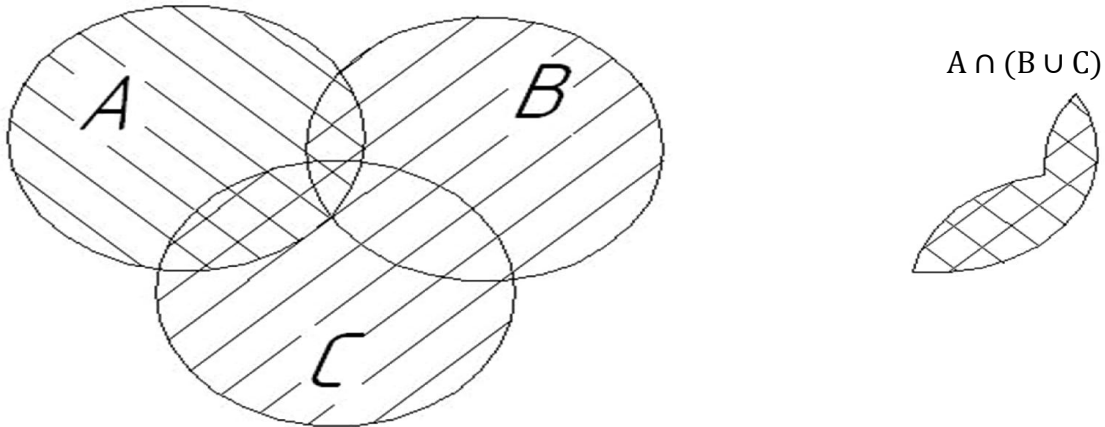


Рисунок 1.5 – Левая часть равенства 3а)

Докажем подробно свойство 3а). Вначале изобразим диаграмму Эйлера-Венна для левой части доказываемого равенства (рисунок 1.5). Затем нарисуем такую диаграмму для правой части (на рисунке 1.6). Видим, что полученные множества совпадают. Но это совпадение – приблизительное (на «глазок»!), поэтому оно ни в коем случае не может считаться строгим доказательством. Для строгого доказательства используем принцип экстенциональности (см. подраздел 1.1). А именно, докажем вначале, что множество в левой части является подмножеством множества правой, а затем наоборот.

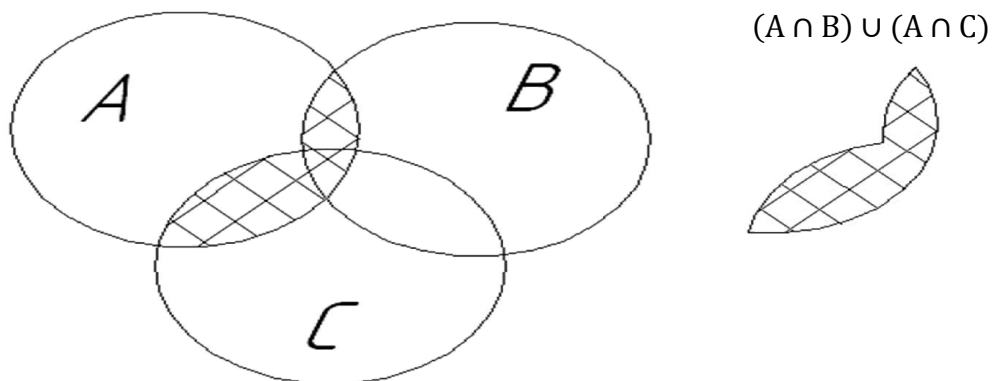


Рисунок 1.6 – Правая часть равенства 3а)

Итак, доказываем $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. При этом используем определение «быть подмножеством»: докажем, что каждый элемент левого множества является также элементом и правого. Пусть x – произвольный элемент множества в левой части, т.е. $x \in A \cap (B \cup C)$. Так как x – элемент пересечения, то по определению пересечения он должен принадлежать каждому множеству, т.е. $x \in A$ и $x \in B \cup C$. Раз $x \in B \cup C$, то по определению объединения $x \in B$ или $x \in C$, т.е. $x \in A$ и ($x \in B$ или $x \in C$). Из последнего сложного утверждения следует, что ($x \in A$ и $x \in B$) или ($x \in A$ и $x \in C$). Отсюда по определению пересечения имеем $x \in A \cap B$ или $x \in A \cap C$. Теперь, по определению объединения получаем: $x \in (A \cap B) \cup (A \cap C)$. А ввиду того, что x

был выбран произвольным элементом левой части, заключаем, что любой элемент левой части входит в правую, т.е. $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ – справедливое соотношение.

Кратко всё это можно записать таким образом:

\subseteq $x \in A \cap (B \cup C) \Rightarrow_1 x \in A$ и $x \in B \cup C \Rightarrow_2 x \in A$ и ($x \in B$ или $x \in C$) \Rightarrow_3 ($x \in A$ и $x \in B$) или ($x \in A$ и $x \in C$) $\Rightarrow_4 x \in A \cap B$ или $x \in A \cap C \Rightarrow_5 x \in (A \cap B) \cup (A \cap C)$; где стрелки № 1,4 справедливы по определению пересечения, стрелки № 2,5 – по определению объединения, а третья – логический закон (см. подраздел 4.2).

Обратное включение – \supseteq), т.е. утверждение о том, что правое множество есть подмножество левого, можно было бы доказать аналогично. Но в данном конкретном случае это можно сделать проще: в приведённом доказательстве все стрелки верны не только слева направо, но и наоборот, т.е. они – двусторонние. Действительно, стрелки № 1,2,4 и 5 – обратимы, так как используются определения, а № 3 – логическая эквивалентность.

Упражнение 1.4 Докажите остальные свойства.

Предостережение. Фокус с обращением всех стрелок проходит не всегда! Бывают необратимыми даже те стрелки, которые используют определения (хотя и редко), а многие логические законы только – односторонние. Поэтому нужно обосновывать обратимость каждой стрелки по отдельности, и если есть сомнения в обратимости хотя бы одной из них, то следует это обратное включение доказывать отдельно.

1.3.2 Возникает естественный вопрос: зачем нужны были рисунки при исследовании свойства 3а), раз они не являются строгим доказательством?

С целью разобраться в этом, рассмотрим следующий

Пример 1.2 Определить верно ли равенство

$$A \setminus (B \cup C) = (A \setminus B) \cup (A \setminus C); \quad (1.1)$$

и если оно не верно, то как его можно исправить. Чтобы понять это, рисуем левую часть равенства (1.1): в левой половине рисунка 1.7 множество A изображено серым, множества B и C – вертикальной штриховкой. Тогда ле-

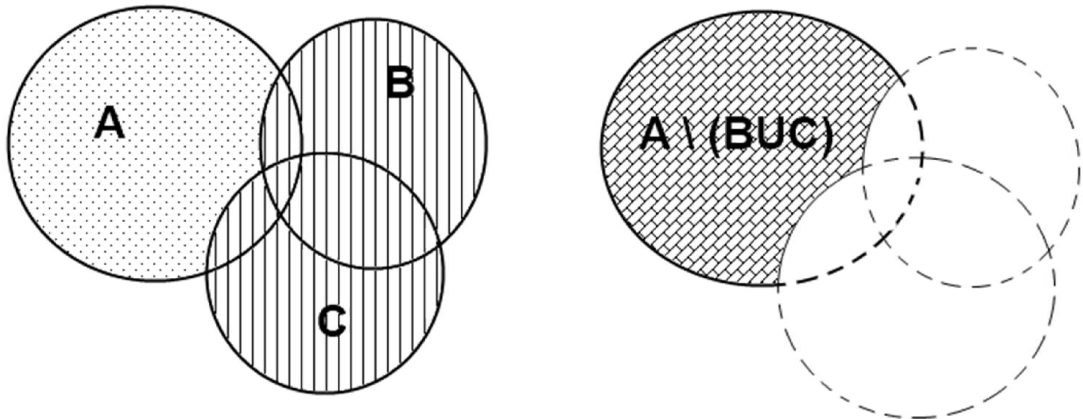


Рисунок 1.7 – Левая часть равенства (1.1)

вая часть, множество $A \setminus (B \cup C)$, это – все те серые точки, которые не стали «полосатыми», т.е. фигура, изображённая в правой половине этого рисунка («дважды откушенная слива»).

Рисуем множество в правой части равенства – правая часть рисунка 1.8.

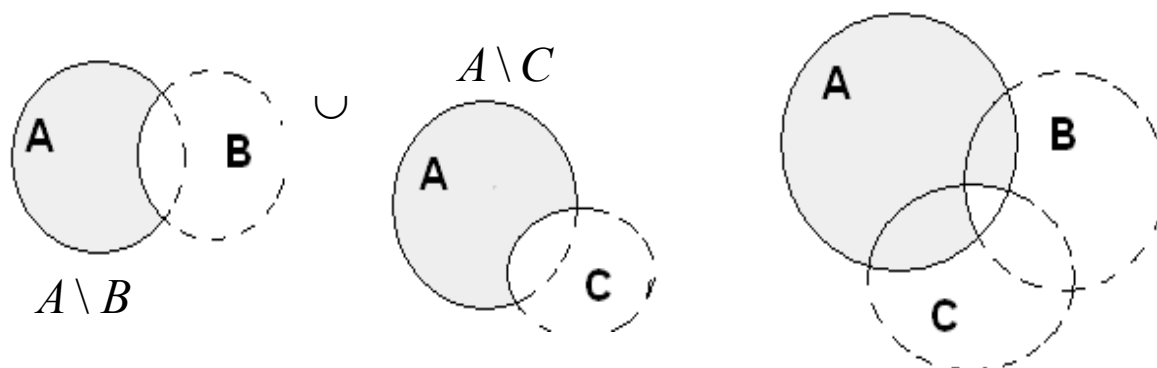


Рисунок 1.8 – Правая часть

Получилась заметно другая фигура, а именно, «клюнутая слива». Но это опять-таки на глазок. Чтобы убедиться в ложности равенства (1.1), строим пример, а рисунки 1.7 и 1.8 нам в этом помогут. Из картинок видно, что равенство будет нарушено, если в A и B имеются такие общие элементы, которых нет во множестве C . Пробуем: $A = \{1, 2, 3, 4\}$, $B = \{3, 4, 5\}$, $C = \{4, 5, 6\}$. Тогда $A \setminus (B \cup C) = \{1, 2, 3, 4\} \setminus \{3, 4, 5, 6\} = \{1, 2\}$, $(A \setminus B) \cup (A \setminus C) = \{1, 2\} \cup \{1, 2, 3\} = \{1, 2, 3\}$, т.е. $A \setminus (B \cup C) \neq (A \setminus B) \cup (A \setminus C)$

На этом примере убеждаемся что, равенство (1) в общем случае неверно. Из рисунков и из приведённого примера можно сделать предположения, что верно включение $A \setminus (B \cup C) \subseteq (A \setminus B) \cup (A \setminus C)$ и равенство $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$ при любых множествах A , B и C .

Упражнение 1.5 Докажите последние утверждения сами.

Упражнение 1.6 Определить какие равенства верны; если какое-то не верно, то как его можно исправить: а) $A \cup (B \setminus C) = (A \cup B) \setminus (A \cup C)$;

б) $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$.

Упражнение 1.7 Коммутативна ли операция разности множеств? А что можно сказать о разности чисел? Всякая ли разность не коммутативна?

1.3.3 Основные свойства операций, при наличии универсального множества U (см. п. 1.2.5). Для любых подмножеств X и Y универсального множества справедливы все соотношения указанные в теореме 1.1, а также следующие:

1. $X \cap \bar{X} = \emptyset$; 2. $X \cup \bar{X} = U$; 3. $\overline{\bar{X}} = X$; 4. $X \setminus Y = X \cap \bar{Y}$; 5. $\overline{X \cup Y} = \bar{X} \cap \bar{Y}$; 6. $\overline{X \cap Y} = \bar{X} \cup \bar{Y}$.

Упражнение 1.8 Докажите эти равенства и нарисуйте диаграммы Эйлера-Венна, соответствующие этим равенствам.