Президентская программа “Дети России”
Министерство общего и профессионального образования
Российской Федерации
Уральский государственный университет
им. А.М. Горького
Специализированный учебно-научный центр

С.А. Ануфриенко

Введение в теорию множеств и комбинаторику

Учебное пособие

Екатеринбург
1998

УДК 510.22(075.3)
А 733

Пособие разработано в рамках федеральной программы “Одаренные дети” по гранту “Развитие российской системы предуниверситетского образования одаренных детей ведущими университетами России” при финансовой поддержке исполнительной дирекции по Президентской программе “Дети России” и Уральского государственного университета им. А.М.Горького

Ануфриенко С.А. Введение в теорию множеств и комбинаторику: Учеб. пособие. Екатеринбург: УрГУ, 1998. 62с.

Рецензенты: канд. физ.-мат. наук **М.И. Альперин**,
науч. сотр. ИММ УрО РАН, канд. физ.-мат. наук **С.Э. Нохрин**

Пособие является элементарным введением в наивную, или канторовскую, теорию множеств. Наряду с традиционными для теории множеств конструкциями представлен единый подход (с помощью продолжений отображений) при доказательстве основных комбинаторных формул. Изложены также некоторые факты о счетных и несчетных множествах, включая теорему Кантора и теорему Кантора–Бернштейна.

Пособие адресовано учащимся и преподавателям лицея, учителям математики, старшеклассникам.

ISBN 5-7996-0015-0

Оглавление

Введение 4

1 Алгебра множеств **5**

1.1 Множество и его элементы. Способы задания множеств 5

1.2 Операции над множествами и их свойства 8

1.3 Декартово произведение множеств. Соответствия 11

2 Введение в комбинаторику **17**

2.1 Конечные множества. Принцип Дирихле 17

2.2 Степень данного множества и его мощность 22

2.3 Отображения конечных множеств. Размещения с повторениями 24

2.4 Взаимно однозначные отображения одного множества в другое. Размещения без повторений. Перестановки 27

2.5 Число сочетаний n-элементного множества по m элементов. Треугольник Паскаля. Бином Ньютона 30

2.6 Перестановки и сочетания с повторениями 34

3 Бесконечные множества **37**

3.1 Счетные множества 37

3.2 Несчетные множества 41

3.3 Теорема Кантора–Бернштейна 45

3.4 Отношения на множестве. Отношения порядка и отношения эквивалентности 49

3.5 Антиномии. Аксиомы теории множеств 58

Введение

Теория множеств — одна из самых молодых математических дисциплин. Ее появление связано с работами немецкого математика Георга Кантора, опубликованными в 1874—1884 годах. Самой значительной из них стала серия, состоящая из шести частей, под общим названием “О бесконечных линейных точечных многообразиях”. В качестве синонима для термина “точечное многообразие” Кантор использует более короткое понятие — “множество”, под которым он понимает “объединение в одно целое хорошо различаемых объектов нашей интуиции или мысли”. Понятие множества оказалось настолько общим и в то же время полезным, что многие сложные конструкции алгебры, геометрии и математического анализа получили ясное теоретико-множественное описание. Это сделало теорию множеств универсальным математическим языком. С другой стороны, математиков давно интересовал вопрос логического обоснования своей науки. Развитие логики в XIX веке и появление теории множеств привело к значительному прогрессу в этих исследованиях. В настоящее время теория множеств — активно развивающаяся область математики.

Первая глава пособия (“Алгебра множеств”) содержит основные способы задания множеств, а также способы конструирования новых множеств из ранее построенных с помощью некоторых операций. Соответствие между множествами, определенное в последнем параграфе этой главы, позволяет устанавливать связи между множествами и сравнивать свойства множеств. Стоит отметить, что частными случаями соответствий являются последовательности и функции в анализе, а также алгебраические операции и геометрические преобразования.

Соответствия будут активно использоваться при изучении конечных множеств. Теорию конечных множеств называют комбинаторикой. Основные комбинаторные формулы, выведенные во второй главе, дают возможность сравнительно легко определять количество элементов множеств, описанных достаточно сложными условиями.

В последней главе изучаются свойства бесконечных множеств, доказываются три теоремы Г.Кантора. В заключение обсуждается вопрос об антиномиях и приводится одна из известных аксиоматических систем теории множеств (система Цермело–Френкеля).

Глава 1

Алгебра множеств

1.1 Множество и его элементы. Способы задания множеств

Во многих математических теориях существуют первоначальные, или неопределяемые, понятия. Причина, по которой невозможно определить абсолютно все понятия, которые мы используем, состоит в следующем. Определяя некоторое понятие через другие, необходимо следить за тем, чтобы это понятие не было определено само через себя. Иначе может возникнуть определение, которое в математике называется "порочным кругом" и считается недопустимым. Вот несколько примеров таких "определений": "ромб — это ромб", "угол имеет величину 90^0, если его стороны перпендикулярны; перпендикулярными прямыми называются прямые, угол между которыми 90^0" и т.д. Каждое определение в математике — это замаскированная цепочка определений, каждое звено которой является переходом к определению более простого понятия. Поскольку замыкать цепь нельзя, то каждый нижний уровень цепи является неопределяемым понятием. Так, давая строгое определение ромба, можно через определение замкнутой простой ломаной и ее звена дойти до двух не определяемых в геометрии понятий — точки и прямой. От первоначальных понятий требуется очень многое: при небольшом количестве они должны обеспечить все многообразие понятий данной математической теории. Все необходимые для этого свойства неопределяемых понятий описываются с помощью системы аксиом. Аксиомы — это утверждения о неопределяемых понятиях, которые мы заранее (т.е. по определению) считаем истинными. Так, по Гильберту, в геометрии существуют три неопределяемых понятия, которые описываются двадцатью аксиомами.

Единственным неопределяемым понятием в теории множеств является понятие множества. В качестве синонимов множеству мы будем использовать "совокупность элементов" или "класс элементов". Смысл множества интуитивно ясен — множество объединяет некоторые, вполне определенные, элементы в одно целое. Трудно найти объекты, которые не являются множествами. Так, эта страница является множеством, состоящим из строк, каждая строка — множество, состоящее из некоторых символов, каждый символ — множество точек на плоскости.

Множества мы будем обозначать большими буквами (A , B , X , Y), его элементы — малыми (a, b, x, y). Тот факт, что a является элементом множества A , будем обозначать $a \in A$ (читается: a принадлежит множеству A). Знак $\in$ был введен итальянским математиком Дж.Пеано и является сокращением греческого слова $\epsilon\sigma\tau\iota$ — "быть". Запись $a \notin A$ означает, что a не является элементом множества A .

Множество полностью определяется своими элементами. Это означает, что множества совпадают в том и только в том случае, когда они состоят из одних и тех же элементов. Символьная запись определения равенства двух множеств такова: $A = B \iff$ (для любого $a \in A \Rightarrow a \in B$ и для любого $b \in B \Rightarrow b \in A$).

Существует два основных способа задания множеств. Для конечных множеств, содержащих небольшое количество элементов, часто просто перечисляют все входящие в него элементы. Так, например, $A = \{a, b, c\}$ — это множество, элементами которого являются только a, b и c .

Самым распространенным является задание множества с помощью некоторого условия $P(a)$, которому удовлетворяют все элементы этого множества и только они. Иными словами, условие $P(a)$ истинно во всех случаях, когда элемент a должен принадлежать определяемому множеству, и ложно для всех элементов, не участвующих в образовании этого множества. Запись $A = \{a : P(a)\}$ означает, что множество A состоит из всех элементов, которые удовлетворяют условию $P(a)$ (знак ":" означает "такие, что"). Например, $N_2 = \{n : n \in N \text{ и существует некоторое } k \in N, \text{ что } n = 2k\}$ — множество всех четных натуральных чисел; множество $R^+ = \{x : x \in R \text{ и } x \geqslant 0\}$ состоит из всех неотрицательных вещественных чисел, $B = \{b : b \text{ является выпуклым четырехугольником}\}$ — множество, состоящее из всех выпуклых четырехугольников, или такое экзотичное множество, как $Y = \{y : y$ – крокодил, обитающий в море Лаптевых $\}$. Для сокращения записи вместо $A = \{a : a \in B \text{ и } P(a)\}$ будем использовать запись $A = \{a \in B : P(a)\}$.

Множества могут являться частью других множеств. Так, множество натуральных чисел N содержится во множестве всех целых чисел Z , последнее — во множестве рациональных чисел Q , и, наконец, множество Q содержится во множестве вещественных чисел R .

Определение. *Множество A содержится во множестве B (обозначается $A \subseteq B$), если каждый элемент множества A является элементом множества B (рис. 1).*

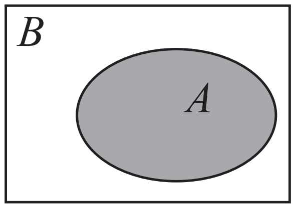

Рис. 1

Попытайтесь доказать следующую простую теорему.

Теорема 1.1.1. *$A = B$ тогда и только тогда, когда одновременно $A \subseteq B$ и $B \subseteq A$ (т.е. $A = B \Longleftrightarrow A \subseteq B$ и $B \subseteq A$).*

Бывают случаи, когда условие $P(a)$ определено таким образом, что нет ни одного элемента, который бы удовлетворял этому условию. Например, $P(a) =$ “ a является четным и одновременно нечетным натуральным числом”. Множество, не содержащее ни одного элемента, обозначается $\varnothing$ и называется пустым множеством. Его можно определить еще и таким образом: $\varnothing = \{x : x$ — множество и $x \neq x\}$. Сделаем одно важное замечание о пустом множестве. Предположим, необходимо доказать, что каждый элемент x данного множества A удовлетворяет некоторому свойству $P'(x)$. В случае, когда множество A не содержит элементов, т.е. является пустым, принято считать, что каждый его элемент удовлетворяет свойству $P'(x)$.

Упражнения

1. Назовите три неопределяемых геометрических понятия.

2. Сколько элементов содержит множество людей, знающих определение множества?

3. Доказать, что $\varnothing$ содержится в любом множестве.

4. Доказать, что пустое множество единственно.

5. Принадлежит ли $\varnothing$ множествам $\{\varnothing, 1\}, \Big\{\{\varnothing\}\Big\}, \Big\{\varnothing, \{\varnothing\}\Big\}$?

6. Равны ли между собой множества $\{\varnothing, 1\}$ и $\{1\}$; $\{\varnothing\}$ и $\varnothing$?

7. Доказать, что $\{y : y$ – крокодил, обитающий в море Лаптевых $\}$ содержится во множестве простых чисел.

8. Еще раз попытайтесь доказать теорему этого параграфа.

9. Доказать, что $\{a, b\} = \{b, a\}$.

10. Доказать, что $\{a, b, c\} = \{a, a, b, b, c, c\}$.

11. Содержится ли множество простых чисел во множестве нечетных чисел?

12. Покажите, что различных бесконечных множеств бесконечно много.

13. Кому принадлежат следующие слова: “Математика полностью свободна в своем развитии, и ее понятия связаны только необходимостью быть непротиворечивыми и согла-

сованными с понятиями, введенными ранее посредством точных определений" (Леонардо да Винчи, Эдгару По, М.В. Ломоносову, Г. Кантору)?

14. Кто из четырех перечисленных выше людей имел математическое образование?

15. Одним из крупнейших специалистов по теории функций в XIX веке был Карл Вейерштрасс (1815—1897). Известно, что Кантор, обучаясь в берлинском университете, слушал лекции Вейерштрасса. Кроме того, именно Вейерштрасс принимал у Кантора докторский экзамен по алгебре и теории функций. Условием этого экзамена было то, что отвечающий должен был давать ответы на вопросы без подготовки. Пришлось ли Кантору подвергаться столь серьезному испытанию и по теории множеств?

16. Действительно ли Г.Кантор родился в Санкт-Петербурге и учился там в начальной школе?

1.2 Операции над множествами и их свойства

Довольно часто новые множества с требуемыми свойствами получаются из ранее построенных с помощью теоретико-множественных операций. Последние имеют своими историческими предшественниками логические операции, свойства которых были хорошо изучены [1] уже к середине XIX века. В этом параграфе изучаются основные теоретико-множественные операции: пересечение, объединение, разность множеств и взятие дополнения.

Определение. *Пересечением множеств A и B (обозначается $A \cap B$) называется множество, состоящее из всех элементов, которые одновременно принадлежат и A, и B. Символьная запись этого определения такова: $A \cap B = \{x : x \in A \text{ и } x \in B\}$.*

Определение. *Объединением множеств A и B (обозначается $A \cup B$) называется множество, состоящее из всех элементов, принадлежащих или A, или B. И соответствующая символьная запись: $A \cup B = \{x : x \in A \text{ или } x \in B\}$.*

Диаграммы Эйлера–Венна, изображенные на рис.1 и 2, являются иллюстрацией для включения множеств, а также операций пересечения и объединения.

Рассмотрим несколько примеров. Если $A = \{1, 2, 3\}$ и $B = \{3, 4\}$, то их пересечением будет множество $A \cap B = \{3\}$, а объединением — $A \cup B = \{1, 2, 3, 4\}$. Пересечение множества, состоящего из всех квадратов плоскости, и множества четырехугольников, не являющихся квадратами, пусто, в то время как их объединение дает множество всех четырехугольников на плоскости.

[1] Заслуга в этом принадлежит английскому математику Дж. Булю (1815—1864).

Решением любой системы уравнений является пересечение решений каждого из входящих в систему уравнений. Пересечение двух различных прямых не может содержать более одной точки, а объединение всегда бесконечно, так как содержит каждую из этих прямых.

Перед тем как определить еще одну операцию над множествами, обсудим понятие универсального множества. Часто рассматривают множества какого-то определенного типа, т.е. все они одновременно содержатся в некотором "большом" множестве. Такое множество, которое содержит все рассматриваемые множества данного типа, называется универсальным для этого типа множеством. Так, для знакомого множества крокодилов моря Лаптевых универсальным множеством является множество всех крокодилов. Для четырехугольников универсальным множеством является плоскость. Для числовых множеств — множество всех вещественных чисел R. Далее универсальное множество будем обозначать через $\mathbf{I}$.

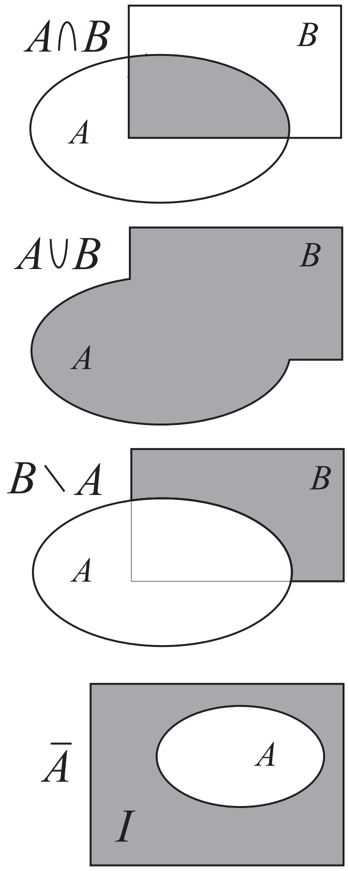

Рис. 2

Определение. *Разностью множеств* B *и* A *(обозначается* $B \backslash A$ *) называется множество, состоящее из всех элементов множества* B *, не принадлежащих множеству* A *(т.е.* $B \backslash A = \{x : x \in B \text{ и } x \notin A\}$ *) (рис. 2).*

Определение. *Дополнением множества* A *(обозначение —* $\overline{A}$ *) называется разность между универсальным множеством* $\mathbf{I}$ *и множеством* A *(т.е.* $\overline{A} = \{x : x \in \mathbf{I} \text{ и } x \notin A\}$ *) (рис. 2).*

Если по-прежнему $A = \{1, 2, 3\}$ и $B = \{3, 4\}$, то $B \backslash A = \{4\}$, а $A \backslash B = \{1, 2\}$. Разностью между множеством натуральных чисел N и множеством всех четных натуральных чисел N_2 является множество всех нечетных натуральных чисел.

Операции объединения и пересечения удовлетворяют следующим свойствам.

Теорема 1.2.1. *Пусть* A, B *и* C *— произвольные множества. Тогда* *справедливы следующие равенства* [2]*:*

1. $A \cup A = A$.	1′. $A \cap A = A$.
2. $A \cup B = B \cup A$.	2′. $A \cap B = B \cap A$.
3. $(A \cup B) \cup C = A \cup (B \cup C)$.	3′. $(A \cap B) \cap C = A \cap (B \cap C)$.
4. $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.	4′. $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

Доказательство. Каждое из этих свойств следует из определения операций и из теоремы 1.1.1. Докажем только 4-е свойство.

Обозначим через X и Y левую и правую части в равенстве 4. Покажем, что оба условия теоремы 1.1.1 выполняются.

1. Докажем сначала, что $X \subseteq Y$. Для этого выберем произвольный элемент $x \in X$. Тогда x одновременно принадлежит $A \cup B$ и C. Из условия $x \in A \cup B$ следует, что $x \in A$ или $x \in B$. Если $x \in A$, то $x \in A \cap C$. Если $x \in B$, то $x \in B \cap C$. Следовательно, в любом случае $x \in A \cap C$ или $x \in B \cap C$. Значит, $x \in Y$.

2. Докажем, что выполняется и обратное включение ($Y \subseteq X$). Возьмем произвольный $y \in Y$, тогда $y \in (A \cap C) \cup (B \cap C) \Rightarrow y \in A \cap C$ или $y \in B \cap C$. Если $y \in A \cap C \Rightarrow y \in A$ и $y \in C \Rightarrow y \in A \cup B$ и $y \in C \Rightarrow y \in (A \cup B) \cap C = X$. Если $y \in B \cap C \Rightarrow y \in B$ и $y \in C \Rightarrow y \in A \cup B$ и $y \in C \Rightarrow y \in (A \cup B) \cap C = X$. Итак, $y \in X$.

Из теоремы 1.1.1 теперь следует, что $X = Y$.

Остальные свойства операций проверяются аналогично.

■

Легко заметить, что операции $\cup$ и $\cap$ обладают некоторой симметричностью. Так, при одновременной замене всех $\cup$ на $\cap$ и всех $\cap$ на $\cup$ каждая из приведенных выше формул останется верной. В следующей теореме доказываются основные свойства разности множеств.

Теорема 1.2.2. *Пусть A и B произвольные множества. Тогда выполняются следующие свойства* [3]*:*

5. $A \cup \varnothing = A$.	5′. $A \cap \varnothing = \varnothing$.
6. $A \cup \mathbf{I} = \mathbf{I}$.	6′. $A \cap \mathbf{I} = A$.
7. $\overline{A \cup B} = \overline{A} \cap \overline{B}$.	7′. $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
8. $\overline{\overline{A}} = A$.	

Доказательство. Свойство 7. Обозначим через X и Y соответственно левую и правую части этого равенства. Покажем, что $X \subseteq Y$ и $Y \subseteq X$.

[2] Свойства 2 и $2'$ называются законом коммутативности операций $\cup$ и $\cap$, 3 и $3'$ — законом ассоциативности, 4 и $4'$ — дистрибутивности.

[3] Свойства 7 и $7'$ называются законами де Моргана.

Для любого $x \in X$ выполняется $x \notin A \cup B \Rightarrow x \notin A$ и $x \notin B \Rightarrow x \in \overline{A}$ и $x \in \overline{B} \Rightarrow x \in Y$. Следовательно, $X \subseteq Y$.

Для любого $y \in Y$ выполняется $y \in \overline{A}$ и $x \in \overline{B} \Rightarrow x \notin A$ и $x \notin B \Rightarrow x \notin A \cup B \Rightarrow x \in X$. Следовательно, $Y \subseteq X$.

Свойство 8. $x \in \overline{\overline{A}} \Leftrightarrow x \notin \overline{A} \Leftrightarrow x \in A$.

■

Упражнения

17. Доказать, что всегда $A \cap B \subseteq A \cup B$. В каком случае $A \cup B \subseteq A \cap B$?

18. Известно, что $\{a, b\} \subseteq \{c\}$. Что можно сказать об элементах этих множеств?

19. В каком случае $A \cup B = A \cap B$? Описать все такие случаи.

20. Доказать, что выполняется $A \backslash B = A \backslash (A \cap B)$.

21. В чем сходство и различие свойств операций над множествами $\cup, \cap, \backslash$ и операций над числами $+, \cdot, -$. Найти четыре сходства и два различия.

22. Докажите, что следующие условия эквивалентны:

$$A \subseteq B, \qquad A \cap B = A, \qquad A \cup B = B,$$
$$I \backslash B \subseteq I \backslash A, \qquad A \cap (I \backslash B) = \varnothing, \qquad (I \backslash A) \cup B = I.$$

23. Докажите, что для любых двух множеств A и B выполняется

$$B \backslash (B \backslash A) = B \cap A.$$

24. Правда ли, что теоремы 1.2.1, 1.2.2 были доказаны непальским математиком Дж. Булем (1815—1864)?

25. Дано n множеств. Попытаться доказать, что с помощью операций $\cup, \cap, \backslash$ можно получить конечное число различных множеств.

1.3 Декартово произведение множеств. Соответствия

В 1637 году вышел философский трактат “Рассуждение о методе” французского философа и математика Рене Декарта (1596—1650). Последняя часть этой работы была посвящена новому геометрическому методу — методу координат. Каждой точке плоскости Декарт поставил в соответствие упорядоченную пару вещественных чисел — ее первую и вторую координаты. При этом многие геометрические фигуры стали описываться с помощью алгебраических уравнений. Координаты каждой точки данной фигуры удовлетворяли соответствующему уравнению, координаты всех остальных точек плоскости не удовлетворяли этому уравнению. Таким образом, многие геометрические задачи были переведены на алгебраический язык и были решены алгебраическими средствами. Эта часть математики, которая возникла на границе геометрии и алгебры, стала называться аналитической геометрией.

Рассмотренное Декартом множество всех упорядоченных пар вещественных чисел является примером произведения множества на себя. Для определения произведения множеств в общем случае необходимо понятие упорядоченной пары. Пусть A и B — произвольные непустые множества и $a \in A$, $b \in B$. Заметим сразу, что множества [4] $\{a, b\}$ и $\{b, a\}$ равны между собой и поэтому не дают возможности определить, какой из двух элементов пары является первым, а какой — вторым. Последнее важно, так как, например, точки с координатами $(1, 2)$ и $(2, 1)$ различны, в то время как множества $\{1, 2\}$ и $\{2, 1\}$ совпадают. Существует несколько определений упорядоченной пары (a, b), одно из них принадлежит Н.Винеру и К.Куратовскому.

Определение. *Пусть* $a \in A, b \in B$. *Упорядоченной парой* (a, b) *называется множество* $\Big\{\{a\}, \{a, b\}\Big\}$, *при этом* a *называется первым элементом упорядоченной пары, а* b *— вторым.*

Теорема 1.3.1. $(a, b) = (c, d) \Leftrightarrow a = c$ *и* $b = d$.

Доказательство. $\Leftarrow$). Очевидно.

$\Rightarrow$). Пусть $\Big\{\{a\}, \{a, b\}\Big\} = \Big\{\{c\}, \{c, d\}\Big\}$.

1-й случай. $a = b$. Тогда $\{\{a\}, \{a, b\}\} = \{\{a\}\} = \{\{c\}, \{c, d\}\}$. Следовательно, $\{a\} = \{c\} = \{c, d\} \Rightarrow a = c = d$.

2-й случай. $a \neq b$. Из равенства множеств получаем, что $\{a\} \in \Big\{\{c\}, \{c, d\}\Big\}$ $\Rightarrow \{a\} = \{c\}$ или $\{a\} = \{c, d\}$.

а) $\{a\} = \{c\}$. Поэтому $a = c$ и $\Big\{\{a\}, \{a, b\}\Big\} = \Big\{\{a\}, \{a, d\}\Big\}$. Заметим, что $\{a, b\} \neq \{a\}$, иначе $a = b$. Следовательно, $\{a, b\} = \{a, d\} \Rightarrow b = d$.

б) $\{a\} = \{c, d\} \Rightarrow c = d = a \Rightarrow \Big\{\{a\}, \{a, b\}\Big\} = \Big\{\{c\}\Big\} \Rightarrow \{a, b\} = \{a\} \Rightarrow a = b$. Противоречие.

■

Итак, запись (a, b) означает, что пара образована двумя элементами a и b, причем a является первым элементом этой пары. В предыдущей теореме доказано основное свойство упорядоченных пар: две упорядоченные пары совпадают тогда и только тогда, когда совпадают их первые элементы и вторые элементы также равны между собой. Это, в частности, означает, что $(a, b) = (b, a)$ только в исключительном случае: когда $a = b$.

Определение. *Произведением двух множеств* A *и* B *называют множество* $A \times B$, *состоящее из всех упорядоченных пар, первые элементы которых выбираются из* A, *вторые — из* B *(т.е.* $A \times B = \{(a, b) : a \in A,\ b \in B\}$ *).*

На рис. 3 изображено произведение множеств $A = \{1, 2, 3\}$ и $B = \{a, b\}$.

[4] Множество $\{a, b\} = \{b, a\}$ называется неупорядоченной парой.

Произведение двух множеств A и B часто называют декартовым произведением. Заметим, что множества A и B не обязаны быть различными, в случае их совпадения множество $A \times A$ обозначают через A^2 и называют квадратом (декартовым квадратом) множества A. Так, например, R^2 — декартова плоскость, Z^2 — ее подмножество, состоящее из всех точек с целочисленными координатами.

Заметим, что часто $A \times B \neq B \times A$. Так, $(1,-2) \in N \times Z$, но $(1,-2) \notin Z \times N$.

Теорема 1.3.2. *Пусть A, B и C — произвольные множества, тогда выполняются следующие свойства:*

1. $(A \cup B) \times C = (A \times C) \cup (B \times C)$,

1′. $(A \cap B) \times C = (A \times C) \cap (B \times C)$.

Доказательство. Обозначим через X и Y левую и правую части равенства 1.

Если $x \in X \Rightarrow x = (d, c)$, где $d \in A \cup B, c \in C$. Если $d \in A \Rightarrow x \in A \times C$. Аналогично, если $d \in B \Rightarrow x \in B \times C$. Следовательно, $X \subseteq Y$.

Так как $A \times C$ и $B \times C$ содержатся в X, то $Y \subseteq X$.

По теореме 1.1.1 множества X и Y совпадают.

Свойство $1'$ доказывается аналогично.

■

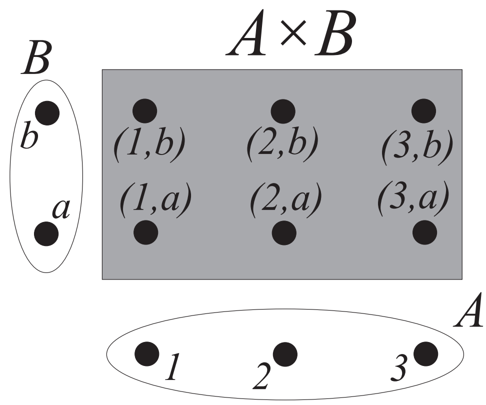

Рис. 3

Ниже обсудим понятие соответствия.

Определение. *Соответствием φ между множествами A и B называется произвольное подмножество их произведения $A \times B$ (т.е. $\varphi \subseteq A \times B$)* [5].

Итак, соответствие состоит из упорядоченных пар. Каждая пара $(a, b) \in \varphi$ указывает, что элементу $a \in A$ соответствует элемент $b \in B$ при данном соответствии φ.

Иногда соответствие удобно изображать с помощью стрелок, начало которых указывает первый элемент упорядоченных пар, конец — второй элемент. Так, рис. 4 является изображением для следующего соответствия:

$$\varphi = \{(1, b),\ (3, a),\ (3, c),\ (4, b)\}.$$

Заметим, что некоторым элементам из A может соответствовать несколько элементов множества B, а некоторым элементам из A может не соответствовать ни один элемент множества B.

Определение. *Областью определения соответствия φ называется множество $Dom\,\varphi = \{a \in A :$ существует элемент $b \in B$, что $(a, b) \in \varphi\}$ (т.е.*

[5] Греческие буквы φ, ψ, χ читаются соответственно “фи”,“пси”,“хи”.

это все элементы из A, которым соответствует хотя бы один элемент из B).

Определение. *Множеством значений соответствия φ называют множество $Im\,\varphi = \{b \in B :$ существует элемент $a \in A$, что $(a,b) \in \varphi\}$ (т.е. это все элементы из B, которые соответствуют хотя бы одному элементу из A).*

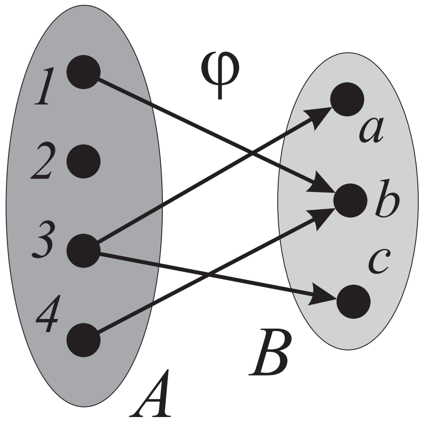

Рис. 4

П р и м е р 1. Для φ, изображенного на рис. 4, $Dom\,\varphi = \{1,3,4\}$ и $Im\,\varphi = \{a,b,c\}$.

Для обозначения соответствия φ между множествами A и B будем использовать $A \xrightarrow{\varphi} B$ или $\varphi : A \to B$.

Опишем некоторые типы соответствий.

Определение. *Соответствие φ называется*
1) всюду определенным, если $Dom\,\varphi = A$;
2) сюръективным, если $Im\,\varphi = B$;
3) однозначным, если каждому $a \in Dom\,\varphi$ соответствует единственный элемент b из B, т.е. из $(a,b) \in \varphi$ и $(a,b_1) \in \varphi \Rightarrow b = b_1$;
4) инъективным, если разным элементам из $Dom\,\varphi$ соответствуют разные элементы из B, т.е. из $(a,b) \in \varphi$ и $(a_1,b) \in \varphi \Rightarrow a = a_1$.

П р и м е р 2. Так, соответствие φ из примера 1 сюръективно, но не всюду определено ($2 \notin Dom\,\varphi$), не однозначно (так как $(3,a),(3,c) \in \varphi$), не инъективно (так как $(1,b),(4,b) \in \varphi$). Чаще всего мы будем иметь дело с хорошими соответствиями — отображениями и биекциями.

Определение. *Отображением называется всюду определенное и однозначное соответствие (выполняются свойства 1 и 3). Функцией называют отображение в вещественную прямую (т.е. $B = R$).*

Определение. *Биекцией называют всюду определенное, сюръективное, однозначное и инъективное соответствие (выполняются все свойства 1—4).*

Например, квадратичная функция каждому числу $x \in R$ (поэтому она всюду определена) ставит в соответствие одно число $ax^2 + bx + c$ (она однозначна). Но квадратичная функция не является инъективным соответствием (некоторым различным числам она ставит в соответствие одно и то же число). Поэтому это не биекция. С другой стороны, функция $f(x) = kx + b$ является биекцией при $k \neq 0$.

К соответствиям можно применять две операции — рассматривать обратное соответствие и брать композицию соответствий.

Определение. *Обратным соответствием к соответствию* $\varphi \subseteq A \times B$ *называют* $\varphi^{-1} = \{(b, a) : (a, b) \in \varphi\}$.

Заметим, что $\varphi^{-1} \subseteq B \times A$, поэтому φ^{-1} — это соответствие уже между B и A . На рис. 5 показано обратное соответствие к φ , изображенному на рис. 4. В этом случае $\varphi^{-1} = \{(b, 1),\ (a, 3),\ (c, 3),\ (b, 4)\}$.

Определение. *Композицией соответствий* $\varphi \subseteq A \times B$ *и* $\psi \subseteq B \times C$ *называют соответствие* $\chi \subseteq A \times C$ *такое, что* $\chi = \{(a, c) :$ *существует элемент* $b \in B$*, что* $(a, b) \in \varphi$ *и* $(b, c) \in \psi\}$ *(обозначается композиция так:* $\chi = \psi \circ \varphi$ *).*

Композиция соответствий, изображенных на ри с. 6, является множеством $\psi \circ \varphi = \{(1, y),\ (3, x),\ (4, y)\}$.

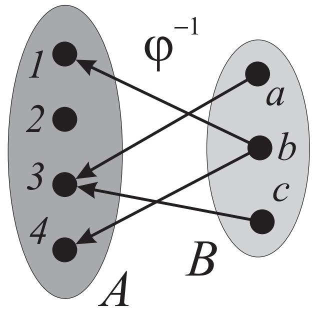

Рис. 5

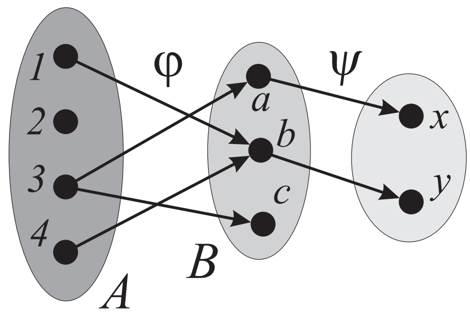

Рис. 6

Биекции устойчивы к операции взятия композиции и перехода к обратному соответствию.

Теорема 1.3.3. *Если* $\varphi \subseteq A \times B$ *и* $\psi \subseteq B \times C$ *— биекции, то*
1) φ^{-1} *является биекцией между* B *и* A *;*
2) $\psi \circ \varphi$ *является биекцией между* A *и* C *.*

Доказательство. 1. Так как φ всюду определено, то φ^{-1} сюръективно. Так как φ сюръективно, то φ^{-1} всюду определено. Два оставшихся свойства проверяются аналогично.

2. Поскольку φ и ψ всюду определены, то и их композиция $\psi \circ \varphi$ будет определена в каждой точке множества A . Так как φ действует на все B и ψ — на все C , то $\psi \circ \varphi$ является сюръективным соответствием. Однозначность и инъективность также легко проверить.

■

Упражнения

26. Найти пересечение множеств $A = \{1, a, 2\}$ и $B = \{a, b, 3\}$. Найти пересечение R и R^2 .

27. Какая плоская фигура соответствует $\{(x, y) \in R^2 : Ax + By + C = 0,$ где $A, B, C \in R\}$? Рассмотреть все случаи A , B , C .

28. Какая плоская фигура соответствует множеству $\{(x,y) \in R^2 : (|x|-|y|)(x^2+y^2-4x) = 0\}$?

29. Известно, что $A \times B = \varnothing$. Что можно сказать о множествах A и B ?

30. Пусть для множеств A, B, C имеет место условие $(A \times B) \cup (B \times A) = C \times C$. Доказать, что $A = B = C$.

31. В каком случае $A \times B = B \times A$? Описать все такие случаи.

32. Являются ли биекциями $f(x) = x^3$, $f(x) = \sqrt[3]{x}$, $f(x) = \sqrt{x}$?

33. Если φ — отображение, то соотношение $(a,b) \in \varphi$ будем записывать в виде $b = \varphi(a)$. (Почему это можно сделать только для отображений?) Тогда композицию $\psi \circ \varphi$ можно записать так: $\psi(\varphi(a))$ (т.е. сначала на элемент из A действует φ , а затем на получившийся элемент $\varphi(a) \in B$ действует ψ). Пусть $f(x) = x^2$ и $g(x) = x + 1$, найти $g \circ f$ и $f \circ g$.

34. Пусть $A \xrightarrow{f} A$ и $f \circ f \circ \ldots \circ f = id_A$, где id_A — тождественное соответствие на A , т.е. для любого $a \in A$ выполняется $id_A(a) = a$. Доказать, что f — биекция.

35. Пусть $A \xrightarrow{f} B$. Доказать, что f — инъективное соответствие $\Leftrightarrow$ для любых $g, h(g : B \longrightarrow A,\ h : B \longrightarrow A)$ из равенства $f \circ g = f \circ h$ следует $g = h$.

36. Пусть $X \xrightarrow{f} Y$, $X \neq \varnothing$. Доказать, что f — сюръективное соответствие $\Leftrightarrow$ для любых $g, h(g : Y \longrightarrow X,\ h : Y \longrightarrow X)$, из того, что $g \circ f = h \circ f$, следует, что $g = h$.

37. Пусть F — отображение $F : X \longrightarrow Y$. Покажите, что эквивалентны следующие свойства:

1. F — инъективное отображение;
2. $F^{-1}\Big(F(A)\Big) = A$ для любого подмножества $A \subseteq X$;
3. $F(A \cap B) = F(A) \cap F(B)$ для любой пары A, B подмножеств X ;
4. $F(A) \cap F(B) = \varnothing$ для любой пары A, B подмножеств X таких, что $A \cap B = \varnothing$;
5. $F(A \backslash B) = F(A) \backslash F(B)$ для любой пары A, B подмножеств X , для которой $B \subseteq A$.

Глава 2

Введение в комбинаторику

2.1 Конечные множества. Принцип Дирихле

Сравнивать между собой количества элементов двух различных конечных множеств A и B кажется простой задачей. Для этого можно определить число элементов в A, затем в B и сравнить получившиеся два целых числа. Теперь усложним задачу. Попытайтесь представить себе такую ситуацию, что вы разучились считать, но вам необходимо определить: одинаковое количество элементов во множествах A и B или нет. Если вы справились с первой частью задачи, то вторую часть задачи можно решить с помощью биекции. Следует выбирать по элементу из каждого множества, образуя пары (пары соответствия), до тех пор, пока не закончатся элементы хотя бы в одном из этих двух множеств. Если это произойдет одновременно, то получится биекция между этими множествами, и, следовательно, во множествах A и B одинаковое количество элементов.

Определение. *Множества A и B называются равномощными ($A \sim B$), если существует биекция между ними (т.е. существует $A \xrightarrow{\varphi} B$, что φ — биекция).*

Теорема 2.1.1. *Пусть A, B и C — некоторые множества. Тогда выполняются свойства [6]:*

1. $A \sim A$.
2. $A \sim B \Rightarrow B \sim A$.
3. $A \sim B$ *и* $B \sim C \Rightarrow A \sim C$.

[6] Первое из этих свойств называется рефлексивностью, второе — симметричностью и третье — транзитивностью.

Доказательство. 1. Биекцию A на себя построить легко: пусть по определению $\varphi(a) = a$ для любого $a \in A$ [7]. φ — искомая биекция.

2. Пусть $A \xrightarrow{\varphi} B$ —биекция между A и B, тогда φ^{-1} — биекция между B и A (см. теорему 1.3.3).

3. Пусть $A \xrightarrow{\varphi} B$, $B \xrightarrow{\psi} C$ —биекции между A, B и B, C соответственно, тогда $\psi \circ \varphi$ — биекция между A и C (см. теорему 1.3.3).

∎

Определение. *Пусть $n \in N$, тогда множество $N_{\leqslant n} = \{1, 2, \ldots, n\}$ называют начальным отрезком натурального ряда.*

Лемма 2.1.1. $N_{\leqslant n} \sim N_{\leqslant m} \Leftrightarrow n = m$.

Доказательство. $\Leftarrow$). Если $n = m$, то $N_{\leqslant n} = N_{\leqslant m}$ и используем первое свойство теоремы 2.1.1 .

$\Rightarrow$). Пусть $N_{\leqslant n} \sim N_{\leqslant m}$, тогда существует биекция $N_{\leqslant n} \xrightarrow{\varphi} N_{\leqslant m}$. Изменим эту биекцию следующим образом. Пусть $\varphi(1) = k$, где $k \leqslant m$, и существует $l \leqslant n$, что $\varphi(l) = 1$. Рассмотрим $\varphi_1 = \Big(\varphi \backslash \{(1, k),\ (l, 1)\}\Big) \cup \cup \{(1, 1),\ (l, k)\}$. Ясно, что φ_1 — биекция, так как мы поменяли местами значения φ на двух элементах (в 1 и l). Заметим, что уже $\varphi_1(1) = 1$. Аналогично построим биекцию φ_2 со свойством $\varphi_2(1) = 1, \varphi_2(2) = 2$ и т.д. В конце концов мы получим φ_n со свойством $\varphi_n(i) = i, \quad i \leqslant n$. Так как φ_n сюръективно и сохраняет порядок, то $\varphi_n(n) = m$, с другой стороны, $\varphi_n(n) = n \Rightarrow n = m$.

∎

Определение. *Множество A называется конечным множеством, если $A = \varnothing$ или существует $n \in N$, что $A \sim N_{\leqslant n}$. При этом будем говорить, что мощность множества A равна n ($|A| = n$). Если множество пусто, то по определению считаем, что его мощность равна нулю.*

Например, если $\text{А}_{\text{рус}}$ — множество всех букв русского алфавита, то $|\text{А}_{\text{рус}}| = 33$.

Теорема 2.1.2. *Пусть $|A| = n$ и $|B| = m$. Тогда $A \sim B \Leftrightarrow n = m$.*

Доказательство. $\Rightarrow$). Поскольку $|A| = n$, существует биекция $A \xrightarrow{\varphi} N_{\leqslant n}$. Из определения равномощности A и B найдется биекция $A \xrightarrow{\psi} B$. Тогда соответствие $\varphi \circ \psi^{-1}$ является биекцией между B и $N_{\leqslant n}$. Следовательно, $|B| = n$ (на рис. 7 и 8 изображены *коммутативные диаграммы*, которые являются иллюстрацией к доказательству этой теоремы).

---

[7] Такая биекция называется тождественным отображением A на себя и обозначается id_A.

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "\psi"'] & N_{\leqslant n} \\ B \arrow[ur, "\varphi\circ\psi^{-1}"'] & \end{tikzcd}$$

Рис. 7

$$\begin{tikzcd} A \arrow[rr, "\psi^{-1}\circ\varphi"] \arrow[dr, "\varphi"'] & & B \arrow[dl, "\psi"] \\ & N_{\leqslant n} & \end{tikzcd}$$

Рис. 8

$\Leftarrow$). Пусть $|A| = |B| = n$. Тогда существуют биекции $A \xrightarrow{\varphi} N_{\leqslant n}$ и $B \xrightarrow{\psi} N_{\leqslant n}$. Следовательно, $\psi^{-1} \circ \varphi$ — биекция между A и B (рис. 8).

■

Следствие 1. $|A| = n \Leftrightarrow$ *когда множество A можно представить в виде $\{a_1, \ldots, a_n\}$, где $a_i \neq a_j, i \neq j$.*

Доказательство. Так как существует биекция $A \xrightarrow{\varphi} N_{\leqslant n}$, то, обозначив $\varphi^{-1}(i)$ через a_i, мы получим искомое представление. Обратно, если такое представление задано, биекцию можно построить так: $\varphi(a_i) = i$.

■

Следствие 2. *Пусть $|A| = n$, $a \in A$ и $k \leqslant n$, $k \in N$, тогда $A = \{a_1, \ldots, a_k, \ldots, a_n\}$, где $a_k = a$. То есть можно занумеровать элементы множества A так, что наперед выбранный элемент a будет иметь номер k.*

Доказательство. Пусть $\varphi : A \to N_{\leqslant n}$ — биекция. Если $\varphi(a) = k$, то используем предыдущее следствие. Иначе существуют $(a, l), (b, k) \in \varphi$, что $a \neq b$. Определим $\psi = \Big(\varphi \backslash \{(a, l), (b, k)\}\Big) \cup \{(a, k), (b, l)\}$. Это соответствие является искомой биекцией. Осталось применить предыдущее следствие.

■

Следствие 3 *(принцип Дирихле). Пусть $n \neq m$, тогда n кроликов нельзя рассадить в m ящиков так, чтобы в каждом ящике было по одному кролику.*

Доказательство. От противного (далее — о/п). Если это можно сделать, то существует биекция между множеством кроликов и множеством ящиков. Тогда по предыдущей теореме $n = m$. Противоречие (далее — ⤫).

■

П р и м е р 1. В равностороннем треугольнике со стороной 1 расположены 5 точек. Доказать, что существует по крайней мере две точки, расстояние между которыми не больше $1/2$. Для решения достаточно заметить, что средние линии треугольника разбивают его на четыре равносторонних треугольника со стороной $1/2$. По принципу Дирихле две точки попадут в один из этих треугольников. Расстояние между ними будет не больше $1/2$.

П р и м е р 2. Доказать, что существует $n \in N$ такое, что 7^n оканчивается на 000001. Рассмотрим множество остатков от деления чисел вида 7^n на 1000000. Среди чисел 7^n при $n \leqslant 1000001$ найдутся по крайней мере два (по принципу Дирихле), дающих при делении на 1000000 одинаковые остатки, т.е. $7^{k_1} \equiv 7^{k_2} (mod 1000000)$ для некоторых $k_1 \neq k_2, \quad k_1, k_2 \leqslant 1000001$. Следовательно, $7^{k_1}(7^{k_2-k_1} - 1) \vdots 1000000$. Заметим, что 7^{k_1} взаимно просто с числом 1000000. Следовательно, число $k_2 - k_1$ искомое.

Теорема 2.1.3. *Пусть* $|A| = n$ *и* $|B| = m$ *— конечные множества, тогда*

1. *если* $A \cap B = \varnothing$, *то* $|A \cup B| = |A| + |B|$,
2. *если* $C \subseteq B$, *то* $|B \backslash C| = |B| - |C|$,
3. $|A \cup B| = |A| + |B| - |A \cap B|$.

Доказательство. 1. Пусть $A \xrightarrow{\varphi} N_{\leqslant n}$ и $B \xrightarrow{\psi} N_{\leqslant m}$. Тогда существует биекция $A \cup B \xrightarrow{\chi} N_{\leqslant n+m}$, где χ задается по правилу:

$$\chi(c) = \begin{cases} \varphi(c), & \text{если } c \in A; \\ \psi(c) + n, & \text{если } c \in B. \end{cases}$$

2. Пусть $C \subseteq B$ и $|C| = k$, тогда по второму следствию теоремы 2.1.2 существует представление $B = \{b_1, \ldots, b_{m-k}, \quad b_{m-k+1}, \ldots, b_m\}$, где $C = \{b_{m-k+1}, \ldots, b_m\}$. Следовательно, $B \backslash C = \{b_1, \ldots, b_{m-k}\}$. Используя первое следствие, получаем $|B \backslash C| = m - k$.

3. $A \cup B = A \cup (B \backslash (A \cap B))$. Используя свойство 1, получаем $|A \cup B| = |A| + |B \backslash (A \cap B)|$. По свойству 2 $|A \cup B| = |A| + |B| - |A \cap B|$.

■

Следующая теорема усиливает третье свойство предыдущей теоремы. Она позволяет найти число элементов объединения произвольного конечного числа конечных множеств. Формула этой теоремы называется формулой *включений* и *исключений*.

Теорема 2.1.4. *Пусть* $A_1, \ldots, A_n$ *— конечные множества. Тогда*

$$|A_1 \cup A_2 \cup \ldots \cup A_n| =$$
$$(|A_1| + |A_2| + \ldots + |A_n|) - \underbrace{(|A_1 \cap A_2| + \ldots + |A_{n-1} \cap A_n|)}_{\textit{все попарные пересечения}} +$$
$$+ \ldots (-1)^{k-1} \underbrace{(|A_1 \cap A_2 \cap \ldots \cap A_k| + \ldots + |A_{n-k+1} \cap \ldots \cap A_n|)}_{\textit{все пересечения по } k \textit{ множеств}} +$$
$$+ \ldots (-1)^{n-1}(|A_1 \cap A_2 \cap \ldots \cap A_n|).$$

Доказательство. Индукция по n. Случай $n = 1$ очевиден, а $n = 2$ доказан в предыдущей теореме. Пусть для любых объединений из k множеств, где $k < n$ и $k \in N$, формула справедлива, и докажем ее для n. Введем обозначение $A_1 \cup A_2 \cup \ldots \cup A_{n-1} = \Phi$, тогда по базе индукции получаем

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = |\Phi| + |A_n| - |\Phi \cap A_n|. \tag{1}$$

По предположению индукции

$$\begin{aligned}
|\Phi| = &\Big(|A_1| + |A_2| + \ldots + |A_{n-1}|\Big) - \\
- &\underbrace{\Big(|A_1 \cap A_2| + |A_1 \cap A_3| + \ldots + |A_{n-2} \cap A_{n-1}|\Big)}_{\text{все попарные пересечения, в которые не входит } A_n} + \\
+ \ldots (-1)^{k-1} &\underbrace{\Big(|A_1 \cap \ldots \cap A_k| + \ldots + |A_{n-k} \cap A_{n-k+1} \cap \ldots \cap A_{n-1}|\Big)}_{\text{все пересечения по k элементов, в которые не входит } A_n} + \\
+ \ldots (-1)^{n-2} &\Big(|A_1 \cap A_2 \cap \ldots \cap A_{n-1}|\Big).
\end{aligned} \tag{2}$$

По теореме 1.2.1

$$\Phi \cap A_n = (A_1 \cap A_n) \cup (A_2 \cap A_n) \cup \ldots \cup (A_{n-1} \cap A_n).$$

Заметим, что в объединении участвуют $n - 1$ множеств. Снова используем предположение индукции.

$$\begin{aligned}
|\Phi \cap A_n| = &\Big(|A_1 \cap A_n| + |A_2 \cap A_n| + \ldots + |A_{n-1} \cap A_n|\Big) - \\
- &\underbrace{\Big(|A_1 \cap A_2 \cap A_n| + \ldots + |A_{n-2} \cap A_{n-1} \cap A_n|\Big)}_{\text{все пересечения по три элемента, в которые входит } A_n} + \ldots + \\
(-1)^{k-1} &\underbrace{\Big(|A_1 \cap \ldots \cap A_k \cap A_n| + \ldots + |A_{n-k} \cap A_{n-k+1} \cap \ldots \cap A_{n-1} \cap A_n|\Big)}_{\text{все пересечения по } k+1 \text{ элементу, в которые входит } A_n} + \\
+ \ldots (-1)^{n-2} &\Big(|A_1 \cap A_2 \cap \ldots \cap A_{n-1} \cap A_n|\Big)
\end{aligned} \tag{3}$$

Подстановка правых частей уравнений (2) и (3) в уравнение (1) завершает доказательство.

■

Следствие.

1. $|A_1 \cup A_2 \cup A_3| = (|A_1| + |A_2| + |A_3|) - (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) + (|A_1 \cap A_2 \cap A_3|)$.

2. $|\overline{A_1 \cap A_2 \cap A_3}| = (|\overline{A_1}| + |\overline{A_2}| + |\overline{A_3}|) - (|\overline{A_1} \cap \overline{A_2}| + |\overline{A_1} \cap \overline{A_3}| + |\overline{A_2} \cap \overline{A_3}|) + (|\overline{A_1} \cap \overline{A_2} \cap \overline{A_3}|)$.

Доказательство. Если в предыдущей теореме $n = 3$, то получается первое из этих двух утверждений. Чтобы доказать второе, достаточно воспользоваться одной из формул де Моргана: $\overline{A_1 \cap A_2 \cap A_3} = \overline{A_1} \cup \overline{A_2} \cup \overline{A_3}$.

■

Упражнения

38. Определить мощность $A_{\text{лат}}$, где $\text{А}_{\text{лат}}$ – множество, состоящее из всех латинских букв.

39. Пусть $|A| = n$ и $a \neq b, a, b \in A$, тогда множество A можно представить в виде $A = \{a_1, \ldots, a_n\}$, где $a = a_1, b = a_n$.

40. Как при доказательстве первого пункта теоремы 2.1.3 использовалось условие $A \cap B = \varnothing$?

41. Доказать, что если A – конечное множество, то A не равномощно множеству $A \backslash \{a\}$, где $a \in A$.

42. Доказать, что A – конечное множество $\Leftrightarrow$ A не равномощно никакому своему собственному (т.е. $B \subseteq A$ и $B \neq A$).

43. Доказать следующее усиление принципа Дирихле. Пусть n, k, m – натуральные числа и $n \cdot k < m$. Тогда нельзя рассадить n кроликов в m ящиков так, чтобы в каждом ящике было не более k кроликов.

44. Попытаться решить “веселую задачу” Л.Кэролла: в неравном бою из 100 пиратов 90 потеряли руку, 80 – ногу, 70 – глаз. Определить наименьшее количество “счастливчиков”, потерявших одновременно и руку, и ногу, и глаз.

2.2 Степень данного множества и его мощность

В предыдущих параграфах не раз встречались множества, элементы которых также являлись множествами. Определение упорядоченной пары дает нам один из возможных примеров. Рассмотрим произвольное множество A. Будем теперь рассматривать новые множества, элементами которых являются подмножества множества A (так как $\varnothing, A \subseteq A$, то среди таких множеств будут $\{\varnothing\}, \Big\{\varnothing, \{A\}\Big\}$). В этом подразделе нас будет интересовать “максимальное" [8] из множеств, которые конструируются только из подмножеств множества A.

Определение. *Пусть A — произвольное множество. Степенью множества A называется множество (обозначается через $\mathcal{P}(A)$ или 2^A), состоящее из всех подмножеств множества A ($\mathcal{P}(A) = \{B : B \subseteq A\}$).*

Степень множества также называется множеством всех подмножеств множества A.

Пример 1. Пусть $A = \{a\}$. Тогда $\mathcal{P}(A) = \{\varnothing, \{a\}\}$, $|A| = 1$, $|\mathcal{P}(A)| = 2 = 2^1$. Заметим, что $\varnothing \in \mathcal{P}(A)$ и $A \in \mathcal{P}(A)$ для любого множества A.

Пример 2. $A = \{1, a, B\}$. Тогда

$$\mathcal{P}(A) = \{\varnothing, \{1\}, \{a\}, \{B\}, \{1, a\}, \{1, B\}, \{a, B\}, \{1, a, B\}\},$$

$|A| = 3$, $|\mathcal{P}(A)| = 8 = 2^3$. Множество $\mathcal{P}(A)$ можно разбить на два —

$$\{\varnothing, \{a\}, \{B\}, \{a, B\}\} \quad \text{и} \quad \{\{1\}, \{1, a\}, \{1, B\}, \{1, a, B\}\}.$$

Заметим, что элементы первого множества не содержат 1, а каждый элемент второго множества, напротив, содержит 1. Эти два множества равномощны. Биекцию легко построить, используя предыдущее замечание: каждому элементу первого множества мы поставим в соответствие это же самое множество, объединенное с $\{1\}$ (а это уже элемент второго множества). Эта идея используется при доказательстве следующей теоремы.

Теорема 2.2.1. *Пусть $|A| = n$. Тогда $|\mathcal{P}(A)| = 2^n = 2^{|A|}$.*

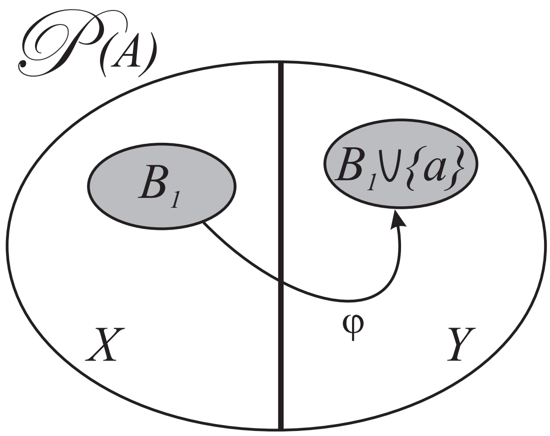

Рис. 9

Доказательство. Индукция по n.

База индукции (далее — Б.И.). $n = 1$. Тогда $A = \{a\} \Rightarrow \mathcal{P}(A) = \{\varnothing, \{a\}\} \Rightarrow |\mathcal{P}(A)| = 2^1$.

Шаг индукции (далее — Ш.И.). Предположим, что если $|A| = k \Rightarrow |\mathcal{P}(A)| = 2^k$. Пусть теперь $|A| = k + 1$. Выберем некоторый $a \in A$ и обозначим через $A_1 = A \setminus \{a\}$. Тогда $A = A_1 \cup \{a\}$ и $|A_1| = k$.

Заметим, что $B \subseteq A \Leftrightarrow B \subseteq A_1$ или существует такое множество $B_1 \subseteq A_1$, что $B = B_1 \cup \{a\}$.

Пусть $X = \{B_1 : B_1 \subseteq A_1\}$, т.е. это все те подмножества множества A, которым не принадлежит элемент a. И $Y = \{B \subseteq A : a \in B\}$ — все остальные подмножества из A.

[8] В 3.4 определяются понятия порядка и максимального элемента; там же доказывается, что $\subseteq$ является отношением порядка.

Используя предыдущее замечание, получаем, что X и Y удовлетворяют следующим свойствам:

1. $X = \mathcal{P}(A_1)$.
2. $X \cup Y = \mathcal{P}(A)$.
3. $X \cap Y = \varnothing$.

Множества X и Y равномощны. Биекцию φ можно задать правилом: если $B_1 \in X$, то $\varphi(B_1) = B_1 \cup \{a\}$ (рис. 9). По предположению индукции и по свойству 1 получаем $|X| = 2^k$. Из свойств 2 и 3 $|\mathcal{P}(A)| = |X| + |Y| = 2|X|$. Следовательно, $|\mathcal{P}(A)| = 2^{k+1}$.

■

Упражнения

45. Попытайтесь представить себе множество всех подмножеств четырехугольника. Принадлежат ли этому множеству стороны этого четырехугольника, его вершины, точка пересечения его диагоналей?

46. Найти $\mathcal{P}(N_{\leqslant 4})$.

47. Пусть A и B — конечные множества. Доказать, что $A = B \Leftrightarrow \mathcal{P}(A) = \mathcal{P}(B)$.

48. Какому из двух множеств, X или Y , в предыдущей теореме принадлежит $\varnothing$?

49. Докажите, что соответствие φ в теореме этого параграфа является биекцией.

50. Что ставит в соответствие биекция φ пустому множеству?

2.3 Отображения конечных множеств. Размещения с повторениями

Напомним, что в 1.4 было определено отображение между множествами. Всякое отображение из B в A является подмножеством $B \times A$ (так как это соответствие), в качестве первых элементов этих пар используются все элементы множества B (так как отображение всюду определено), и элементы множества B не могут использоваться в качестве первых элементов пар данного соответствия более одного раза (так как отображение однозначно).

Множество всех отображений одного конечного множества в другое полезно своими комбинаторными приложениями.

Определение.

$$A^B = \{f : f - \textit{отображение из } B \textit{ в } A\}$$

(читается: A в степени B).

Договоримся использовать символы f, g, h для обозначения отображений.

П р и м е р 1. Пусть $B = \{a, b, c\}$ и $A = \{1, 2\}$, тогда $f_1 = \{(a,1), (b,1), (c,1)\} \in A^B$ и $f_2 = \{(a,1), (b,1), (c,2)\} \in A^B$. Аналогично можно построить шесть оставшихся элементов множества A^B.

В общем случае какова мощность множества A^B? Ответ на этот вопрос дает следующая теорема.

Теорема 2.3.1. *Пусть* $|A| = n,\ |B| = m$. *Тогда* $|A^B| = n^m = |A|^{|B|}$.

Доказательство. Докажем индукцией по m. Пусть $A = \{a_1, \ldots, a_n\}$.

Б.И. $m = 1$. Тогда $B = \{b\}$. Следовательно, $A^B = \{f_1, \ldots, f_n\}$, где $f_1 = \{(b, a_1)\}, \ldots, f_n = \{(b, a_n)\}$.

Ш.И. Предположим, что если $|B| = k$, то $|A^B| = n^k$.

Пусть теперь $|B| = k+1$. Выберем $b \in B$ и обозначим $B_1 = B \backslash \{b\}$. Тогда $B = B_1 \cup \{b\}$. По предположению $|A^{B_1}| = n^k$. Выберем произвольное отображение $f \in A^{B_1}$ (оно не определено в b, поэтому $f \notin A^B$) и доопределим его на b. Существует в точности n различных продолжений этого отображения (рис. 10):

$$
f \qquad \begin{array}{c} f \cup \{(b, a_1)\} = f_1 \in A^B, \\ f \cup \{(b, a_2)\} = f_2 \in A^B, \\ \vdots \\ f \cup \{(b, a_n)\} = f_n \in A^B. \end{array}
$$

Нетрудно заметить, что если отображения $f, g \in A^{B_1}$ различны, то любое продолжение отображения f отличается от любого продолжения отображения g. Поэтому $|A^B| = |A^{B_1}| \times (\text{количество продолжений}) = n^k \cdot n = n^{k+1}$.

■

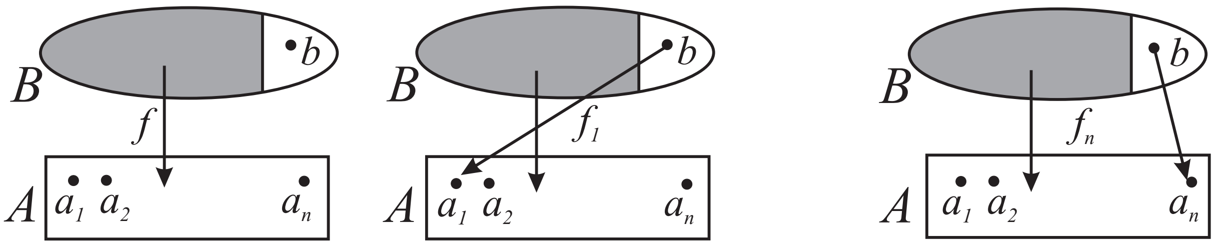

Рис. 10

Прежде чем ввести новое понятие размещения с повторениями, обсудим понятие упорядоченного m-набора $(a_1, \ldots, a_m)$, состоящего из элементов некоторого множества A. Он отличается от ранее введенного понятия упорядоченной пары (которая является упорядоченным 2-набором) только количеством элементов (конечно, если $m > 2$). Основное свойство m-набора такое же: $(a_1, \ldots, a_m) = (b_1, \ldots, b_m) \Leftrightarrow$ одновременно $a_1 = b_1, \ldots, a_m = b_m$.

П р и м е р 2. $(1,a,2) = (b,3,c) \Leftrightarrow 1 = b, a = 3, 2 = c$, но $(1,2,3) \neq (1,3,2)$.

Определение. *Пусть A — конечное множество ($|A| = n$). Тогда размещением из n элементов по m элементов с повторениями называют произвольный упорядоченный m-набор элементов множества A. $\overline{A}_n^m$ — количество всех размещений с повторениями из n по m элементов.*

П р и м е р 3. Пусть $A = \{a, b\}$. Ниже выписаны все размещения по три элемента. Непосредственным подсчетом убеждаемся, что $\overline{A}_2^3 = 2^3 = 8$.

$$\begin{array}{cccc} (a,a,a) & (a,a,b) & (a,b,a) & (b,a,a) \\ (b,b,b) & (b,b,a) & (b,a,b) & (a,b,b) \end{array}.$$

Теорема 2.3.2. $\overline{A}_n^m = n^m$.

Доказательство. Достаточно показать, что искомых размещений столько же, сколько элементов во множестве $A^{N_{\leqslant m}}$. Для этого каждому размещению однозначно поставим в соответствие отображение по следующему правилу:

$$(a_1, \ldots, a_m) \xrightarrow{\varphi} \{(1,a_1), \ldots (m, a_m)\} = f \in A^{N_{\leqslant m}}.$$

Легко проверить, что φ — биекция. Поэтому $\overline{A}_n^m = |A^{N_{\leqslant m}}| = n^m$.

■

Заметим, что в предыдущей теореме мы указали способ, как свести понятие упорядоченного m-набора к понятию множества, состоящего из упорядоченных пар. Другой путь определения m-набора указан в упражнениях этого параграфа.

П р и м е р 4. Используя формулу предыдущей теоремы, можно определить количество всевозможных четырехзначных автомобильных номеров. Каждый такой номер — это упорядоченный 4-набор (так как порядок цифр важен). Каждая цифра — элемент множества $\{0,1,2,3,4,5,6,7,8,9\}$. Поэтому искомое число равно $\overline{A}_{10}^4 = 10^4$.

Упражнения

51. Выпишите все восемь отображений из первого примера.

52. Справедлива ли первая теорема этого параграфа, если $B = \varnothing$?

53. Убедиться в том, что в результате продолжений отображений из A^{B_1} в первой теореме получатся все элементы множества A^B .

54. Доказать, что во второй теореме этого параграфа φ действительно является биекцией.

55. Определите упорядоченную тройку следующим образом: $(a, b, c) = ((a, b), c)$. Докажите, что $(a, b, c) = (x, y, z) \Leftrightarrow a = x, b = y, c = z$. Укажите путь строгого определения упорядоченного m -набора.

56. Сколькими способами можно распределить десять бильярдных шаров по шести лузам?

2.4 Взаимно однозначные отображения одного множества в другое. Размещения без повторений. Перестановки

Когда речь идет о биекции между множествами B и A , часто используют математический синоним: взаимно однозначное отображение B **на** A . Если число элементов во множестве B меньше (не больше), чем в A , тогда B взаимно однозначно можно отобразить только на подмножество из A (сохраняя свойство инъективности, мы не требуем, чтобы отображение было сюръективным). В этом случае мы будем использовать термин — “взаимно однозначное отображение B в A ”.

П р и м е р 1. Пусть $B = \{1, 2\}$ и $A = \{a, b, c\}$. Тогда $f_1 = \{(1, a), (2, b)\}$, $f_2 = \{(1, b), \ (2, c)\}$, $f_3 = \{(1, b), \ (2, a)\}$, $f_4 = \{(1, c), \ (2, b)\}$ и $f_5 = \{(1, a), \ (2, c)\}$ $f_6 = \{(1, c), \ (2, a)\}$ — примеры всех взаимно однозначных отображений B в A .

Определение. $^{B}A = \{f : f$ *— взаимно однозначное отображение* B *в* $A\}$.

Теорема 2.4.1. *Пусть* $|A| = n$ *и* $|B| = m$ $n \geqslant m$. *Тогда*

$$|^{B}A| = \underbrace{n(n-1) \cdot \ldots \cdot (n-m+1)}_{m \text{ множителей}}.$$

Доказательство. Индукция по m . Пусть $A = \{a_1, \ldots, a_n\}$.

Б.И. $m = 1$. Тогда $B = \{b\}$. Обозначим через $f_1 = \{(b, a_1)\}$, $\ldots$, $f_n = \{(b, a_n)\}$. Следовательно, $^{B}A = \{f_1, \ldots, f_n\}$. Поэтому $|^{B}A| = n$.

Ш.И. Предположим, что если $|B| = k$, то $|^{B}A| = n(n-1) \cdot \ldots \cdot (n-k+1)$.

Пусть теперь $|B| = k + 1$. Выберем $b \in B$ и обозначим $B_1 = B \setminus \{b\}$. Тогда $B = B_1 \cup \{b\}$. По предположению $|^{B_1}A| = n(n-1) \cdot \ldots \cdot (n-k+1)$. Выберем произвольное отображение $f \in {}^{B_1}A$ (оно не определено в b, поэтому $f \notin {}^{B}A$) и доопределим его на b. Заметим, что $|f(B_1)| = k = |B_1|$, так как f — биекция. Следовательно, $|A \setminus f(B_1)| = n - k$. Поэтому $A \setminus f(B_1) = \{c_1, \ldots, c_{n-k}\}$. Теперь легко доопределить взаимно однозначное отображение f на элементе b так, чтобы продолжение также было взаимно однозначным (необходимо элементу b ставить в соответствие один из элементов $A \setminus f(B_1)$). Существует (рис. 11) в точности $n - k$ различных продолжений этого отображения:

$$
{}^{B_1}A \ni f \qquad \begin{array}{c} f \cup \{(b, c_1)\} = f_1 \in {}^{B}A, \\ f \cup \{(b, c_2)\} = f_2 \in {}^{B}A, \\ \vdots \\ f \cup \{(b, c_{n-k})\} = f_{n-k} \in {}^{B}A. \end{array}
$$

Нетрудно заметить, что если биекции $f, g \in {}^{B_1}A$ различны, то любое продолжение биекции f отличается от любого продолжения биекции g. Поэтому $|^{B}A| = |^{B_1}A| \times$ (количество продолжений) $= n(n-1) \cdot \ldots \cdot (n-k+1) \times (n - (k+1) + 1)$.

■

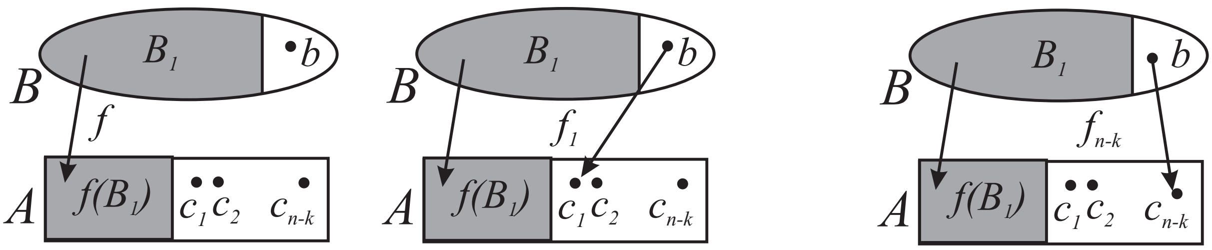

Рис. 11

Следствие.

$$
|^{B}A| = \frac{n!}{(n-m)!}.
$$

Определение. *Пусть A — конечное множество ($|A| = n$ и $n \geqslant m$). Тогда размещением из n элементов по m элементов называют произвольный упорядоченный m-набор различных элементов множества A. A_n^m — количество всех размещений из n по m элементов.*

Теорема 2.4.2.

$$
A_n^m = \frac{n!}{(n-m)!}.
$$

Доказательство. Достаточно показать, что искомых размещений столько же, сколько элементов во множестве ${}^{N_{\leqslant m}}A$. Для этого определим биекцию между размещениями и взаимно однозначными отображениями из ${}^{N_{\leqslant m}}A$ следующим образом:

$$(a_1, \ldots, a_m) \xrightarrow{\varphi} \{(1, a_1), \ldots, (m, a_m)\} = f \in {}^{N_{\leqslant m}}A.$$

Легко проверить, что φ — биекция. Поэтому $A_n^m = |{}^{N_{\leqslant m}}A| = \dfrac{n!}{(n-m)!}$.

■

Определение. *Перестановкой n-элементного множества A называется размещение по n элементов. P_n — количество всех перестановок.*

Следствие. $P_n = n!$.

Каждая перестановка элементов множества A задает на этом множестве порядок. Поэтому последняя формула позволяет легко находить число всевозможных упорядочений данного множества.

П р и м е р 2. Сколькими способами можно расставить 10 томов на книжной полке? Из предыдущего замечания — $10!$.

П р и м е р 3. В предыдущей задаче потребуем, чтобы первый и второй тома стояли рядом. Тогда рассуждать можно следующим образом: будем считать тома 1 и 2 за одну книгу, тогда всевозможных расстановок с заданным условием будет $9!$. Но для каждой такой расстановки тома 1 и 2 можно поменять местами, получив еще одну перестановку. Поэтому всего будет $2 \cdot 9!$ расстановок книг таких, что выбранные два тома стоят рядом.

Упражнения

57. Что можно сказать о множестве ${}^{B}A$, если $|B| > |A|$?

58. Найдите количество расстановок в последнем примере, если тома 1 и 2 не должны стоять рядом.

59. Сколькими способами можно рассадить n человек за круглым столом? Два способа считаются одинаковыми, если для каждого человека сосед справа и слева остался тем же самым.

60. Сколькими способами можно рассадить n женщин и n мужчин за круглым столом так, чтобы мужчины и женщины чередовались?

61. Сколько существует трехзначных чисел, делящихся на 5, каждое из которых состоит из различных цифр?

2.5 Число сочетаний n-элементного множества по m элементов. Треугольник Паскаля. Бином Ньютона

Определение. *Пусть $|A| = n \geqslant m$. Сочетанием по m элементов множества A называют произвольное подмножество $B \subseteq A$, состоящее из m элементов. C_n^m — количество всех сочетаний по m элементов из n -элементного множества.*

Не важно, в каком порядке расположены элементы во множестве. Так, например, $\{1, 2, 3\} = \{3, 2, 1\}$. Этим сочетания отличаются от размещений.

П р и м е р 1. Пусть $A = \{a, b, c\}$. Выпишем все размещения по два элемента и все сочетания по два элемента и определим C_3^2 :

Размещения		Сочетания
(a, b)	(b, a)	$\{a, b\}$
(a, c)	(c, a)	$\{a, c\}$
(b, c)	(c, b)	$\{b, c\}$

Заметим, что размещения в каждой строке отличаются только порядком элементов, и поэтому они дают только одно сочетание. Отсюда $C_3^2 = A_3^2/2! = 3$. Этим замечанием мы воспользуемся в следующей теореме.

Теорема 2.5.1.

$$C_n^m = \frac{n!}{m!(n-m)!}.$$

Доказательство. Пусть $|A| = n$. Обозначим через R_m множество всех размещений множества A по m элементов. Разобьем множество R_m на классы. К одному классу будут относиться те размещения, которые отличаются только порядком элементов. Так, размещения $(b_1, \ldots, b_m)$ и $(c_1, \ldots, c_m)$ попадают в один класс тогда и только тогда, когда $\{b_1, \ldots, b_m\} = \{c_1, \ldots, c_m\}$. Это разбиение удовлетворяет следующим свойствам:

1) количество элементов в каждом классе равно $m!$,
2) классы между собой не пересекаются,
3) каждому классу соответствует в точности одно сочетание,
4) различным классам соответствуют различные сочетания.

Элементами каждого класса являются различные перестановки некоторого m -элементного множества, поэтому выполняется первое свойство. Свойства 2 и 4 следуют из определения классов. В каждом классе перестановки отличаются только порядком элементов, поэтому им соответствует только одно сочетание, состоящее из этих элементов. В результате

$$C_n^m = \frac{A_n^m}{P_m} = \frac{n!}{m!(n-m)!}.$$

■

Теорема 2.5.2. *Число сочетаний удовлетворяет следующим свойствам:*

1. $C_n^m = C_n^{n-m}$,
2. $C_n^0 + C_n^1 + \ldots + C_n^n = \sum\limits_{m=0}^{n} C_n^m = 2^n$,
3. $C_n^{m-1} + C_n^m = C_{n+1}^m$.

Доказательство. Свойство 1 следует из теоремы 2.5.1.

2. C_n^m — это число m -элементных подмножеств множества A $(|A| = n)$. Тогда $C_n^0 + C_n^1 + \ldots + C_n^n$ — это число всех подмножеств множества A. Поэтому $\sum\limits_{m=0}^{n} C_n^m = 2^n$.

$$3. \quad C_n^{m-1} + C_n^m = \frac{n!}{(m-1)!(n-m+1)!} + \frac{n!}{m!(n-m)!} =$$

$$= \frac{n!(n-m+1) + n! \cdot m}{m!(n-m+1)!} = \frac{(n+1)!}{m!(n-m+1)!} = C_{n+1}^m.$$

■

Соотношение 3 называют *основным рекуррентным* свойством числа сочетаний. Оно позволяет легко заполнить первые строчки следующей бесконечной таблицы (она называется треугольником Паскаля). Каждый элемент этой таблицы C_{n+1}^m равен сумме двух соседних элементов C_n^{m-1} и C_n^m, стоящих в предыдущей строке (если они есть).

Треугольник Паскаля
(нахождение C_n^m)

$_n\backslash^m$	0	1	2	3	4	5	6	7	8	9	10	...
0	1											
1	1	1										
2	1	2	1									
3	1	3	3	1								
4	1	4	6	4	1							
5	1	5	10	10	5	1						
6	1	6	15	20	15	6	1					
7	1	7	21	35	35	21	7	1				
8	1	8	28	56	70	56	28	8	1			
9	1	9	36	84	126	126	84	36	9	1		
10	1	10	45	120	210	252	210	120	45	10	1	
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Хорошо известно, что
$(x+y)^1 = 1\cdot x + 1\cdot y, \qquad (x+y)^2 = 1\cdot x^2 + 2\cdot xy + 1\cdot y^2,$
$(x+y)^3 = 1\cdot x^3 + 3\cdot x^2y + 3\cdot xy^2 + 1\cdot y^3.$

Коэффициенты в правых частях равенств совпадают с числами, стоящими в строчках треугольника Паскаля. Это справедливо и в общем случае. Формула следующей теоремы называется формулой *бинома Ньютона.*

Теорема 2.5.3.

$$(x+y)^n = C_n^0x^n + C_n^1x^{n-1}y + \ldots + C_n^mx^{n-m}y^m + \ldots + C_n^ny^n =$$

$$= \sum_{m=0}^{m=n} C_n^mx^{n-m}y^m.$$

Доказательство. Приведем два доказательства этой формулы. Первое будет комбинаторным, второе — по индукции.

1. Представим левую часть формулы в виде произведения n множителей и занумеруем скобки числами от 1 до n :

$$(x+y)^n = \underbrace{(x+y)}_{1}\underbrace{(x+y)}_{2}\cdot\ldots\cdot\underbrace{(x+y)}_{n}.$$

Определим количество слагаемых вида $x^{n-m}y^m$ после раскрытия скобок. Для этого рассмотрим произвольное сочетание по m элементов множества

$A = \{1, 2, \ldots, n\}$. Каждое такое сочетание однозначно определяет номера скобок, из которых выбирается y , из остальных выбирается x . Таким образом, каждому такому сочетанию соответствует одно слагаемое вида $x^{n-m}y^m$ и наоборот. Поэтому количество слагаемых $x^{n-m}y^m$ после раскрытия скобок будет равно C_n^m .

2. Индукция по n .

Б.И. Случай $n = 1$ очевиден.

Ш.И. Предположим, для $n = k$ это утверждение выполняется. Докажем для $n = k + 1$:

$$\begin{aligned}
&(x+y)^{k+1} = (x+y)^k(x+y) = \\
&= (C_k^0 x^k + C_k^1 x^{k-1} y + \ldots + C_k^m x^{k-m} y^m + \ldots + C_k^k y^k)(x+y) = \\
&= C_k^0 x^{k+1} + (C_k^0 + C_k^1) x^k y + \ldots + (C_k^{m-1} + C_k^m) x^{k-m+1} y^m + \ldots + C_k^k y^{k+1} = \\
&= C_{k+1}^0 x^{k+1} + C_{k+1}^1 x^k y + \ldots + C_{k+1}^m x^{k-m+1} y^m + \ldots + C_{k+1}^{k+1} y^{k+1}.
\end{aligned}$$

В последнем переходе мы использовали равенство $C_k^0 = C_{k+1}^0 = C_{k+1}^{k+1} = 1$ и рекуррентное свойство числа сочетаний.

■

Следствие 1.

$$(x-y)^n = C_n^0 x^n - C_n^1 x^{n-1} y + \ldots (-1)^m C_n^m x^{n-m} y^m + \ldots (-1)^n C_n^n y^n.$$

Доказательство. Достаточно заметить, что все слагаемые, в которых степень y нечетна, будут со знаком минус.

■

Следствие 2. *(4-е свойство числа сочетаний)*

$$C_n^0 - C_n^1 + C_n^2 - C_n^3 + \ldots (-1)^m C_n^m + \ldots (-1)^n C_n^n = 0.$$

Доказательство. Необходимо воспользоваться предыдущей формулой для бинома $(1-1)^n$.

■

Упражнения

62. Сравнивая коэффициенты при x^k в обеих частях равенства $(1+x)^m(1+x)^n = (1+x)^{n+m}$, доказать, что

$$C_n^k C_m^0 + C_n^{k-1} C_m^1 + \ldots + C_n^0 C_m^k = C_{m+n}^k.$$

63. Доказать, что сумма квадратов биномиальных коэффициентов равна C_{2n}^n (т.е. $\sum_{k=0}^n (C_n^k)^2 = C_{2n}^n$) .

64. Доказать, что

$$1 - 10C_{2n}^1 + 10^2 C_{2n}^2 - 10^3 C_{2n}^3 + \ldots - 10^{2n-1} C_{2n}^1 + 10^{2n} = (81)^n.$$

65. Упростить выражение $P_1 + 2P_2 + \ldots + nP_n$.

2.6 Перестановки и сочетания с повторениями

Название этого параграфа содержит противоречие: в перестановках и сочетаниях элементы не могут повторяться. Но для решения некоторых задач удобно использовать специальные конструкции, которые лучше называть именно таким образом. Рассмотрим примеры таких задач и затем введем необходимые определения.

П р и м е р 1. Сколько существует различных 5-буквенных слов, полученных перестановкой букв слова “потоп” (словом будем называть любой набор букв)? Сделаем несколько полезных замечаний. Порядок букв в словах важен, так, например, “потоп” это не то же самое, что “оптоп”. С другой стороны, “оптоп” и “оптоп” совпадают, хотя в них и переставлены местами две буквы “о”. Итак, порядок не важен, когда речь идет об одинаковых буквах, и важен в случае, если местами меняются разные буквы. Число всех таких различных 5-буквенных слов будем считать следующим образом: на пять пустых мест будем расставлять сначала буквы одного типа, затем другого и т.д. Количество способов расставить две буквы “о” на 5 пустых мест — это количество способов выбрать 2 места из 5, т.е. C_5^2 . На оставшиеся места для каждой такой расстановки будем размещать две буквы “п”(таких размещений — C_3^2) и, наконец, на оставшееся место поместим “т”(таких размещений — C_1^1). Итак, количество слов равно $C_5^2 \cdot C_3^2 \cdot C_1^1$ (перемножаем, так как для каждой расстановки после первого этапа мы образуем C_3^2 расстановок на втором этапе и т.д.).

Определение. *Пусть дано k_1 элементов 1-го типа, k_2 — 2-го, $\ldots, k_m$ — m-го типа. И $k_1 + k_2 + \ldots + k_m = n$. Тогда перестановкой из n элементов с повторениями $k_1, \ldots, k_m$ называются размещение с повторениями, в котором в точности k_1 элементов 1-го типа, k_2 — 2-го, $\ldots, k_m$ - m-го типа. $\overline{P}_n(k_1, \ldots, k_m)$ — количество всех таких перестановок.*

Так, в предыдущем примере два элемента 1-го типа (две буквы “о”), два элемента 2-го типа (две буквы “п”) и один элемент 3-го типа. Мы нашли, что $\overline{P}_5(2, 2, 1) = 30$.

Общий результат выглядит так:

Теорема 2.6.1.

$$\overline{P}_n(k_1, \ldots, k_m) = \frac{n!}{k_1! k_2! \cdot \ldots \cdot k_m!}.$$

Доказательство. Любую такую перестановку с заданным числом повторений можно получить следующим образом:

выбираем места для элементов 1-го типа — их $C_n^{k_1}$;

выбираем места для элементов 2-го типа из оставшихся — их $C_{n-k_1}^{k_2}$;

$$\vdots$$

выбираем места для элементов m-го типа из оставшихся — их $C_{k_m}^{k_m}$.

Число всех размещений равно

$$\overline{P}_n(k_1,\ldots,k_m) = C_n^{k_1}\cdot C_{n-k_1}^{k_2}\cdot\ldots\cdot C_{k_m}^{k_m} =$$

$$= \frac{n!(n-k_1)!(n-k_1-k_2)!\cdot\ldots\cdot k_m!}{k_1!(n-k_1)!k_2!(n-k_1-k_2)!\cdot\ldots\cdot k_m!k_m!(k_m!-k_m!)} =$$

$$= \frac{n!}{k_1!k_2!\cdot\ldots\cdot k_m!}.$$

■

Заметим только, что результат будет таким же, если вы будете сначала выбирать места для элементов 2-го типа и т.д.

Теперь о сочетаниях с повторениями. Снова начнем с примера.

П р и м е р 2. Предположим, что вы решили купить 5 (пять!) пирожных трех видов, которые есть в продаже. И предположим (это сделать уже сложнее), что у вас нет привязанности к пирожным какого-то определенного типа. Сколько существует различных вариантов выбора? Обозначим через A, B, C виды пирожных. Тогда могут быть такие варианты: $AAAAA$, $ABBBBB$ или $ABCCC$. Снова займемся наблюдениями. Порядок видов пирожных не важен, так, вариант $BABBB$ совпадает с $ABBBB$. Важно только количество пирожных данного типа. Поэтому по каждому выбору будем образовывать перестановку по следующему правилу: ставим k_1 единиц, если выбрано k_1 пирожных первого типа, затем ставим 0 (если пирожных первого типа нет, конечно, сразу ставим 0), далее ставим k_2 единиц, если выбрано k_2 пирожных второго типа, затем снова ставим ноль и, наконец, ставим столько единиц, сколько выбрано пирожных последнего типа. Для выборов выше это будут перестановки с повторениями (1111100), (1011110) и (1010111) соответственно. Итак, 5 единиц и 2 разделяющих нуля. И наоборот, по каждой такой перестановке можно восстановить выбор. Искомое число — $\overline{P}_7(5,2) = 21$.

Определение. *Сочетаниями из n различных типов по m элементов с повторениями называются неупорядоченные совокупности, состоящие из m элементов, каждый из которых принадлежит к одному из этих n типов.*

Число всех таких совокупностей будем обозначать через $\overline{C}_n^m$.

Теорема 2.6.2.
$$\overline{C}_n^m = C_{n+m-1}^m = C_{n+m-1}^{n-1}.$$

Доказательство. Покажем, что таких сочетаний с повторениями столько же, сколько и перестановок с повторениями из m единиц и $n-1$ нулей.

Построение взаимно однозначного соответствия приведено в примере 2. Отличие состоит только в том, что в общем случае будет m единиц и $n-1$ нулей, чтобы отделить один тип элементов от другого. Если сочетания различны, то хотя бы один из разделяющих нулей будет стоять на другой позиции. И наоборот, если один из нулей, скажем, i-го типа, следует после другого количества единиц, это сразу же означает, что выбрано неодинаковое количество элементов этого типа и сочетания получаются различными. Поэтому
$$\overline{C}_n^m = \overline{P}_{n+m-1}(m, n-1) = \frac{(n+m-1)!}{m!(n-1)!} = C_{n+m-1}^m.$$
Последнее равенство следует из второго свойства числа сочетаний.

■

Следуя комбинаторному доказательству формулы бинома Ньютона, можно получить формулу

$$(a_1 + a_2 + \ldots + a_m)^n = \sum_{k_1+\ldots+k_m=n} \overline{P}_n(k_1, k_2, \ldots, k_m) a_1^{k_1} a_2^{k_2} \cdot \ldots \cdot a_m^{k_m}.$$

Упражнения

66. Докажите последнюю формулу, занумеровав скобки и определив количество слагаемых вида $a_1^{k_1} a_2^{k_2} \cdot \ldots \cdot a_m^{k_m}$.

Глава 3

Бесконечные множества

3.1 Счетные множества

В этом параграфе мы начинаем изучение бесконечных множеств. Немного забегая вперед, сделаем на первый взгляд странное утверждение: бесконечные множества могут быть по-разному бесконечны. Поэтому мы начнем с самых маленьких из бесконечных — со счетных множеств. Напомним, что при определении конечных множеств мы пользовались начальными отрезками натурального ряда. Теперь нашим эталоном будет все множество натуральных чисел.

Определение. *Счетным множеством называется произвольное множество* A *, равномощное множеству* N *(как обычно, существует биекция* $A \xrightarrow{\varphi} N$ *).*

П р и м е р 1. Множество всех натуральных чисел, начиная с двойки, т.е. $N_{\geqslant 2} = \{n \in N : n \geqslant 2\}$, является счетным множеством. Одна из возможных биекций задается правилом: $\varphi(k) = k - 1, \quad k \in N_{\geqslant 2}$,

$$
\begin{array}{cccccccc}
2 & 3 & 4 & \dots & n & \dots & & N_{\geqslant 2} \\
\downarrow & \downarrow & \downarrow & \dots & \downarrow & \dots & & \\
1 & 2 & 3 & \dots & n-1 & \dots & & N
\end{array}
$$

П р и м е р 2. Множество всех четных натуральных чисел (N_2) также счетно. Биекцию можно задать, например, так: $\varphi(n) = 2n, \quad n \in N$.

$$
\begin{array}{cccccccc}
1 & 2 & 3 & \dots & n & \dots & & N \\
\downarrow & \downarrow & \downarrow & \dots & \downarrow & \dots & & \\
2 & 4 & 6 & \dots & 2n & \dots & & N_2
\end{array}
$$

Лемма 3.1.1. *Множество* A *счетно в том и только в том случае, когда его можно представить в виде* $A = \{a_1, a_2, \dots, a_n, \dots\}$ *, где* $a_i \neq a_j$ *для всех различных* $i, j \in N$ *.*

Доказательство. Действительно, если биекция $A \xrightarrow{\varphi} N$ существует, то, обозначив через $a_n = \varphi^{-1}(n)$, мы получим искомое представление.

Обратно, если такое представление задано, то биекцию можно задать правилом $\varphi(n) = a_n, \quad n \in N$.

■

Теорема 3.1.1. *Любое бесконечное подмножество множества N счетно.*

Доказательство. Пусть $A \subseteq N$ и A бесконечно. По индукции занумеруем элементы множества A .

Б.И. $n = 1$. Пусть a_1 — минимальный элемент множества A . Его можно найти, так как в любом непустом подмножестве N найдется минимальный элемент. Заметим, что $a_1 \geqslant 1$.

Ш.И. Пусть для $n = k$ выбраны $a_1, a_2, \ldots, a_k \in A$ так, что выполняются следующие свойства:
1) $a_1 < a_2 < \ldots < a_k$;
2) $a_i \geqslant i$ для любого $i \leqslant k$;
3) каждый элемент множества $A \backslash \{a_1, a_2, \ldots, a_k\}$ больше любого из a_1 , $a_2, \ldots$, a_k .

В качестве элемента a_{k+1} выберем минимальный элемент множества $A \backslash \{a_1, a_2, \ldots, a_k\}$. Он найдется в силу бесконечности множества A . Так как выполняется свойство 3 предположения индукции, то $a_{k+1} > a_k \geqslant k \Rightarrow a_{k+1} \geqslant k+1$. И, наконец, третье свойство уже для a_{k+1} выполняется в силу минимальности элемента a_{k+1} в множестве $A \backslash \{a_1, a_2, \ldots, a_k\}$. Итак, мы получили некоторое множество $\{a_1, a_2, \ldots, a_n, \ldots\}$. Покажем, что это множество совпадает со множеством A . Достаточно доказать, что для любого $a \in A$ следует, что $a \in \{a_1, a_2, \ldots, a_n, \ldots\}$. О/п. Пусть существует $a \in A$, что $a \notin \{a_1, a_2, \ldots, a_n, \ldots\}$. Заметим, что $a = m$ для некоторого $m \in N$. Тогда $a = m \leqslant a_m$. С другой стороны, из третьего свойства следует, что $a \in A \backslash \{a_1, a_2, \ldots, a_m\} \Rightarrow a > a_m$. ⤫ .

Поэтому $A = \{a_1, a_2, \ldots, a_n, \ldots\}$. По предыдущей лемме A — счетное множество.

■

Следствие 1. *Множество простых чисел счетно.*

Следствие 2. *Множество $N_m = \{m^n : n \in N\}$, где $m \in N$ счетно, если $m \neq 1$.*

Следствие 3. *Любое бесконечное подмножество B счетного множества A счетно.*

Доказательство. Пусть $B \subseteq A$ и B — бесконечно. Так как $A \sim N$, то существует биекция $A \xrightarrow{\varphi} N$. Тогда $\varphi(B)$ — бесконечное подмножество N. По предыдущей теореме оно счетно. Следовательно, $B \sim \varphi(B) \sim N$. Поэтому B — счетное множество.

■

В следующей теореме используется операция счетного объединения. До сих пор мы объединяли не более чем конечное число множеств. Пусть теперь дано счетное число множеств $A_1, A_2, \ldots, A_n, \ldots$. Тогда

$$\cup_{n=1}^{\infty} A_n = \{a : a \in A_n \text{ хотя бы для одного } n \in N\}.$$

Например, $\cup_{n=1}^{\infty}\{n\} = N$ или $\cup_{n=1}^{\infty} N_{\leqslant n} = N$. Оказывается, счетные объединения не выводят из класса счетных множеств, т.е., объединяя в счетном числе счетные множества, всегда будет получаться счетное множество.

Теорема 3.1.2. *Счетное объединение счетных множеств счетно.*

Доказательство. Пусть $A_1, A_2, \ldots, A_n, \ldots$ — счетные множества.

Рассмотрим случай, когда эти множества попарно не пересекаются. Выше определялись множества N_m. Мы будем рассматривать множества N_{p_n}, где p_n — n-е по счету простое число. Заметим, что множества N_{p_i} и N_{p_j} попарно не пересекаются при $i \neq j$. Иначе $(p_i)^k = (p_j)^l$ при некоторых $k, l \in N$, но правая и левая части этого равенства имеют различные делители.

Так как множества A_n и N_{p_n} счетны, то существует биекция $\varphi_n : A_n \longrightarrow N_{p_n}$. Определим теперь биекцию $\varphi : \cup_{n=1}^{\infty} A_n \longrightarrow \cup_{n=1}^{\infty} N_{p_n}$ следующим образом:

$$\text{если } a \in A_n, \text{ то } \varphi(a) = \varphi_n(a).$$

Множество $\cup_{n=1}^{\infty} N_{p_n}$ счетно как бесконечное подмножество N. Следовательно, $\cup_{n=1}^{\infty} A_n$ также счетно.

Теперь рассмотрим общий случай, когда A_i и A_j могут пересекаться между собой. Тогда рассмотрим множества $B_1 = A_1, B_2 = A_2 \backslash A_1, \ldots, B_n = A_n \backslash (\cup_{k=1}^{n-1} A_k)$. Заметим, что

- $\cup_{n=1}^{\infty} A_n = \cup_{n=1}^{\infty} B_n$,
- $\cup_{n=1}^{\infty} B_n$ — бесконечно,
- B_i и B_j при различных i и j между собой не пересекаются.

Снова будем рассматривать отображения φ_n, определенные выше, но уже для B_n. Если некоторое B_n окажется конечным, то φ_n — взаимно однозначное отображение B_n в N_{p_n} (если $B_n = \varnothing$, то и $\varphi_n = \varnothing$). В результате φ также будет взаимно однозначным отображением $\cup_{n=1}^{\infty} B_n$ в $\cup_{n=1}^{\infty} N_{p_n}$.

Следовательно, φ — это биекция между $\cup_{n=1}^{\infty} B_n$ и $\varphi(\cup_{n=1}^{\infty} B_n)$. Множество $\varphi(\cup_{n=1}^{\infty} B_n)$, как бесконечное подмножество N, счетно. Следовательно, $\cup_{n=1}^{\infty} A_n = \cup_{n=1}^{\infty} B_n$ — счетное множество.

■

Следствие 1. *Множество целых чисел Z счетно.*

Доказательство. Действительно, $Z = N \cup \{-n : n \in N\} \cup \{0\}$, т.е. это объединение двух счетных множеств и конечного множества.

■

Следствие 2. *Множество пар $Z_n = \{(k, n) : k \in Z\}$ счетно, где $n \in N$.*

Доказательство. Каждое из этих множеств равномощно с Z, так как n фиксировано.

■

Следствие 3. *Множество рациональных чисел Q счетно.*

Доказательство. Любое рациональное число можно представить в виде упорядоченной пары (k, n), где $k \in Z, \quad n \in N$. Следовательно, $Q \subseteq \subseteq \cup_{n=1}^{\infty} Z_n$. Множество Q является счетным объединением счетных множеств.

■

Следствие 4. *Множество чисел на плоскости с обеими рациональными координатами, т.е. множество $Q \times Q$, счетно.*

Доказательство. $Q \times Q = \cup_{r \in Q} (Q \times \{r\})$. В этом равенстве справа стоит счетное объединение счетных множеств.

■

Ранее количество элементов в конечных множествах мы обозначали через $|A| = n$, где n — натуральное число. Для обозначения мощности бесконечных множеств используют бесконечные кардинальные числа. Так, мощность N равна $\aleph_0$ (алеф-ноль). По аналогии с предыдущими обозначениями будем записывать $|N| = \aleph_0$. В следующем параграфе выяснится, что счетные множества не являются единственными представителями класса бесконечных множеств, то есть существуют другие кардинальные числа.

Упражнения

67. Можно ли определение φ в теореме 3.1.2 заменить определением

$$\varphi = \cup_{n=1}^{\infty} \varphi_n \ ?$$

3.2 Несчетные множества

Биекции между счетными множествами часто задаются с помощью формул. Приведем примеры других способов описаний биекций. Интервал от 0 до 1 равномощен вещественной прямой R ($(0;1) \sim R$). Доказать это утверждение можно в два этапа: установить равномощность интервала и дуги окружности (без концевых точек), на рис. 12 это делается с помощью биекции ψ, и равномощность последней с вещественной прямой (биекция φ) доказывается с помощью проектирования из центра этой окружности. Композиция этих биекций будет искомой биекцией.

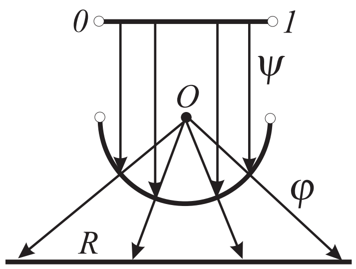

Рис. 12

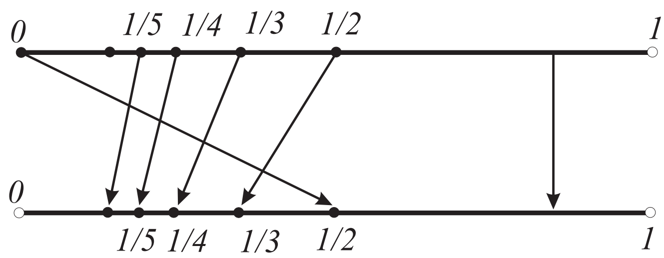

Рис. 13

Сложнее построить биекцию между полуинтервалом $[0\ 1)$ и интервалом $(0;1)$. Для этого выберем счетное множество $A = \{1/n : n \in N, n \geqslant 2\}$. Заметим, что $A \subseteq (0;1) \subseteq [0;1)$. Зададим биекцию между отрезком и интервалом следующим образом (рис. 13):

$$\varphi(x) = \begin{cases} 1/2, & x = 0, \\ 1/(n+1), & x = 1/n, \\ x, & \text{во всех остальных случаях.} \end{cases}$$

Этой идеей мы воспользуемся при доказательстве следующей теоремы.

Лемма 3.2.1. *В любом бесконечном множестве X существует счетное подмножество.*

Доказательство. Пусть X бесконечно. Будем строить два счетных непересекающихся подмножества A и B по индукции.

Б.И. $n = 1$. Пусть a_1 — произвольный элемент множества X, а b_1 — произвольный элемент из $X \backslash \{a_1\}$.

Ш.И. Предположим, что уже выбраны различные $a_1, \ldots, a_k$, $b_1, \ldots, b_k$. Тогда множество $X \backslash \{a_1, \ldots, a_k,\ b_1, \ldots, b_k\}$ бесконечно и поэтому содержит по крайней мере два различных элемента. Один из них мы обозначим через a_{k+1}, другой — через b_{k+1}.

В результате мы получим два непересекающихся счетных множества: $A = \{a_1, \ldots, a_n, \ldots\}$ и $B = \{b_1, \ldots, b_n, \ldots\}$.

■

Кроме того, что мы нашли счетное подмножество в X (например, A), мы показали, что его можно выбрать так, чтобы $X \setminus A$ продолжало оставаться бесконечным.

Теорема 3.2.1. *Если X бесконечно и Y — конечно или счетно, то $X \cup Y \sim X$.*

Доказательство. 1. Пусть пересечение $X \cap Y = \varnothing$ (рис. 14). Тогда, пользуясь предыдущей леммой, выделим счетное подмножество $A \subseteq X$. Множество $A \cup Y$ счетно, поэтому существует биекция $\varphi : (A \cup Y) \longrightarrow A$. Теперь опишем биекцию между $X \cup Y$ и X. Пусть

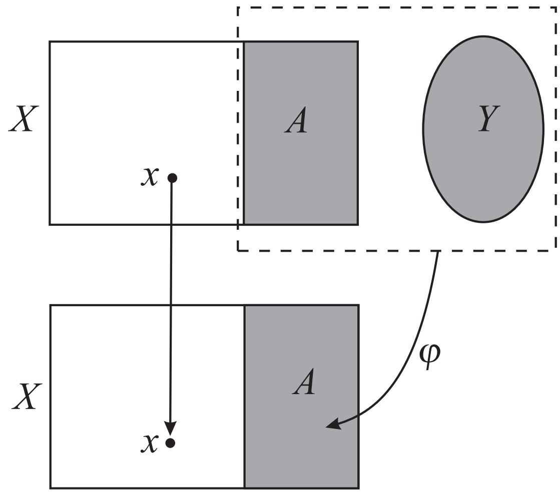

Рис. 14

$$\psi(x) = \begin{cases} \varphi(x), & \text{если } x \in (A \cup Y), \\ x, & \text{в остальных случаях.} \end{cases}$$

2. Если $X \cap Y \neq \varnothing$, то заметим, что $X \cup Y = X \cup Y_1$, где $Y_1 = Y \setminus X$. Осталось применить первый случай к Y_1 и X.

■

Определение. *Если существует взаимно однозначное отображение множества X на подмножество из Y, будем писать $|X| \leqslant |Y|$ (мощность X не превосходит мощности Y). Если при этом не существует взаимно однозначного отображения X на все Y, будем писать $|X| < |Y|$ (мощность X строго меньше мощности Y). Если существует биекция между X и Y, тогда будем использовать обозначение $|X| = |Y|$ (мощности множеств X и Y совпадают).*

Так, если A — счетное множество, то $|A| = |N| = \aleph_0$. Кроме того, из леммы следует, что для любого бесконечного X выполняется $|N| \leqslant |X|$.

Каждое ли бесконечное множество является счетным? Оказывается, нетрудно получить множество строго большей мощности. Кантор заметил, что операция взятия множества всех подмножеств всегда приводит к образованию множества строго большей мощности.

Теорема (Кантор) 3.2.2. *Для любого множества X выполняется неравенство $|\mathcal{P}(X)| > |X|$.*

Доказательство. Нам необходимо проверить, что существует взаимно однозначное отображение X в $\mathcal{P}(X)$ и при этом между ними не существует биекции.

1. Пусть $\varphi(x) = \{x\}, \quad x \in X$. Тогда φ —взаимно однозначно отображает X на множество $\{\{x\} : x \in X\}$. Последнее содержится в $\mathcal{P}(X)$.

2. Покажем, что любое отображение из X не является отображением на $\mathcal{P}(X)$ (т. е. нет ни одного сюръективного отображения, тем более не существует биекции). Возьмем произвольное отображение $f : X \longrightarrow \mathcal{P}(X)$. Это отображение ставит в соответствие элементам множества X некоторые подмножества X , которые являются элементами $\mathcal{P}(X)$. Найдем множество A , которое не поставлено в соответствие ни одному элементу из X . Определим его так:

$$A = \{x \in X : x \notin f(x)\}.$$

Покажем, что оно искомое.

О/п. Пусть существует $x_0 \in X$, что $f(x_0) = A \in \mathcal{P}(X)$. Возможны два случая: $x_0 \in A$ или $x_0 \notin A$.

а) Пусть $x_0 \in A \Rightarrow x_0 \notin f(x_0) \Rightarrow x_0 \notin A$. $\times$.

б) Пусть теперь $x_0 \notin A \Rightarrow x_0 \notin f(x_0) \Rightarrow x_0 \in A$. $\times$.

Итак, отображение f не является отображением “на”, поэтому не может быть биекцией.

■

Следствие. $\aleph_0 = |N| < |\mathcal{P}(N)|$.

Определение. $c = |\mathcal{P}(N)|$. *Кардинальное число c называют мощностью континуума.*

Определение. $2^{\aleph_0} = |\{0,1\}^N|$, *т.е. кардинальное число $2^{\aleph_0}$ является мощностью множества всех отображений из N в двухэлементное множество $\{0,1\}$.*

Лемма 3.2.2. $c = 2^{\aleph_0}$.

Доказательство. Достаточно доказать, что множества $\mathcal{P}(N)$ и $\{0,1\}^N$ равномощны. Построим биекцию между ними. Пусть A — произвольное подмножество из N , тогда обозначим через f_A такое отображение:

$$f_A(n) = \begin{cases} 1, & \text{если } n \in A; \\ 0, & \text{если } n \notin A. \end{cases}$$

Тогда искомой биекцией будет $\varphi(A) = f_A$. Соответствие φ всюду определено и взаимно однозначно. Покажем, что оно сюръективно. Для произвольного $f \in \{0,1\}^N$ образуем такое множество $A = \{n \in N : f(n) = 1\}$. Тогда $f_A = f \Rightarrow \varphi(A) = f$.

$\blacksquare$

Следующие две теоремы отвечают на вопрос: какова же мощность R . Первая из них утверждает, что R несчетно. Метод, который используется при доказательстве этой теоремы, называется *диагональным методом Кантора.* Вторая теорема уточняет результат первой теоремы: множества R и $\mathcal{P}(N)$ равномощны.

Теорема (Кантор) 3.2.3. $|R| > |N|$.

Доказательство. О/п. Предположим, что R счетно. Тогда и интервал $(0;1)$ счетен, поэтому $(0;1)$ можно представить в виде $\{a_1, a_2, \ldots, a_n, \ldots\}$. Каждое вещественное число a_n запишем в виде бесконечной десятичной дроби $a_n = 0, a_1^n a_2^n \ldots a_n^n \ldots$. Получим следующее представление:

$$\begin{gathered} a_1 = 0, a_1^1 a_2^1 \ldots a_n^1 \ldots \\ a_2 = 0, a_1^2 a_2^2 \ldots a_n^2 \ldots \\ \vdots \\ a_n = 0, a_1^n a_2^n \ldots a_n^n \ldots \\ \vdots \end{gathered}$$

Покажем, что среди выписанных чисел нет по крайней мере одного числа $a^* = 0, a_1^* a_2^* \ldots a_n^* \ldots$ из $(0\ \ 1)$. Определим его десятичные знаки следующим образом: $a_1^* \in \{4,5\} \backslash \{a_1^1\}$; $a_2^* \in \{4,5\} \backslash \{a_2^2\}; \ldots$ $a_n^* \in \{4,5\} \backslash \{a_n^n\}; \ldots$ Первая цифра после запятой отличает a^* от a_1 , вторая — от a_2 , от a_n число a^* отличается n -й цифрой после запятой, поэтому $a \notin (0;1) = \{a_1, a_2, \ldots, a_n, \ldots\}$. С другой стороны, числа a_i^* выбираются так, что не может получиться 0 и 9 в периоде, поэтому $a^* \in (0;1)$. $\nwarrow\!\!\!\!\!\nearrow$.

$\blacksquare$

Теорема 3.2.4. $|R| = c$.

Доказательство. В начале этого параграфа мы показали, что $[0;1) \sim (0;1) \sim R$. Поэтому достаточно доказать, что $|[0;1)| = c$.

Каждому числу из $[0;1)$ однозначно можно поставить в соответствие его двоичное представление вида $0, b_1 b_2 \ldots b_n \ldots$, $b_i \in \{0,1\}$ для любого $i \in N$ (договоримся, что не может быть бесконечного периода из единиц, начиная с некоторого места). Но каждому такому представлению однозначно соответствует отображение $f \in \{0,1\}^N$ такое, что

$$f(n) = \begin{cases} 1, & \text{если } b_n = 1; \\ 0, & \text{если } b_n = 0. \end{cases}$$

Обозначим множество всех отображений, которые соответствуют числам из $[0;1)$, через X, и через Y — множество $\{0,1\}^N \backslash X$. Для каждого $f \in Y$ найдется такое натуральное число $n \in N$, что $f(i) = 1$ для всех $i \geqslant n$, т.е. отображение f принимает значение 1, начиная с n. Теперь легко доказать счетность множества Y. Действительно, различных отображений, принимающих значение 1, начиная с n, только конечное число (их не более 2^n). Поэтому Y является счетным объединением конечных множеств. Следовательно, Y счетно или конечно. Уже доказано, что $[0;1) \sim X$, теперь же по теореме 3.2.1 получаем, что

$$|R| = |[0;1)| = |X| = |X \cup Y| = |\{0,1\}^N| = |\mathcal{P}(N)| = c.$$

■

Упражнения

68. Доказать, что соответствия φ и ψ, с помощью которых строилась биекция между интервалом $(0;1)$ и R в начале этого подраздела, являются биекциями.

3.3 Теорема Кантора–Бернштейна

В предыдущем параграфе было определено отношение $|X| \leqslant |Y|$ (существует биекция множества X на некоторое подмножество из Y). Очевидно, что $|X| \leqslant |X|$. Если $|X| \leqslant |Y|$ (φ — биекция, отображающая X на подмножество из Y) и $|Y| \leqslant |Z|$ (ψ — биекция, отображающая Y на подмножество из Z), то $\psi \circ \varphi$ взаимно однозначно отображает X на некоторое подмножество Z, следовательно, $|X| \leqslant |Z|$. Предположим теперь, что существует биекция X на подмножество из Y и, наоборот, существует биекция Y на подмножество из X (т.е. $|X| \leqslant |Y|$, и $|X| \leqslant |Y|$), можно ли в этом случае построить биекцию уже между множествами X и Y (т.е. $|X| = |Y|$)? Утвердительный ответ на этот вопрос, впервые поставленный Г. Кантором, был дан его учеником Феликсом Бернштейном зимой 1896-1897г.

Теорема(Кантор–Бернштейн) 3.3.1. *Если существует взаимно однозначное отображение A в B и, наоборот, из B в A, то между A и B можно построить биекцию.* ($|A| \leqslant |B|$ *и* $|A| \geqslant |B| \Rightarrow |A| = |B|$).

Доказательство. Рассмотрим сначала частный случай теоремы.

1. Пусть $B \subseteq (A \backslash A_1)$ и $A \sim A_1$ (рис. 15). Докажем, что $(B \cup A_1) \sim A_1$. Так как $A \sim A_1$, то существует биекция $f : A \longrightarrow A_1$. Построим биекцию между $(B \cup A_1)$ и A_1. Введем некоторые обозначения. Пусть $B_0 = B$, $B_1 = f(B)$. В общем случае $B_{i+1} = f(B_i)$.

Заметим, что $B \subseteq A \Rightarrow B_1 = f(B) \subseteq f(A) = A_1$. Покажем сначала, что B_i и B_j при разных значениях i и j не пересекаются. $B_0 \subseteq (A \backslash A_1)$ и $B_1 \subseteq A_1 \Rightarrow B_0 \cap B_1 = \varnothing$. Теперь предположим, что для любых $i < j < n \Rightarrow B_i \cap B_j = \varnothing$. Покажем, что $B_j \cap B_n = \varnothing$. По предположению $B_{j-1} \cap B_{n-1} = \varnothing$. По свойству биекции для любых $C \cap D = \varnothing \Rightarrow f(C) \cap f(D) = \varnothing$. Поэтому $f(B_{j-1}) \cap f(B_{n-1}) = \varnothing$. Но $f(B_{j-1}) = B_j$ и $f(B_{n-1}) = B_n \Rightarrow B_j \cap B_n = \varnothing$.

Теперь опишем искомую биекцию:

$$\varphi(x) = \begin{cases} f(x), & \text{если } x \in B_i, \text{ для некоторого } i \in N \cup \{0\}; \\ x, & \text{в остальных случаях.} \end{cases}$$

На рис. 15 темные места множества $B \cup A_1$ соответствуют точкам, которые переходят сами в себя (т.е. остаются неподвижными), светлые множества B_i переходят последовательно друг в друга. Покажем, что φ является биекцией между $B \cup A_1$ и A_1. Очевидно, что φ всюду определено. Так как f, являясь биекцией, отображает множество B_i на множество B_{i+1} и

$$A_1 = (A_1 \backslash \cup_{i=1}^{\infty} B_i) \cup (\cup_{i=1}^{\infty} B_i),$$

то φ сюръективно. Однозначность следует из однозначности f и того факта, что выполняется в точности одно из двух условий: $x \in B_i$ для некоторого $i \in N \cup \{0\}$ или нет. Немного сложнее проверить инъективность (разным $x, y \in B \cup A_1$ соответствуют разные $\varphi(x), \varphi(y) \in A_1$). Пусть $x, y \in B \cup A_1, \quad x \neq y$, тогда возможны четыре случая:

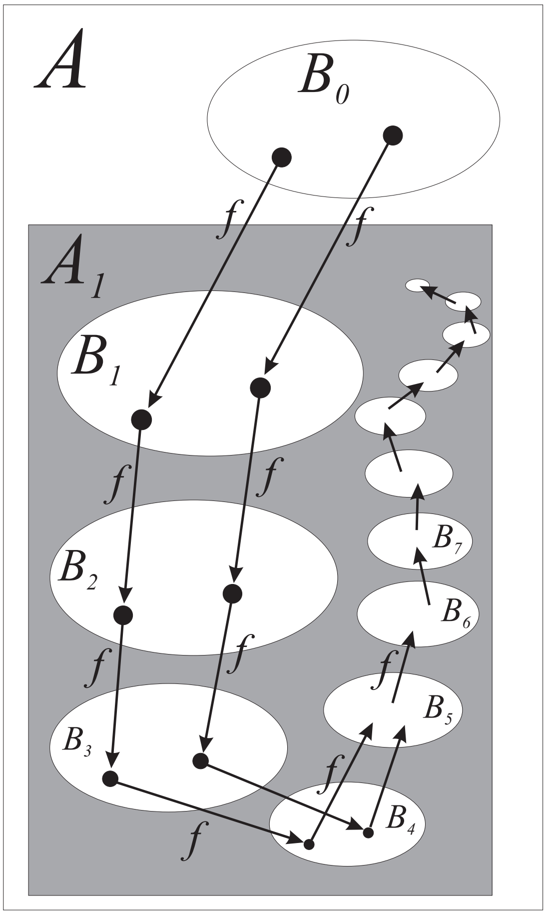

Рис. 15

1. x, y принадлежат темной (неподвижной) части (т.е. $x, y \notin B_i$ для любого $i \in N \cup \{0\}$), тогда $\varphi(x) = x \neq y = \varphi(y)$.

2. Один из них, например, x, принадлежит темной части, другой — одному из B_i, тогда $\varphi(y)$ принадлежит следующему светлому множеству — B_{i+1}, а $\varphi(x) = x \ \Rightarrow \varphi(x) \neq \varphi(y)$.

3. x, y принадлежат различным светлым множествам B_i и B_j, тогда $\varphi(x), \varphi(x)$ также принадлежат различным светлым множествам — B_{i+1} и B_{j+1}. Следовательно $\varphi(x) \neq \varphi(y)$.

4. x, y принадлежат одному светлому множеству B_i. Так как f — биекция, то $\varphi(x) \neq \varphi(y)$.

Все свойства биекции проверены.

2. Докажем теперь, что все промежуточные множества между двумя равномощными множествами им равномощны. Пусть $A_1 \subseteq \subseteq B \subseteq A$ и $A \sim A_1$. Тогда $B = (B \backslash A_1) \cup A_1$ и по предыдущему случаю $B \sim A_1 \sim A$.

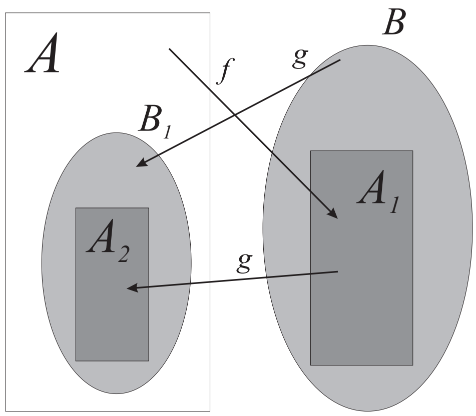

Рис. 16

3. Перейдем к доказательству общего случая. Пусть теперь $A \sim f(A) = A_1 \subseteq B$ и $B \sim g(B) = B_1 \subseteq A$, где f и g — биекции на соответствующие подмножества (рис. 16). Тогда $A \sim A_1 \sim g(A_1) = A_2$ и $A_2 \subseteq B_1$.

Применяя второй случай для множеств A, B_1, A_2, получаем, что существует биекция φ между A и B_1. Следовательно, $g^{-1} \circ \varphi$ — искомое взаимно однозначное отображение A на B.

■

Следствие 1. $(0;1] \sim (0;1)$.

Доказательство. $(0;1] \sim (0;\frac{1}{2}] \subseteq (0;1)$ ($f(x) = \frac{1}{2}x$ — биекция между $(0;1]$ и $(0;\frac{1}{2}]$). С другой стороны, $(0;1) \subseteq (0;1]$, и остается применить предыдущую теорему. Заметим, что каждое B_i состоит только из одной точки: $B_0 = 1$, $B_1 = \frac{1}{2}$, $B_i = \frac{1}{i+1}$. Если строить биекцию между $[0;1]$ и $(0;1)$, то каждое B_i будет состоять из двух точек.

■

Используя проектирование и центральное проектирование (см. начало предыдущего параграфа), можно показать, что круг без границы равномощен полусфере без ограничивающей окружности; последняя, в свою очередь, равномощна плоскости (предлагаем повращать рис. 12 относительно прямой, проходящей через точку О и перпендикулярной к прямой R).

Следствие 2. *Квадрат без границы равномощен кругу без ограничивающей окружности.*

Доказательство. Пусть A — квадрат без границы и B — круг без ограничивающей окружности. Тогда существует круг без границы $B_1 \subseteq A$. Так как $B_1 \sim B \Rightarrow |B| \leqslant |A|$. Аналогично в B содержится некоторый квадрат без границы A_1 (при этом $A_1 \sim A \Rightarrow |A| \leqslant |B|$). По теореме Кантора–Бернштейна $|A| = |B|$.

■

Следствие 3. *Квадрат без границы* $(0;1) \times (0;1)$ *равномощен интервалу* $(0;1)$.

Доказательство. Очевидно, что $|(0;1)| \leqslant |(0;1)\times(0;1)|$ (так как $(0;1) \sim \sim \{\frac{1}{2}\} \times (0;1)$).

Построим биекцию $(0;1) \times (0;1)$ на некоторое подмножество интервала $(0;1)$. Пусть $(x, y) \in (0;1) \times (0;1)$. Рассмотрим представление x и y в виде бесконечных десятичных дробей: $x = 0, x_1x_2\ldots$ и $y = 0, y_1y_2\ldots$ Зададим теперь отображение следующим образом: $f((x, y)) = z = 0, x_1y_1x_2y_2\ldots$ Это отображение ставит в соответствие число, у которого после запятой на нечетных местах стоят десятичные знаки x, а на четных — десятичные знаки y. Если $(x, y) \neq (x', y')$, то они различаются хотя бы по одной координате, значит, десятичные представления этих координат отличаются в некотором десятичном разряде, следовательно, $z \neq z'$. Итак, f — взаимно однозначное отображение $(0;1) \times (0;1)$ в $(0\ 1)$.

По теореме Кантора–Бернштейна $(0;1) \times (0;1) \sim (0;1)$.

■

Следствие 4. **(Кантор)** $|R| = |R \times R|$.

Доказательство. $R \sim (0;1) \sim (0;1) \times (0;1) \sim$ (кругу без границы) $\sim \sim$ (полусфере без ограничивающей окружности) $\sim R \times R$.

■

Предыдущий результат фактически означает следующее: на прямой и на плоскости одинаковое количество точек.

Упражнения

69. Сравните доказательства того факта, что $[a;b) \sim (a;b)$, приведенные в этом и предыдущем параграфах.

70. Докажите, что любые два круга равномощны.

71. Является ли отображение f, построенное в доказательстве следствия 3, биекцией квадрата без границы на интервал?

72. Докажите, что точек в пространстве столько же, сколько их на прямой.

73. Докажите, что если $X \sim Y$ и X, Y — бесконечные множества, то $X \cup Y \sim X$.

74. Справедлив ли предыдущий результат для пересечения множеств?

75. Докажите, что $R^n \sim R$ для любого $n \in N$.

76. Докажите, что если для любого $n \in N$ выполняется $X_n \sim Y$ и X, Y — бесконечные множества, то $\cup_{n=1}^{\infty} X_n \sim Y$.

77. Докажите, что $\cup_{n=1}^{\infty} R^n \sim R$.

3.4 Отношения на множестве. Отношения порядка и отношения эквивалентности

Соответствие может устанавливать связи между элементами разных множеств A и B , а может связывать между собой элементы одного и того же множества, т.е. когда $B = A$. В последнем случае такое соответствие принято называть отношением на множестве A .

Определение. *Отношением ρ на множестве A называют произвольное подмножество декартового квадрата $A \times A$ (т.е. $\rho \subseteq A \times A$). Если $(x, y) \in \rho$, будем использовать обозначение $x \ \rho \ y$ (x и y находятся между собой в отношении ρ)* [9].

Так, например, любое отношение на множестве вещественных чисел является подмножеством плоскости $R \times R$. Изображение этого подмножества называют *графиком* отношения. Таким образом, отношение на множестве R и его график означают одно и то же множество плоскости.

Рассмотрим некоторые примеры отношений и их графиков.

П р и м е р 1. $\rho \subseteq P \times P$, где P — множество всех людей. Отношение ρ зададим так: $a \ \rho \ b \Leftrightarrow$ когда дни рождения a и b совпадают.

П р и м е р 2. $\rho \subseteq N \times N$. Пусть $n \ \rho \ m \Leftrightarrow$ когда n делит m . Это отношение делимости на множестве N .

П р и м е р 3. $\rho \subseteq N \times N$. Пусть $n \ \rho \ m \Leftrightarrow$ когда $n \equiv m \pmod{k}$. Это отношение означает “быть сравнимыми между собой по модулю $k \in N \backslash \{1\}$ ”.

П р и м е р 4. $\rho \subseteq R \times R$. $x \ \rho \ y \Leftrightarrow y = kx + b$. График этого отношения — прямая $y = kx + b$ (рис. 17).

П р и м е р 5. $\rho \subseteq R \times R$. $x \ \rho \ y \Leftrightarrow x^2 + (y-4)^2 = 4$. График этого отношения — окружность с центром в (0,4) и радиусом 2 (рис. 17).

П р и м е р 6. $\rho \subseteq R \times R$. $x \ \rho \ y \Leftrightarrow (x+4)^2 + y^2 \leqslant 1$. График этого отношения — круг с центром в $(-4, 0)$ и радиусом 1 (рис. 17).

---

[9] Греческая буква ρ читается как “ро”.

П р и м е р 7. $\rho \subseteq R \times R$. Зададим его с помощью некоторой фигуры Φ на плоскости. $x \ \rho \ y \Leftrightarrow (x, y) \in \Phi$. Графиком этого отношения будет в точности эта фигура Φ (рис. 17).

П р и м е р 8. $\rho \subseteq L \times L$, где L — множество всех прямых на плоскости или в пространстве. Пусть $a, b \in L$, $a \ \rho \ b \Leftrightarrow$ когда прямые a и b между собой параллельны. Будем считать по определению, что совпадающие прямые также параллельны.

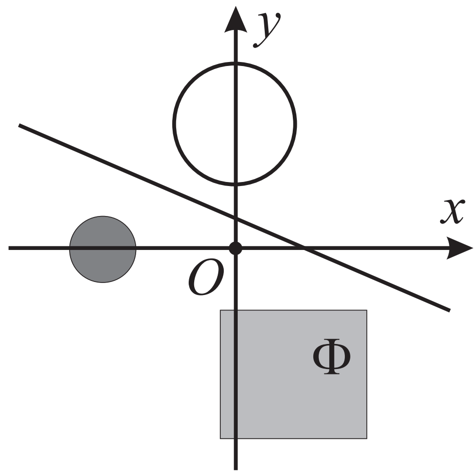

Рис. 17

П р и м е р 9. $\rho \subseteq T \times T$. Где T — множество всех треугольников на плоскости. Пусть $\triangle ABC, \triangle DEF \in T$, $\triangle ABC \ \rho \ \triangle DEF \Leftrightarrow$ когда треугольники $\triangle ABC$ и $\triangle DEF$ подобны.

П р и м е р 10. $\rho \subseteq \mathcal{P}(X) \times \mathcal{P}(X)$, где X — некоторое множество. Пусть $A, B \subseteq X$. Тогда $A \rho B \Leftrightarrow A \subseteq B$.

Среди огромного числа отношений на множестве A мы выделим несколько важных типов:

1) ρ рефлексивно, если $a \ \rho \ a$ для любых $a \in A$,

2) ρ симметрично, если $a \ \rho \ b \Rightarrow b \ \rho \ a$,

3) ρ антисимметрично, если $a \ \rho \ b$ и $b \ \rho \ a \Rightarrow a = b$,

4) ρ транзитивно, если $a \ \rho \ b$ и $b \ \rho \ c \Rightarrow a \ \rho \ c$,

5) ρ — отношение порядка, если оно рефлексивно, антисимметрично и транзитивно,

6) ρ — отношение эквивалентности, если оно рефлексивно, симметрично и транзитивно.

Примеры 1, 3, 8 и 9 являются примерами отношений эквивалентности. Скажем, в примере 3, если n, m и m, l дают одинаковые остатки при делении на k, то n и l также дают одинаковые остатки при делении на k. Поэтому отношение сравнения по модулю k транзитивно. Также легко проверить остальные свойства для этого и других отношений.

Отношение, определенное в примере 2, является отношением порядка. Очевидно, что n делит n. Если n делит m и m делит n, то они совпадают. И, наконец, если n делит m и m делит l, то n делит l. Поэтому выполняются соответственно свойства рефлексивности, антисимметричности и транзитивности для данного отношения.

Отношение порядка будем обозначать с помощью $\leqslant$ или $\preceq$. Часто к свойствам порядка добавляется четвертое свойство — любые два элемента $a, b \in A$ можно сравнить между собой.

Определение. *Отношение порядка* $\leqslant$ *называется отношением линейного порядка, если для любых* $a, b \in A$ *выполняется* $a \leqslant b$ *или* $b \leqslant a$.

Порядок в примере 2 не является линейным — уже для 2 и 3 не выполняется ни утверждение "два делит три", ни "три делит два". Примерами линейных порядков являются отношения $\leqslant$ на множествах натуральных, целых, вещественных чисел.

Определение. *Множество* A *вместе с отношением порядка* $\leqslant$ *на этом множестве мы будем обозначать* $(A, \leqslant)$. *Пусть* $B \subseteq A$. *Тогда* $a_0 \in B$ *называют наименьшим (соответственно наибольшим) в* B , *если для любых* $b \in B$ *выполняется неравенство* $a_0 \leqslant b$ ($b \leqslant a_0$). *Элемент* $a_0 \in B$ *называют минимальным (соответственно максимальным) в* B , *если для любых* $b \in B, b \leqslant a_0$ ($b \in B, a_0 \leqslant b$) *выполняется* $b = a_0$ ($b = a_0$).

Быть наименьшим или наибольшим элементом — это более сильное свойство, чем быть просто минимальным или максимальным элементом. Так, в двухэлементном множестве $A = \{a, b\}$, с очень бедным порядком $\leqslant = \{(a, a),\ (b, b)\}$ (свойства порядка легко проверяются), a и b являются одновременно максимальными и минимальными элементами по очень простой причине: нет элементов в A больших или меньших их. Но ни один из них не является наибольшим или наименьшим элементом — для этого они должны быть больше или меньше другого, а это не так. Во множествах с линейным порядком, где любые два элемента сравнимы между собой, соответствующие пары терминов означают одно и то же.

Определение. *Отношение линейного порядка на множестве* A *называется отношением полного порядка, если в любом его непустом подмножестве* $B \subseteq A$ *найдется минимальный элемент. Множество с полным порядком на нем называют вполне упорядоченным множеством.*

$(N, \leqslant)$ — пример вполне упорядоченного множества. В любом непустом подмножестве $M \subseteq N$ легко найти минимальный элемент. В то же время Z не является вполне упорядоченным. В качестве подмножества без минимального элемента можно взять само множество Z . Оказывается, по вполне упорядоченным множествам можно проводить индуктивные доказательства. Такой тип доказательства называют *трансфинитной* индукцией.

Теорема 3.4.1. *Пусть* $(A, \leqslant)$ *— вполне упорядоченное множество и* a_0 *— минимальный элемент в* A . *Кроме того,* $p(a)$ *— некоторое утверждение, принимающее для любого* $a \in A$ *истинное или ложное значение и удовлетворяющее двум свойствам:*

(a) базе, т.е. $p(a_0)$ истинно;
(b) для него доказан шаг, т.е. в предположении, что для любого $a < b$ утверждение $p(a)$ — истинно, доказано, что $p(b)$ также истинно.
Тогда $p(a)$ истинно для любого $a \in A$.

Доказательство. О/п. Пусть это не так, т.е. найдется $b_0 \in A$, для которого $p(b_0)$ ложно. Рассмотрим множество $B = \{b \in A : p(b) — \text{ложно}\}$. Это множество не является пустым, поэтому, в силу полноты порядка, в нем найдется минимальный элемент. Обозначим его через b^*. Тогда для любого $a < b^*$ выполняется $a \notin B \Rightarrow p(a)$ — истинно. Так как шаг доказан, из истинности $p(a)$ для любого $a < b^*$ следует, что $p(b^*)$ — истинно. $\times$.

■

Следующим широко распространенным отношением является отношение эквивалентности. Отношение эквивалентности мы будем обозначать через $\sim$ (отношение равномощности между множествами также является отношением эквивалентности).

Определение. *Пусть $(A, \sim)$ — множество с отношением эквивалентности на нем. Множество $A(a) = \{b \in A : b \sim a\}$ мы будем называть классом эквивалентности по этому отношению $\sim$ (рис 18).*

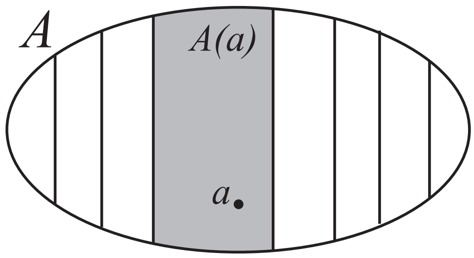

Рис. 18

Определение. *Множество A разбивается на подмножества A_s, $s \in S$, где S — некоторое множество индексов, если $A = \cup_{s \in S} A_s$ и множества A_s и $A_{s'}$ совпадают или не пересекаются.*

Теорема 3.4.2. *Пусть $(A, \sim)$ — множество с отношением эквивалентности на нем. Тогда отношением $\sim$ это множество разбивается на классы эквивалентности. И наоборот, если существует разбиение множества $A = \cup_{s \in S} A_s$, то существует такое отношение эквивалентности на множестве A, что каждое A_s будет классом эквивалентности.*

Доказательство. Пусть $\sim$ — отношение эквивалентности. В силу рефлексивности $a \sim a \Rightarrow A = \cup_{a \in A} A(a)$. Покажем, что любые два класса или совпадают, или не пересекаются. Если $c \in A(a) \cap A(b)$, то, используя транзитивность, $a \sim c \sim b \Rightarrow a \sim b$. Следовательно, $A(a) = A(b)$. Получим искомое представление $A = \cup_{a \in A} A(a)$.

Наоборот, если задано разбиение $A = \cup_{s \in S} A_s$, то введем отношение следующим образом: $a \, \rho \, b \Rightarrow a, b \in A_s$ для некоторого $s \in S$. Легко проверить, что оно искомое.

■

В заключительной части параграфа рассмотрим пример использования трансфинитной индукции при доказательстве одного алгебраического факта. Речь пойдет о представлении произвольного симметрического многочлена в виде многочлена от элементарных симметрических многочленов. Доказательство этой важной теоремы потребует от нас значительного числа вспомогательных понятий и утверждений, поэтому при первом чтении этот материал может быть пропущен.

Определение. *Одночленом от переменных* x_1 , $x_2, \ldots, x_n$ *называется выражение вида* $ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$, *где* $a \in R$ *и* k_i *являются неотрицательными целыми числами для всех* $i \in N_{\leqslant n}$. *Сумма* $\sum_{i=1}^{n} k_i$ *называется степенью одночлена, если* $a \neq 0$. *Если коэффициент* a *равен нулю, то одночлен называется нулевым и его степень равна нулю.*

Определение. *Два ненулевых одночлена* $ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$ *и* $bx_1^{l_1}x_2^{l_2}\ldots x_n^{l_n}$ *называются подобными, если одновременно* $k_i = l_i$ *для всех* $i \in N_{\leqslant n}$. *При этом их суммой называется одночлен* $(a+b)x_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$.

Определение. *Многочленом от переменных* x_1 , $x_2, \ldots, x_n$ *называется сумма конечного числа одночленов от этих переменных.*

В силу двух последних определений можно считать, что многочлен не содержит подобных слагаемых. В этом случае его степенью мы будем называть максимальную из степеней входящих в него слагаемых. Так, например, степень многочлена от трех переменных $f(x,y,z) = x^4y + x^4 + x^2y^3 + z^5$ равна пяти. Заметим, что $f(x,y,z)$ содержит три слагаемых пятой степени. Порядок, в котором выписаны эти слагаемые, называется *лексикографическим.*

Определение. *Пусть* $(X_1, \leqslant_1)$, $(X_2, \leqslant_2), \ldots, (X_n, \leqslant_n)$ *— упорядоченные множества. Отношение* $\leqslant$ *называется* лексикографическим порядком *на произведении* $X = X_1 \times X_2 \times \ldots \times X_n = \prod\limits_{i=1}^{n} X_i$, *если оно определяется следующим образом: для любых* $x_i, y_i \in X_i$, *где* $i \in N_{\leqslant n}$

$$(x_1, x_2, \ldots, x_n) \leqslant (y_1, y_2, \ldots, y_n) \Leftrightarrow \text{ существует такое}$$

$$i_0 \in \{0, \ldots, n\}, \text{ что } x_i = y_i \text{ при } i \in \{0, \ldots, i_0\} \text{ и } x_{i_0+1} < y_{i_0+1}.$$

Например, если лексикографически упорядочить декартову плоскость, то $(1,5) < (2,1)$ (здесь $i_0 = 0$). По похожему принципу упорядочиваются слова в словарях и энциклопедиях: сначала по первой букве, затем по второй и т.д. Теперь понятно и происхождение термина. Является ли лексикографический порядок отношением порядка? Следующая теорема, в частности, дает ответ и на этот вопрос.

Теорема 3.4.3. *Пусть даны вполне упорядоченные множества* $(X_1, \leqslant_1)$, $(X_2, \leqslant_2), \ldots, (X_n, \leqslant_n)$. *Тогда лексикографический порядок является полным порядком на множестве* $X = \prod_{i=1}^{n} X_i$.

Доказательство. Докажем индукцией по n . В качестве базы рассмотрим случай $n = 2$ (если $n = 1$, доказательство очевидно). Проверим выполнение всех пяти свойств отношения полного порядка.

Рефлексивность. Так как для любого $a \in X_1$ и $b \in X_2 \Rightarrow a \leqslant_1 a$ и $b \leqslant_2 b$, то $(a, b) \leqslant (a, b)$. Поэтому " $\leqslant$ " удовлетворяет рефлекивности.

Антисимметричность. Предположим, что одновременно $(a, b) \leqslant (a_1, b_1)$ и $(a_1, b_1) \leqslant (a, b)$. Из первого отношения получаем $a <_1 a_1$ или $a = a_1$ и $b \leqslant_2 b_1$. Если $a <_1 a_1$, то второе соотношение ложно, поэтому $a = a_1$. Аналогично $b = b_1$. Получаем, что антисимметричность также выполняется.

Транзитивность. Преположим, что $(a, b) \leqslant (c, d)$ и $(c, d) \leqslant (e, f)$. Покажем, что $(a, b) \leqslant (e, f)$. Исключим из дальнейшего рассмотрения только тривиальный случай совпадения двух или сразу всех пар.

1. $a <_1 c$. Поскольку $c \leqslant_1 e \Rightarrow a <_1 e \Rightarrow (a, b) < (e, f)$.

2. $a = c \Rightarrow b <_2 d$.

   (a) $c <_1 e \Rightarrow a <_1 e \Rightarrow (a, b) < (e, f)$.

   (b) $c = e \Rightarrow d <_2 f \Rightarrow b <_2 f \Rightarrow (a, b) < (e, f)$.

Линейность. Рассмотрим две произвольные пары (a, b) , $(c, d) \in X$. Так как порядок $\leqslant_1$ линеен, то выполняется одно из трех соотношений: $a <_1 c$, $a >_1 c$ или $a = c$. В первом и во втором случае получаем соответственно $(a, b) < (c, d)$ и $(a, b) > (c, d)$.

Если же $a = c$, то используем линейность порядка $\leqslant_2$: $b >_2 d$ или $b \leqslant_2 d$. Окончательно получаем, что $(a, b) > (c, d)$ или $(a, b) \leqslant (c, d)$.

Существование минимального элемента. Пусть C — произвольное непустое подмножество $X = X_1 \times X_2$. Рассмотрим множество $A = \{a \in X_1 :$ существует такой элемент $b \in X_2$, что $(a, b) \in C\}$ (т.е. $A = Dom\ C$). Так как $(X_1, \leqslant_1)$ является вполне упорядоченным множеством, то в A найдется минимальный элемент. Обозначим его через a^* и рассмотрим множество $B = \{b \in X_2 : (a^*, b) \in C\}$. Это множество не пусто и, в силу полноты порядка $\leqslant_2$, в нем также найдется минимальный элемент — b^* . Покажем, что (a^*, b^*) является минимальным элементом в C. Действительно, для любой пары $(a, b) \in C \Rightarrow a^* <_1 a$ или $a^* = a$. В первом случае получаем $(a^*, b^*) < (a, b)$, а во втором — $(a^*, b^*) \leqslant (a, b)$, используя уже минимальность b^* во множестве B.

Ш.И. Предположим, что утверждение истинно, если $n < k$, и докажем его для $n = k$. Для этого первые два сомножителя в произведении $X = X_1 \times X_2 \times \ldots \times X_k$ обозначим через $Y = X_1 \times X_2$. Последовательно используя базу и предположение индукции, получаем, что лексикографические порядки на Y и на $Y \times X_3 \times \ldots \times X_k$ являются отношениями полного порядка. Осталось только заметить, что лексикографический порядок на $Y \times X_3 \times \ldots \times X_k$ совпадает с лексикографическим порядком на X, что и завершает доказательство.

■

Обозначим через N^+ множество $N \cup \{0\}$. Легко проверить, что $(N^+, \leqslant)$ является вполне упорядоченным множеством. Из предыдущей теоремы сразу получаем

Следствие. *Пусть $X_i = N^+$ для каждого $i \in N_{\leqslant n}$. Тогда лексикографический порядок на $X = \prod_{i=1}^{n} X_i$ является отношением полного порядка.*

Теперь легко упорядочить слагаемые многочлена.

Определение. *Ненулевой одночлен $ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$ будем считать старше ненулевого одночлена $bx_1^{l_1}x_2^{l_2}\ldots x_n^{l_n}$, если выполняется следующее неравенство: $(k_1, k_2, \ldots, k_n) > (l_1, l_2, \ldots, l_n)$. Нулевой одночлен по определению младше любого другого одночлена.*

Нетрудно заметить, что введенное отношение вполне упорядочивает слагаемые любого многочлена. А поскольку число слагаемых в многочлене конечно, то среди них найдется самое старшее слагаемое, которое мы будем называть старшим слагаемым данного многочлена.

Произведением одночленов $ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$ и $bx_1^{l_1}x_2^{l_2}\ldots x_n^{l_n}$ называется одночлен $abx_1^{k_1+l_1}x_2^{k_2+l_2}\ldots x_n^{k_n+l_n}$. Теперь, чтобы получить произведение $f \cdot g$ двух многочленов $f(x_1, \ldots, x_n)$ и $g(x_1, \ldots, x_n)$, достаточно сложить все попарные произведения одночленов f на одночлены g. Можно доказать, что старшим слагаемым произведения $f \cdot g$ будет являться произведение старшего слагаемого f на старшее слагаемое g.

Среди многочленов от n переменных особое место занимают симметрические многочлены и элементарные симметрические многочлены.

Определение. *Многочлен $f(x_1, \ldots, x_n)$ называется симметрическим многочленом, если для любых $i, j \in N_{\leqslant n}$ и $i < j \Rightarrow$*

$$f(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) = f(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n).$$

Это означает, что многочлен f не изменяется при одновременной замене во всех его одночленах переменной x_i на x_j и переменной x_j на x_i.

Так, например, многочлены x^3y+y^3x и x^2-xy+y^2 являются симметрическими от двух переменных. Легко проверяется, что сумма и произведение симметрических многочленов от одних и тех же переменных также является симметрическим многочленом от этих переменных. Кроме того, старшее слагаемое любого симметрического многочлена обладает следующим свойством.

Лемма 3.4.1. *Пусть $ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$ — старшее слагаемое симметрического многочлена $f(x_1,\ldots,x_n)$. Тогда $k_1 \geqslant k_2 \geqslant \ldots \geqslant k_n$.*

Доказательство. О/п. Предположим, что существует такое наименьшее $i<n$, что $k_i<k_{i+1}$. Так как f является симметрическим многочленом, то в него также входит одночлен $ax_1^{k_1}\ldots x_{i+1}^{k_i}x_i^{k_{i+1}}\ldots x_n^{k_n}$. Легко заметить, что это слагаемое старше $ax_1^{k_1}\ldots x_i^{k_i}x_{i+1}^{k_{i+1}}\ldots x_n^{k_n}$. $\times$.

■

Определение. *Элементарными симметрическими многочленами от переменных $x_1,\ldots,x_n$ называются следующие многочлены:*

$$\begin{aligned}
&\sigma_1(x_1,\ldots,x_n) = x_1+x_2+\ldots+x_n,\\
&\sigma_2(x_1,\ldots,x_n) = x_1x_2+x_1x_3+\ldots+x_{n-1}x_n = \sum_{i<j\leqslant n} x_ix_j,\\
&\vdots\\
&\sigma_n(x_1,\ldots,x_n) = x_1x_2\ldots x_n.
\end{aligned}$$

Рассмотренные ранее многочлены $f(x,y)=x^3y+y^3x$ и $g(x,y)=x^2-$ $-xy+y^2$ могут быть представлены в виде многочленов от $\sigma_1(x,y)=x+y$ и $\sigma_2(x,y)=xy$, т.е. записаны в виде $f(x,y)=xy\Big((x+y)^2-2xy\Big)=\sigma_2({\sigma_1}^2-$ $-2\sigma_2)=f_1(\sigma_1,\sigma_2)$ и $g(x,y)={\sigma_1}^2-3\sigma_2=g_1(\sigma_1,\sigma_2)$. Этот факт справедлив для любого симметрического многочлена.

Теорема 3.4.4. *Любой симметрический многочлен $f(x_1,\ldots,x_n)$ может быть представлен в виде многочлена от элементарных симметрических многочленов от переменных $x_1,\ldots,x_n$.*

Доказательство. Как уже известно (лемма 3.4.1), показатели степеней у старшего слагаемого многочлена f убывают. Поэтому во множестве $X=(N^+)^n$ рассмотрим подмножество $A=\{(k_1,k_2,\ldots,k_n): k_1\geqslant k_2\geqslant\ldots\geqslant k_n\}$. Если между элементами множества A рассматривать тот же порядок, что был между ними на множестве X (т.е. рассмотреть пересечение лексикографического порядка с множеством $A\times A$), то полученный порядок также будет полным. Далее применим трансфинитную индукцию в доказательстве следующего утверждения: $T(k_1,k_2,\dots,k_n)$ = "любой симметрический многочлен со старшим слагаемым $ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$, где $(k_1,k_2,\dots,k_n)\in A$, может быть представлен в виде многочлена от $\sigma_1,\sigma_2,\dots,\sigma_n$".

Б.И. Докажем $T(0,0,\dots,0)$. Поскольку $ax_1^0x_2^0\dots x_n^0$ является старшим слагаемым f, то $f=a\sigma_1^0\sigma_2^0\dots\sigma_n^0$, что и завершает доказательство базы.

Ш.И. Предположим теперь, что $T(l_1,l_2,\dots,l_n)$ истинно для любого $(l_1,l_2,\dots,l_n)<(k_1,k_2,\dots,k_n)$ (т.е. любой многочлен со старшим слагаемым $ax_1^{l_1}x_2^{l_2}\dots x_n^{l_n}$, где $(l_1,l_2,\dots,l_n)<(k_1,k_2,\dots,k_n)$, представим в виде $f_1(\sigma_1,\sigma_2,\dots,\sigma_n)$). Докажем, что $T(k_1,k_2,\dots,k_n)$ также истинно. Для этого рассмотрим вспомогательный одночлен

$$g_0(\sigma_1,\sigma_2,\dots,\sigma_n)=a\sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3}\dots\sigma_{n-1}^{k_{n-1}-k_n}\sigma_n^{k_n}.$$

Заметим, что при замене $\sigma_1,\sigma_2,\dots,\sigma_n$ на их значения от $x_1,x_2,\dots,x_n$ получится некоторый многочлен от переменных $x_1,x_2,\dots,x_n$. Легко определяется его старшее слагаемое. Действительно, оно равно произведению старших слагаемых $\sigma_1(x_1,\dots,x_n)$, $\sigma_2(x_1,\dots,x_n),\dots,$ $\sigma_n(x_1,\dots,x_n)$, т.е.

$$a(x_1)^{k_1-k_2}\cdot(x_1x_2)^{k_2-k_3}\cdot\ldots\cdot(x_1x_2\dots x_{n-1})^{k_{n-1}-k_n}\cdot(x_1x_2\dots x_n)^{k_n}=$$
$$=ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}.$$

В результате старшее слагаемое f равно старшему слагаемому g_0. Таким образом, многочлен $g=f-g_0$ имеет своим старшим слагаемым слагаемое, которое строго младше $ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$. Применяя к g предположение индукции, имеем

$$g(x_1,\dots,x_n)=g_1(\sigma_1,\dots,\sigma_n)\Rightarrow f=g+g_0=f_1(\sigma_1,\dots,\sigma_n).$$

Упражнения

78. Рассмотрите отношение эквивалентности "быть сравнимыми между собой по $\pmod 7$" на множестве натуральных чисел. Найти формулу, описывающую все элементы класса, содержащего 4.

79. Пусть $Z=\{(n,m):n,m\in N\}$. Определим отношение на этом множестве следующим образом: $(n,m)\rho(k,l)\Leftrightarrow n+l=m+k$. Докажите, что это отношение является отношением эквивалентности. Пусть $(n,m)+(k,l)=(n+k,m+l)$. Докажите, что эта операция не зависит от выбора представителей, т.е. если $(n,m)\rho(n_1,m_1)$ и $(k,l)\rho(k_1,l_1)$, то выполняется $\Big((n,m)+(k,l)\Big)\,\rho\,\Big((n_1,m_1)+(k_1,l_1)\Big)$.

80. Определите на множестве лучей отношение "быть сонаправленными друг с другом". Докажите, что это отношение является отношением эквивалентности.

81. Сколько существует полных порядков на множестве $N_{\leqslant n}$? Сколько вообще существует порядков на этом множестве?

3.5 Антиномии. Аксиомы теории множеств

Заключительный параграф состоит из трех частей: примеров наиболее известных парадоксов или антиномий, введения некоторых логических обозначений для сокращения записи утверждений и аксиоматической системы Цермело–Френкеля.

При чтении всего предыдущего материала может возникнуть чувство ясного представления, что такое множество. Поэтому необходимо сделать предупреждение: существует прекрасная возможность утратить это чувство, прочитав этот параграф целиком.

В обсуждении самого понятия множества мы недалеко ушли от того значения, которое используется в обычном языке: объекты, являющиеся элементами множества, могут быть любой природы, и правила $P(x)$, по которым элементы объединяются в множество, также могут быть произвольными. Эту ситуацию нельзя считать окончательной ввиду следующих парадоксов.

Парадокс Рассела. Определим K следующим образом: произвольное множество $X \in K \Leftrightarrow X \notin X$. Предположим, что K — множество, тогда можно попытаться выяснить, $K \in K$ или $K \notin K$? Но если $K \in K$, то по определению $K = \{X : X \notin X\} \Rightarrow K \notin K$. $\nwarrow\!\!\!\nearrow$.Если $K \in K$, то опять, воспользовавшись определением $K = \{X : X \notin X\}$, получаем, что $K \notin K$. $\nwarrow\!\!\!\nearrow$.

Парадокс о брадобрее. Пусть Б — брадобрей. По определению будем считать, что он должен брить тех и только тех людей, кто не бреет себя сам. Бреет ли он сам себя? Если да, то он не должен этого делать. А если он не бреет себя сам, то он должен себя брить согласно определению.

Лексический парадокс. Будем определять натуральные числа, используя слова русского языка. Сделаем только одно ограничение: в определении мы не будем использовать больше одиннадцати слов. Слов конечное число (ограничиваясь словарем Даля, будем считать, что их не более 200000). Поэтому и количество чисел, которые можно определить таким образом, конечно. В силу полноты порядка на N существует минимальное из чисел, которое мы не можем определить. Зададим это число следующим образом: “минимальное из натуральных чисел, которые нельзя определить с помощью одиннадцати слов”. Нетрудно убедиться, что в этом определении в точности одиннадцать слов.

Парадокс Бурали–Форти. Это самый первый из появившихся парадоксов. Чтобы его сформулировать, понадобится совокупность, очень похожая на K из парадокса Рассела. Пусть K_1 вместе с каждым множеством содержит каждый его элемент. Пусть теперь K_1 является множеством, тогда по теореме Кантора $|K_1| < |\mathcal{P}(K_1)|$, но по определению K_1 множество $\mathcal{P}(K_1) \subseteq K_1 \Rightarrow |\mathcal{P}(K_1)| \leqslant |K_1|$. ⤫.

Чтобы избежать парадоксов, необходимо наложить некоторые ограничения на то, из каких элементов состоит множество и с помощью каких правил оно строится. Было бы логично потребовать, чтобы множество собиралось из элементов, которые уже существуют. Так, например, при построении множества нельзя использовать в качестве его элемента само это множество. Таким образом, мы приходим к очень естественной идее: множество, кроме того, что оно является некоторой совокупностью, является одновременно и неким процессом собирания ранее построенных элементов.

Итак, каждое множество должно строиться на некотором шаге $\mathbf{s}$. Этот шаг должен иметь предшествующие шаги, на которых должны быть построены все элементы этого множества. Каждый шаг имеет последующий, что позволяет образовывать все новые и новые множества. Более того, каждое множество шагов также имеет последующий, но вся совокупность шагов (которая множеством не является) не имеет последующего, иначе легко было бы получить парадокс, похожий на парадокс Бурали–Форти.

Система аксиом позволяет избежать парадоксов при переходе от одного множества к другому. Фактически она описывает естественные способы получения одних множеств из других и позволяет безопасно путешествовать от одного шага к другому. Так, в частности, все рассмотренные нами ранее операции над множествами будут приводить к образованию новых множеств.

При формулировке аксиом мы воспользуемся средствами математической логики, которая является еще одной фундаментальной математической дисциплиной. Поэтому начнем с определения этих полезных обозначений и понятий.

Определение. *В качестве логических связок мы будем использовать:* $\Rightarrow$ *для “следует”,* $\Leftrightarrow$ *для “тогда и только тогда”,* $\&$ *для “и, одновременно”,* $\vee$ *для “или, хотя бы одно из двух”. Кроме того, будем использовать квантор всеобщности* $\forall$ *(например,* $\forall x \in R \Rightarrow cos^2 x + sin^2 x = 1$ *— для всех вещественных* x *выполняется* $\ldots$*) и квантор существования* $\exists$ *(например,* $\exists x \in R : x^2 = 1$ *— существует хотя бы один* $x \in R$*, что* $\ldots$*). И, наконец, предикатом, или высказывательной функцией, мы будем называть отображение* $P(x)$*, которое ставит в соответствие элементам или множествам одно из двух значений — истина или ложь. Если этот предикат задан на некотором множестве, то мы будем говорить, что он ограничен (так, например, преди-*

кат $P(x) =$ “$x \leqslant 0$”, *заданный на множестве* R, *ограничен; легко видеть, что* $P(1) = \text{Л}$ *и* $P(-1) = \text{И}$ *).*

Следующая аксиоматическая система была впервые предложена Цермело и усовершенствована Френкелем (им добавлена аксиома выделения). Напоминаем, что символы A, B, X, Y мы используем только для обозначения множеств.

Первая аксиома закрепляет то положение, что множество полностью определяется своими элементами.

Аксиома объемности. Если $\forall x(x \in A \Leftrightarrow x \in B)$, то $A = B$.

Следующая аксиома гарантирует, что для двух множеств A, B существует их множество-пара, т.е. множество $\{A, B\}$, единственными элементами которого являются именно эти два множества.

Аксиома пары. $\forall A \forall B \exists X(Y \in X \Leftrightarrow Y = A \vee Y = B)$.

Если элементы множества A сами являются множествами, то можно рассмотреть объединение всех этих элементов. Третья аксиома говорит о том, что это объединение также является множеством.

Аксиома объединения. $\forall A \exists X(Y \in X \Leftrightarrow \exists B \in A : Y \in B)$.

Взятие множества всех подмножеств множества A также приводит к образованию множеств. Об этом следующая аксиома.

Аксиома степени. $\forall A \exists X(Y \in X \Leftrightarrow Y \subseteq A)$.

Если каждое множество, на котором некоторый предикат принимает истинные значения, является элементом некоторого большего множества, то из них можно образовать новую совокупность, которая будет множеством.

Аксиома выделения. Для каждого множества A и предиката $P(a)$ справедливо следующее. Если $(P(a) = \text{И} \Rightarrow a \in A) \Rightarrow \exists X : X = \{a : P(a)\}$.

Без следующей аксиомы наш мир мог бы состоять только из конечных множеств. Богатство разнообразных по мощности множеств достигается путем введения всего лишь одного бесконечного множества, содержащего $\varnothing$ и вместе с каждым элементом A множество $\{A\}$.

Аксиома бесконечности. $\exists X(Y \in X \Leftrightarrow Y = \varnothing \vee \exists A \in X : Y = \{A\})$.

Если задано некоторое отображение F на множестве A, которое каждому элементу a этого множества ставит в соответствие некоторое множество $Y = F(a)$, то совокупность, состоящая из образов и только из них, также является множеством. Об этом аксиома подстановки.

Аксиома подстановки. Для каждого множества A и отображения F справедливо следующее. $\exists X(Y \in X \Leftrightarrow Y = F(a)$ при некотором $a \in A)$.

При обсуждении понятия множества мы заметили, что его элементы должны строиться на предыдущих шагах. Каждый из этих элементов, сам будучи множеством, строится из элементов, образованных еще на более ранних шагах, и т.д. Чтобы этот процесс не был бесконечным вниз по "лестнице" шагов, вводится следующая и последняя аксиома. Она гарантирует существование минимального элемента. При этом минимальным элементом в непустом множестве A называют такой элемент $B \in A$, что B и A не имеют общих элементов. Это означает, что при построении A не используется ни один из элементов множества B.

Аксиома регулярности. $\forall A(A \neq \varnothing) \Rightarrow (\exists B \in A : \forall X \in B \Rightarrow X \notin A)$.

Сергей Александрович Ануфриенко

Введение в теорию множеств и комбинаторику

Учебное пособие

Редактор Т.А. Сасина
Технический редактор Э.А. Максимова
Компьютерный набор и верстка С.А. Ануфриенко

ЛР т 020257 от 22.11.96.

Подписано в печать 5.11.98. Формат $60 \times 84\ 1/16$.
Бумага для множительных аппаратов. Печать офсетная.
Уч.-изд.л. 4,4. Усл. печ. л. 4,3. Зак. . Тираж экз.
Уральский государственный университет им. А.М. Горького.
Екатеринбург, пр. Ленина, 51.
