

B12 я 43  
Д84

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ  
ЯРОСЛАВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИМ. П.Г. ДЕМИДОВА

В.Г. ДУРНЕВ

# ВВЕДЕНИЕ В МАТЕМАТИЧЕСКУЮ ЛОГИКУ

УЧЕБНОЕ ПОСОБИЕ

Рекомендовано Научно-методическим советом по математике и механике  
Учебно-методического объединения университетов РФ для математических  
специальностей и направлений подготовки университетов

2/3

ЯРОСЛАВЛЬ 2005

267965

ЧИТ. ЗАЛ

УДК 510.6  
ББК В 12 я 73  
Д 84

*Рекомендовано  
Редакционно-издательским советом университета  
в качестве учебного издания. План 2005 года*

Рецензенты:  
кафедра алгебры и геометрии Тульского государственного  
педагогического университета им. Л.Н. Толстого;  
доктор. физ.-матем. наук, профессор С.П. Струнков

Д 84 **Дурнев, В.Г.** Введение в математическую логику: Учеб. пособие / В.Г. Дурнев; Яросл. гос. ун-т. — Ярославль: ЯрГУ, 2005. — 188 с.

ISBN 5-8397-0365-6

В учебном пособии излагаются основные понятия теории множеств, логики и исчисления высказываний.

Пособие предназначено для студентов, обучающихся по направлению подготовки 510100 Математика и по специальностям 010100 Математика и 090102 Компьютерная безопасность. Оно может быть использовано при изучении дисциплин "Введение в теорию множеств и логическую символику", "Математическая логика", "Математическая логика и теория алгоритмов" и "Дискретная математика" (блок ЕН), а также специальных дисциплин.

Библиогр.: 49 назв.

УДК 510.6  
ББК В 12 я 73



ISBN 5-8397-0365-6

- © Ярославский государственный университет  
им. П.Г. Демидова, 2005  
© В.Г. Дурнев, 2005



# ОГЛАВЛЕНИЕ

Предисловие . . . . .	5
ГЛАВА I. ЭЛЕМЕНТЫ ТЕОРИИ МНОЖЕСТВ . . . . .	9
§ 1. Множества и операции над ними . . . . .	9
§ 2. Соответствия, отношения и функции . . . . .	16
§ 3. Некоторые специальные отношения . . . . .	31
§ 4. Равномощность множеств . . . . .	40
§ 5. Конечные и счетные множества . . . . .	46
§ 6. Множества мощности континуума . . . . .	52
§ 7. Операции над кардинальными числами . . . . .	56
§ 8. Вполне упорядоченные множества . . . . .	59
§ 9. Натуральные числа. Системы Пеано . . . . .	82
9.1. Системы Пеано . . . . .	82
9.2. Рекурсивные определения в системах Пеано . . . . .	87
9.3. Определение сложения и умножения натуральных чисел . . . . .	90
§ 10. Некоторые приложения аксиомы выбора . . . . .	92
§ 11. Дополнение . . . . .	108
ГЛАВА II. ЛОГИКА И ИСЧИСЛЕНИЕ ВЫСКАЗЫВАНИЙ . . . . .	119
§ 1. Алфавиты. Слова . . . . .	119
§ 2. Логика Высказываний . . . . .	121
§ 3. Исчисление Высказываний . . . . .	137
§ 4. Дополнительные вопросы Логике и Исчисления Высказываний . . . . .	158
§ 5. Алгебра Линденбаума для Исчисления Высказываний . . . . .	168
ГЛАВА III. ДОПОЛНЕНИЕ . . . . .	171
§ 1. Булевы алгебры . . . . .	171
§ 2. Понятие о нестандартном, или неархимедовом, анализе . . . . .	177
Послесловие . . . . .	184
Литература . . . . .	185

## ПРЕДИСЛОВИЕ

Трудно, на наш взгляд, оспорить утверждение, что значительная часть математики XX века базировалась на теоретико-множественном фундаменте. И в XXI веке, как нам кажется, ситуация не претерпела коренных изменений. Теория множеств лежит в основе большинства современных математических дисциплин, включенных в учебные планы для университетов по математическим специальностям. Элементарные сведения по теории множеств входят в программы курсов алгебры, математического анализа, функционального анализа, топологии, теории вероятностей и т.д. Традиционно каждый лектор, руководствуясь, прежде всего, программой соответствующей дисциплины и своими личными вкусами, выбирает из обширного теоретико-множественного материала то, что ему кажется необходимым, излагает это со своей точки зрения и с использованием собственной или принятой в преподаваемой им дисциплине системы обозначений. Достаточно цельной теоретико-множественной картины при этом, как правило, не возникает. Из математической логики обычно используется лишь система обозначений — логическая символика.

При работе над пособием автором преследовалась цель — попытаться изложить с единых позиций основной, по его мнению, материал по теории множеств и математической логике, необходимый и в то же время в идейном отношении доступный студентам I–II курсов математических факультетов университетов. Преследовалась и еще одна важная, по нашему мнению, цель — чтобы основные вводимые понятия “не повисали в воздухе”, постараться проиллюстрировать их достаточно содержательными примерами применения. Поэтому в пособие включен, может быть, несколько избыточный материал, связанный с применениями аксиомы выбора. О других особенностях отбора материала и выбранного нами способа его изложения будет сказано ниже. Заметим лишь, что автор больше заботился о ясности и полноте, чем о краткости изложения. Насколько это ему удалось — судить читателю. Автор сделал, что мог, пусть другие сделают больше.

При написании пособия использовались включенные в список литературы работы различных авторов на эту тему. Всем им, как и тем, чьи работы не включены в список литературы, однако оказали идейное влияние на формирование взглядов автора на предмет, мы выражаем искреннюю благодарность и признательность. О содержании пособия можно понять по его достаточно подробному оглавлению.

Первая глава, носящая название “Элементы теории множеств”, содержит основной, по нашему мнению, теоретико-множественный материал. В первом параграфе рассматриваются множества, операции над ними и их основные свойства. При этом мы придерживаемся промежуточного между “наивным” и “формальным” способа введения основных понятий, уделяем большее, чем это традиционно делается, внимание разъяснению “очевидных” свойств, например, отношения равенства, которыми обычно содержательно пользуются, но явно их не формулируют. Т.е. мы как бы пытаемся по возможности полно сформули-

ровать “правила игры”, но не доходим до логического конца — не формулируем основные допущения о множествах в виде формул языка первого порядка, не заменяем содержательную математику “игрой в символы”. Мы движемся в направлении аксиоматической теории множеств и интересующийся читатель по другим источникам может с ней познакомиться. Но мы, как нам кажется, во время останавливаемся. И делаем это по двум причинам. Во-первых, нам не представляется возможным убедительно обосновать студентам младших курсов выбор той или иной системы аксиом для теории множеств. Во-вторых, “достаточно полная” система аксиом теории множеств действительно бывает нужна в “идейно сложных” ситуациях, например, чтобы доказать независимость континуум-гипотезы от аксиом теории множеств, т.е. доказать “недостаточную полноту” выбранной системы аксиом. Об общей теореме К. Геделя о неполноте речь пойдет в другом учебном пособии, продолжающем данное. Во втором параграфе изучаются соответствия, отношения и функции. Показывается, как основные математические понятия могут быть определены через понятие множества, причем эти определения достаточно хорошо согласуются с нашими интуитивными представлениями. Изучаются основные типы отображений — инъективные, сюръективные и биективные. Было намерение что-то сказать об использовании отношений в реляционных базах данных, но потом от этой мысли пришлось по ряду причин отказаться. В третьем параграфе изучаются некоторые специальные отношения и, прежде всего, отношения эквивалентности, частичного и линейного порядка. Рассмотрен вопрос о связи отношений эквивалентности с разбиениями множеств. Показывается, как отношения эквивалентности и фактормножества используются при построении на основе системы натуральных чисел кольца целых чисел, полей рациональных и действительных чисел. В четвертом параграфе изучается понятие равномощности множеств, доказывается известная теорема Г. Кантора — Ф. Бернштейна об антисимметричности “отношения частичного порядка для мощностей”, теорема Г. Кантора о множестве-степени. В пятом параграфе рассматриваются некоторые свойства конечных и счетных множеств, которые, по мнению автора, наиболее часто используются в доказательствах математических теорем. В шестом параграфе приводятся некоторые сведения о множествах мощности континуума и об операциях над кардинальными числами. При этом следует особо выделить теоретико-мощностное доказательство существования трансцендентных чисел — доказательство несчетности множества всех трансцендентных чисел. Именно с этой теоремы, доказанной Г. Кантором во второй половине XIX века, и начинается свое “триумфальное шествие” канторовская теория множеств. Седьмой параграф служит введением в теорию вполне упорядоченных множеств. В нем особое внимание уделено доказательству равносильности аксиомы выбора ряду теоретико-множественных утверждений. И чтобы этот материал “не повис в воздухе”, в качестве его приложения рассмотрена теорема о существовании базиса в любом векторном пространстве, а как ее следствие — доказательство невыводимости свойства однородности функции из ее аддитивности. В двух следующих параграфах изложен материал по аксиоматическому подходу к теории

натуральных чисел — системы Пеано, теорема о рекурсивных определениях в системах Пеано и рассмотрены еще два важных, по нашему мнению, применения аксиомы выбора. Заканчивается глава небольшим историческим обзором, который ни в коей мере не претендует на какую-либо полноту. Его назначение — попытаться показать читателю, начинающему серьезно изучать математику, что математические знания создавались многими поколениями исследователей, которым мы должны быть благодарны.

Вторая глава “Элементы математической логики” начинается с вводного параграфа, содержащего необходимый материал по алфавитам, словам и операциям над ними. Второй параграф посвящен логике высказываний, как простейшему, но чрезвычайно важному разделу математической логики. Центральными понятиями этого параграфа являются понятия интерпретации, истинностного значения формулы в интерпретации и логического следствия множества формул. Особое место в этом параграфе, как и во всей второй части, занимает теорема компактности для логики высказываний. Излагаются два доказательства этой теоремы, каждое из которых может быть преобразовано, хотя и не без дополнительных усилий, в доказательство чрезвычайно важной теоремы математической логики — теоремы компактности К. Геделя — А.И. Мальцева для логики предикатов. Эта теорема, особенно ее доказательство, конечно, трудна для студентов младших курсов. Однако в случае логики высказываний можно без особого труда понять как саму идею доказательства, так и технические детали, что несомненно поможет позже понять и доказательство в общем случае исчисления предикатов. Следующий параграф посвящен исчислению высказываний — вводятся логические аксиомы и правила вывода, вывод и вывод из множества гипотез, доказывается теорема дедукции. В качестве подготовки к доказательству теоремы адекватности для исчисления высказываний изучаются основные свойства отношения выводимости. Основной целью служит желание познакомить читателя на примере исчисления высказываний с некоторыми основными понятиями математической логики, теоремами и используемым в их доказательствах аппаратом, который в случае исчисления предикатов достаточно сложен и абстрактен. Завершается глава некоторыми сведениями о неархимедовом, или нестандартном, анализе, речь о котором пойдет в пособии, планы которого только вынашиваются.

Пользуясь случаем, выражаю глубокую благодарность редактору пособия Алле Александровне Аладьевой за терпеливое и высоко качественное редактирование и Михаилу Анатольевичу Башкину за неоценимую помощь в компьютерном наборе и придании пособию достойного внешнего вида.

# ГЛАВА I.

## ЭЛЕМЕНТЫ ТЕОРИИ МНОЖЕСТВ

### 1. Множества и операции над ними

Начало *канторовской*, или, как иногда говорят, “*наивной*”, теории множеств было положено открытиями, содержащимися в публикациях Г. Кантора 1871–1883 гг. В этих работах Г. Кантора содержалось изложение его учения о бесконечности, теории кардинальных и ординальных чисел, а также теория вполне упорядоченных множеств. В связи с исследованиями по теории тригонометрических рядов Г. Кантор подошел к необходимости понять, какие множества можно образовать из точек действительной прямой. В частности, его интересовал вопрос, всегда ли можно занумеровать натуральными числами элементы числовых множеств. В 1874 г. Г. Кантор получил отрицательный ответ на последний вопрос: им была установлена *несчетность множества всех действительных чисел*, а значит, существование бесконечных множеств разной мощности. Первоначально идеи Г. Кантора не нашли широкой поддержки у его современников. Особенно яростной критике они были подвергнуты Л. Кронекером. Однако позже они проникли во многие разделы математики и оказали огромное влияние на их развитие. Официальной датой признания теории множеств можно считать 1897 г. — именно в этом году на Первом международном конгрессе математиков Ж. Адамар и А. Гурвиц привели многочисленные примеры применения теории множеств в математическом анализе, являвшемся в то время одним из основных разделов математики. Теория множеств служит фундаментом таких современных разделов математики, как теория функций действительного переменного, общей алгебры, топологии, функционального анализа, геометрии, теории вероятностей и т.д.

Понятие *множество* является одним из основных *неопределяемых* понятий математики и, как мы увидим в ближайших параграфах, очень многие математические понятия, такие, например, как “*упорядоченная пара элементов*”, “*упорядоченный набор элементов*”, “*функция*”, “*отношение*” и целый ряд других, могут быть определены через понятие множества. Г. Кантор следующим



образом поясняет понятие множества: “Под “множеством” мы понимаем любое объединение в одно целое  $M$  определенных вполне различных объектов  $m$  нашего восприятия или мысли (которые называются *элементами*  $M$ )”.

В этом пояснении Г. Кантора особо следует подчеркнуть слова “... объединение в одно целое ...”. Если мы рассматриваем некоторую совокупность объектов, например, четных натуральных чисел, то здесь нет нужды говорить, что они образуют некоторое объединение, называемое множеством, а можно просто говорить о четных натуральных числах, но когда мы переносим внимание с отдельных четных натуральных чисел на всю их совокупность, с этой совокупностью начинаем оперировать как с некоторым новым объектом, то здесь и появляется понятие множества. *Некоторую совокупность  $M$  объектов мы начинаем рассматривать как множество, если в наших рассуждениях появляется некоторая новая совокупность  $X$  объектов, одним из которых является  $M$ .* Конечно, все эти рассуждения являются нестрогими, несколько “туманными”, но ведь с самого начала было отмечено, что понятие “множество” неопределяемое, а значит, можно только пытаться как-то пояснить его в надежде, что у человека, не владевшего этим понятием, после таких пояснений появится некоторое представление о понятии множества, адекватное нашему пониманию этого понятия.

Чтобы выразить тот факт, что объект  $a$  есть элемент множества  $X$ , пишут  $a \in X$  и говорят, что  $a$  принадлежит множеству  $X$ . Знак  $\in$  введен Дж. Пеано как сокращение греческого слова *εστι* — “быть”. Если же мы попытаемся уточнить, что означает утверждение “ $a$  принадлежит  $X$ ”, то после некоторых раздумий придем к выводу, что нам не остается ничего другого, как признать, что отношение принадлежности  $\in$  следует считать неопределяемым понятием. Кроме введенного отношения  $\in$  нам понадобится еще одно отношение, уже хорошо известное читателю, отношение равенства  $=$ . Запись  $a = b$  означает, что  $a$  и  $b$  обозначают один и тот же объект. Если же читатель попытается уточнить смысл последней фразы, то встретится с трудностями; понятие равенства  $=$  тоже следует отнести к первоначальным понятиям (есть и другие точки зрения, но об этом речь пойдет позже). Утверждение  $a = b$  можно пояснить так: про любое свойство  $P$  можно утверждать, что если им обладает объект, обозначенный через  $a$ , то им обладает и объект, обозначенный через  $b$ . Обычно этим соглашением пользуются без особых оговорок, что будем делать и мы в части, посвященной канторовской теории множеств.

Для дальнейшего нам будет удобно ввести некоторые сокращения. Будем придерживаться следующего соглашения:

знак  $\vee$  является сокращением (обозначением) для союза “или” и называется “дизъюнкцией”, формула  $(A \vee B)$  читается “ $A$  или  $B$ ” или “дизъюнкция  $A, B$ ”;

знак  $\wedge$  (&) является сокращением (обозначением) для союза “и” и называется “конъюнкцией”, формула  $(A \wedge B)$  читается “ $A$  и  $B$ ” или “конъюнкция  $A, B$ ”;

знак  $\Rightarrow$  служит сокращением для “если ..., то ...” и называется “импли-

кацией”, формула  $(A \Rightarrow B)$  читается “если  $A$ , то  $B$ ” или “из  $A$  следует  $B$ ”, или “ $A$  имплицитует  $B$ ”;

знак  $\Leftrightarrow$  служит сокращением для “... тогда и только тогда, когда ...” и называется “эквивалентностью”, формула  $(A \Leftrightarrow B)$  читается “ $A$  выполнено тогда и только тогда, когда выполнено  $B$ ” или “ $A$  эквивалентно  $B$ ”;

знак  $\neg$  служит сокращением для “не” и называется “отрицанием”, формула  $(\neg A)$  читается “не  $A$ ”;

знак  $\forall x$  служит сокращением для “для всех  $x$  ...” и называется “квантором общности или всеобщности”, формула  $(\forall x)A$  читается “для всех  $x$   $A$ ”;

знак  $\exists x$  служит сокращением для “существует  $x$  ...” и называется “квантором существования”, формула  $(\exists x)A$  читается “существует  $x$  такой, что  $A$ ”.

**Замечание.** Наряду с введенной терминологией мы будем иногда называть квантором общности (соответственно существования) и один знак  $\forall$  (соответственно  $\exists$ ), тогда  $\forall x$  и  $\exists x$  называются кванторными комплексами.

Отрицание утверждения  $a \in X$ , т.е.  $\neg(a \in X)$ , будем обозначать часто через  $a \notin X$ , аналогично вместо  $\neg(a = b)$  часто будем писать  $a \neq b$ .

Первоначальная связь между двумя неопределяемыми отношениями  $\in$  и  $=$  может быть выражена следующими формулами, называемыми аксиомами равенства:

1.  $(\forall x)(x = x)$ ;
2.  $(\forall x)(\forall y)(x = y \Rightarrow y = x)$ ;
3.  $(\forall x)(\forall y)(\forall z)(x = y \wedge y = z \Rightarrow x = z)$ ;
4.  $(\forall x)(\forall y)\left(x = y \Rightarrow (\forall z)(x \in z \Leftrightarrow y \in z)\right)$ ;
5.  $(\forall x)(\forall y)\left(x = y \Rightarrow (\forall z)(z \in x \Leftrightarrow z \in y)\right)$ .

Первые три формулы выражают обычные свойства равенства, четвертая формула носит название “тождество неразличимых по Лейбницу”, а пятая утверждает, что равные множества состоят из одних и тех же элементов.

Канторовская теория множеств основывается на нескольких аксиомах, которые обычно называются *основными принципами теории множеств* или ее *нелогическими аксиомами*. Эти принципы мы будем вводить постепенно, да и не все укажем, а только те, которые необходимы для получения первоначальных теорем в теории множеств. Обсуждение вопроса о том, что такое в современном понимании полная система аксиом для теории множеств увело бы нас слишком далеко от канторовской теории множеств.

**Принцип объемности.** Если два множества  $X$  и  $Y$  состоят из одних и тех же элементов, то они считаются равными, т.е. выполнено утверждение

$$(\forall X)(\forall Y)\left((\forall x)(x \in X \Leftrightarrow x \in Y) \Rightarrow X = Y\right).$$

Сделаем некоторые пояснения к этому принципу. *Принцип объемности* устанавливает связь между двумя неопределяемыми отношениями  $\in$  и  $=$ . Точнее, принцип объемности утверждает, что если множества  $X$  и  $Y$  состоят из одних и тех же элементов, т.е.

$$(\forall x)(x \in X \iff x \in Y),$$

то они равны, т.е.  $X = Y$ , при этом считается, что смысл утверждения  $X = Y$  интуитивно ясен, в частности, из ранее данных пояснений следует, что верно и утверждение, обратное принципу объемности: если  $X = Y$ , то

$$(\forall x)(x \in X \iff x \in Y),$$

т.е. множества  $X$  и  $Y$  состоят из одних и тех же элементов.

Кроме того, из свойств  $=$  следует, что если  $X = Y$ , то для любого множества  $S$ :

$$(X \in S \iff Y \in S).$$

Всеми этими фактами обычно пользуются без особых оговорок, за исключением *принципа объемности*, который всегда специально выделяется.

Можно было бы определить равенство множеств и так:

$$X = Y \iff (\forall S)(X \in S \iff Y \in S)$$

(тождество неразличимости по Лейбницу).

Внимательный читатель мог заметить, что наши рассуждения оставляют осадок нестрогости. А опытный читатель мог бы предложить следующее: определить отношение  $=$  через отношение  $\in$ , а именно считать  $X = Y$  сокращением для

$$(\forall x)(x \in X \iff x \in Y).$$

Это возможно, но при этом возникают некоторые трудности. Например, не удастся доказать, что тогда для любого множества  $S$ , если  $X = Y$ , то

$$(X \in S \iff Y \in S).$$

Отрицание утверждения  $X = Y$ , т.е.  $\neg(X = Y)$ , по введенному уже соглашению будем обозначать через  $X \neq Y$ .

**Определение 1.1.** Множество  $X$  называется **подмножеством** множества  $Y$ , если каждый элемент из  $X$  является элементом множества  $Y$ , т.е. если

$$(\forall x)(x \in X \implies x \in Y).$$

Запись  $X \subseteq Y$  будет служить сокращением для утверждения  $X$  — *подмножество* множества  $Y$ .



Таким образом, ясно, что

$$X = Y \iff (X \subseteq Y \wedge Y \subseteq X).$$

Если  $X \subseteq Y$  и  $X \neq Y$ , то  $X$  называется *собственным подмножеством* множества  $Y$  и в этом случае пишут  $X \subset Y$ .

Примем следующее соглашение: если мы пишем  $a \in X$  (или  $a \notin X$ ,  $X \subseteq Y$ ,  $X \not\subseteq Y$  и т.д.), то это означает, что мы **утверждаем**, что  $a$  *принадлежит*  $X$  (соответственно, что  $a$  *не принадлежит*  $X$  и т.д.).

**Определение 1.2.** Если  $X$  — произвольное множество, то через  $P(X)$  будем обозначать множество, элементами которого являются всевозможные подмножества множества  $X$  и только они, т.е.

$$(\forall y) (y \in P(X) \iff y \subseteq X).$$

**Определение 1.3.** Множество  $X$ , не содержащее элементов, т.е. обладающее свойством

$$(\forall y) \neg (y \in X),$$

называется **пустым множеством** и обозначается через  $\emptyset$ .

В силу принципа объемности пустое множество единственно, если вообще оно существует.

В дальнейшем мы считаем, что *пустое множество существует*.

Введем следующее соглашение:

знак  $\Rightarrow$  в формуле  $A \Rightarrow B$  означает, что " $A$  есть по определению  $B$ ", знак  $\Leftarrow$  подобен знаку  $:=$ , используемому в языках программирования.

запись  $\{x \mid P(x)\}$  служит обозначением для множества всех таких объектов  $x$ , для которых выполнено условие  $P(x)$ ,

запись  $\{x_1, \dots, x_n\}$  служит обозначением для множества, элементами которого являются  $x_1, \dots, x_n$ .

Над множествами можно производить некоторые операции, позволяющие по имеющимся множествам строить новые множества.

**Определение 1.4.** Объединением множеств  $A$  и  $B$  называется множество

$$A \cup B \Leftarrow \{x \mid x \in A \vee x \in B\}.$$

Для того, чтобы можно было обобщить введенное понятие объединения на случай более чем двух множеств, удобно ввести понятие *семейства объектов, элементов, множеств*.

**Определение 1.5.** Пусть  $I$  — произвольное непустое множество, называемое множеством индексов. Если каждому элементу  $i$  множества  $I$  поставлен в соответствие некоторый объект  $A_i$ , то говорят, что задано **семейство объектов** и пишут  $(A_i)_{i \in I}$  в качестве обозначения этого семейства; объекты  $A_i$  называются **элементами семейства**.

**Замечание.** Не исключено, что при  $i \neq j$   $A_i = A_j$ .

Если каждый элемент семейства является множеством, то говорят, что задано **семейство множеств**.

**Определение 1.6.** Объединением семейства  $(A_i)_{i \in I}$  множеств называется следующее множество:

$$\bigcup_{i \in I} A_i \rightleftharpoons \{x \mid \text{существует } i \in I \text{ такое, что } x \in A_i\}.$$

Мы приходим к следующему принципу (соглашению).

**Принцип существования объединения семейств множеств.** Объединение любого семейства множеств существует.

Ясно, что объединение двух множеств  $A$  и  $B$  можно рассматривать как объединение семейства  $(A_i)_{i \in I}$ , где  $I = \{1, 2\}$ ,  $A_1 = A$ ,  $A_2 = B$ .

**Определение 1.7.** Пересечением семейства  $(A_i)_{i \in I}$  множеств называется множество

$$\bigcap_{i \in I} A_i \rightleftharpoons \{x \mid \text{для любого } i \in I \quad x \in A_i\}.$$

Можно было бы подумать, что необходим принцип, гарантирующий существование пересечения любого семейства множеств, однако мы не будем вводить соответствующий принцип, так как в дальнейшем будет сформулирован более общий принцип, который, однако, не перекроет принцип существования объединения любого семейства множеств.

**Определение 1.8.** Пересечением множеств  $A$  и  $B$  называется множество

$$A \cap B \rightleftharpoons \{x \mid x \in A \wedge x \in B\}.$$

Ясно, что  $A \cap B$  — это пересечение семейства  $(A_i)_{i \in I}$ , где  $I = \{1, 2\}$ ,  $A_1 = A$ ,  $A_2 = B$ .

**Определение 1.9.** Разностью множеств  $A$  и  $B$  называется множество

$$A \setminus B \rightleftharpoons \{x \mid x \in A \wedge x \notin B\}.$$

Если множество  $B$  является подмножеством множества  $A$ , то разность  $A \setminus B$  называется *дополнением  $B$  до  $A$*  и обозначается через  $\mathbb{C}_A B$  или через  $\mathbb{C}B$ , если ясно, о каком множестве  $A$  идет речь.

Для любых множеств  $A, B, C$  верны следующие равенства:

- 1)  $A \cup A = A \cap A = A$ ;
- 2)  $A \cup B = B \cup A$  и  $A \cap B = B \cap A$ ;
- 3)  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$  и  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ ;
- 4)  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$  и  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ ;
- 5)  $(A \cup B) \cap A = A$  и  $A \cup (B \cap A) = A$ ,

доказательство которых предоставляется читателю.

Если  $(A_i)_{i \in I}$  — семейство множеств такое, что каждое  $A_i$  является подмножеством множества  $U$ , называемого в данном случае *универсальным множеством*, то говорят, что задано семейство подмножеств множества  $U$  и в этом случае  $\mathbb{C}A_i$  — это  $\mathbb{C}_U A_i$ .

**Теорема 1.1.** *Выполняются следующие равенства, носящие название формул двойственности (законы де Моргана):*

$$(1) \quad \mathbb{C}\left(\bigcup_{i \in I} A_i\right) = \bigcap_{i \in I} \mathbb{C}A_i, \quad (2) \quad \mathbb{C}\left(\bigcap_{i \in I} A_i\right) = \bigcup_{i \in I} \mathbb{C}A_i.$$

*Доказательство.* Докажем равенство (1). Пусть  $x \in \mathbb{C}\left(\bigcup_{i \in I} A_i\right)$ , тогда  $x \notin \bigcup_{i \in I} A_i$ , поэтому для любого  $i$ :  $x \notin A_i$ , так как в противном случае  $x \in \bigcup_{i \in I} A_i$ . Значит, для любого  $i$ :  $x \in \mathbb{C}A_i$ , поэтому  $x \in \bigcap_{i \in I} \mathbb{C}A_i$ . Тем самым доказано включение

$$\mathbb{C}\left(\bigcup_{i \in I} A_i\right) \subseteq \bigcap_{i \in I} \mathbb{C}A_i. \quad (*)$$

Для доказательства обратного включения предположим, что  $x \in \bigcap_{i \in I} \mathbb{C}A_i$ , тогда при любом  $i$ :  $x \in \mathbb{C}A_i$ , а значит,  $x \notin A_i$ , поэтому  $x \notin \bigcup_{i \in I} A_i$ , что влечет  $x \in \mathbb{C}\left(\bigcup_{i \in I} A_i\right)$ . Тем самым доказано включение

$$\bigcap_{i \in I} \mathbb{C}A_i \subseteq \mathbb{C}\left(\bigcup_{i \in I} A_i\right),$$

что вместе с (\*) в силу принципа объемности дает равенство (1).

Для доказательства равенства (2) заметим, что из (1) следует равенство

$$\mathbb{C}\left(\bigcup_{i \in I} \mathbb{C}A_i\right) = \bigcap_{i \in I} \mathbb{C}(\mathbb{C}A_i).$$

Кроме того, для любых множеств  $A$  и  $B$  из равенства  $A = B$  следует равенство  $\mathbb{C}A = \mathbb{C}B$ , значит

$$\mathbb{C}(\mathbb{C}(\bigcup_{i \in I} \mathbb{C}A_i)) = \mathbb{C}(\bigcap_{i \in I} \mathbb{C}(\mathbb{C}A_i)),$$

по тогда, используя равенство  $\mathbb{C}(\mathbb{C}A) = A$ , получаем

$$\bigcup_{i \in I} \mathbb{C}A_i = \mathbb{C}(\bigcap_{i \in I} A_i).$$

Тем самым доказано, что равенство (2) следует из равенства (1).  $\square$

### У п р а ж н е н и я

1. Доказать, что для любых двух семейств множеств  $(F_t)_{t \in T}$  и  $(G_t)_{t \in T}$  имеют место следующие равенства и включения:

$$1.1. \bigcap_{t \in T} F_t \subseteq F_t \subseteq \bigcup_{t \in T} F_t;$$

$$1.2. \bigcap_{t \in T} (F_t \cap G_t) = (\bigcap_{t \in T} F_t) \cap (\bigcap_{t \in T} G_t);$$

$$1.3. \bigcup_{t \in T} (F_t \cup G_t) = (\bigcup_{t \in T} F_t) \cup (\bigcup_{t \in T} G_t);$$

$$1.4. (\bigcap_{t \in T} F_t) \cup (\bigcap_{t \in T} G_t) = \bigcap_{t \in T} \bigcap_{k \in T} (F_t \cup G_k) \subseteq \bigcap_{t \in T} (F_t \cup G_t);$$

$$1.5. \bigcup_{t \in T} (F_t \cap G_t) \subseteq \bigcup_{t \in T} \bigcup_{k \in T} (F_t \cap G_k) = (\bigcup_{t \in T} F_t) \cap (\bigcup_{t \in T} G_t);$$

$$1.6. A \cup (\bigcap_{t \in T} F_t) = \bigcap_{t \in T} (A \cup F_t);$$

$$1.7. A \cap (\bigcup_{t \in T} F_t) = \bigcup_{t \in T} (A \cap F_t).$$

2. Если при любом  $t \in T$   $A \subseteq F_t$ , то  $A \subseteq \bigcap_{t \in T} F_t$ .

3. Если при любом  $t \in T$   $F_t \subseteq A$ , то  $\bigcup_{t \in T} F_t \subseteq A$ .

## 2. Соответствия, отношения и функции

Покажем, что многие математические понятия могут быть выражены через понятие *множества*, причем эти выражения будут находиться в полном согласии с нашими интуитивными представлениями о соответствующих математических понятиях.

**Определение 2.1.** Пусть  $a$  и  $b$  — некоторые объекты. Обозначим через  $\langle a, b \rangle$  множество  $\{\{a, b\}, \{b\}\}$ , которое будем называть **упорядоченной парой** элементов  $a$  и  $b$ .

То, что таким образом определенное понятие *упорядоченной пары* элементов отвечает нашим интуитивным представлениям об упорядоченной паре объектов, следует из следующей теоремы.

**Теорема 2.1.** Для любых  $a, b, c, d$

$$\langle a, b \rangle = \langle c, d \rangle \iff a = c \ \& \ b = d.$$

*Доказательство.* Если  $a = c, b = d$ , то

$$\{a, b\} = \{c, d\}, \quad \{b\} = \{d\},$$

поэтому и

$$\{\{a, b\}, \{b\}\} = \{\{c, d\}, \{d\}\}.$$

Обратно, пусть  $\langle a, b \rangle = \langle c, d \rangle$ , т.е.

$$\{\{a, b\}, \{b\}\} = \{\{c, d\}, \{d\}\}.$$

Введем обозначения

$$x_1 \Leftarrow \{a, b\}, \quad x_2 \Leftarrow \{b\}, \quad y_1 \Leftarrow \{c, d\}, \quad y_2 \Leftarrow \{d\},$$

$$A \Leftarrow \{\{a, b\}, \{b\}\} = \{x_1, x_2\}, \quad B \Leftarrow \{\{c, d\}, \{d\}\} = \{y_1, y_2\}.$$

Возможны два случая: (1)  $a = b$ , (2)  $a \neq b$ .

Рассмотрим каждый из них.

(1)  $a = b$ . В этом случае

$$A = \{\{a, b\}, \{b\}\} = \{\{a\}, \{a\}\} = \{\{a\}\},$$

поэтому из равенства  $B = \{y_1, y_2\} = \{\{a\}\}$  следует, что  $y_1 = y_2 = \{a\}$ , т.е.  $\{c, d\} = \{a\}$ , поэтому  $c = d = a$ , что вместе с равенством  $a = b$  дает равенство  $a = b = c = d$ .

(2)  $a \neq b$ . Если бы выполнялось равенство  $c = d$ , то, проводя рассуждения, как и в пункте (1), мы получили бы равенства  $c = d = a = b$ , что невозможно, поэтому  $c \neq d$ .

$x_2 \in A$ , значит,  $x_2 \in B$ , откуда  $x_2 = \{d\}$  либо  $x_2 = \{c, d\}$ .

Но второе невозможно, так как тогда мы имели бы равенство  $c = b = d$ , что противоречит неравенству  $c \neq d$ . Значит,  $x_2 = y_2$ .

Аналогично получаем, что  $x_1 = y_1$ , т.е.

$$\{b\} = \{d\}, \quad \{a, b\} = \{c, d\}.$$

Но тогда  $b = d$ . Из равенства  $\{a, b\} = \{c, d\}$  в силу того, что  $a \neq b$  и  $b = d$  следует, что  $a = c$ . □

**Замечание.** Приведенное определение упорядоченной пары элементов было предложено Норбертом Винером и Казимиром Куратовским.

Теперь индукцией по  $n$  ( $n \geq 2$ ) введем понятие *упорядоченного набора из  $n$  элементов* (или понятие *упорядоченной  $n$ -ки элементов*).

При  $n = 2$  это уже сделано.

Переход от  $n$  к  $n + 1$  осуществляется следующим образом

$$\langle a_1, \dots, a_n, a_{n+1} \rangle = \langle \langle a_1, \dots, a_n \rangle, a_{n+1} \rangle,$$

где  $\langle a_1, \dots, a_n \rangle$  обозначает *упорядоченный набор из  $n$  элементов*.

Индукцией по  $n$  доказывается следующая теорема, являющаяся обобщением теоремы 2.1.

**Теорема 2.2.** При любом  $n$  для любых  $a_1, \dots, a_n, b_1, \dots, b_n$  выполняется эквивалентность

$$\langle a_1, \dots, a_n \rangle = \langle b_1, \dots, b_n \rangle \iff a_1 = b_1 \& \dots \& a_n = b_n.$$

**Определение 2.2.** Прямое (декартовое) произведение множеств  $A_1, \dots, A_n$  называется следующее множество:

$$\{ \langle x_1, \dots, x_n \rangle \mid x_1 \in A_1 \& \dots \& x_n \in A_n \},$$

обозначаемое через  $A_1 \times \dots \times A_n$  или  $\prod_{i=1}^n A_i$ .

В случае, когда  $A_1 = \dots = A_n = A$ , множество  $A_1 \times \dots \times A_n$  называется **прямой (декартовой) степенью множества  $A$**  и обозначается через  $A^n$ .

**Определение 2.3.** Любое множество  $R$  упорядоченных пар называется **двуместным или бинарным отношением или соответствием**, т.е.  $R$  — **бинарное отношение**, если для любого  $x \in R$  найдутся такие  $u, v$ , что  $x = \langle u, v \rangle$ .

Если для бинарного отношения  $R$  множества  $A$  и  $B$  таковы, что

$$R \subseteq A \times B,$$

то  $R$  называется **бинарным отношением между элементами множеств  $A$  и  $B$**  (именно в таком порядке) или **соответствием из  $A$  в  $B$** , при этом множество  $A$  называется **областью отправления** соответствия  $R$ , а  $B$  — его **областью прибытия**; если же  $R \subseteq A \times A$ , то  $R$  называется **бинарным отношением на  $A$** .

Если  $\langle u, v \rangle \in R$ , то говорят, что элементы  $u$  и  $v$  *находятся в отношении  $R$*  и пишут  $u R v$ .

С каждым бинарным отношением  $R$  естественным образом связаны два множества, называемые *областью определения* и, соответственно, *областью значений* (областью изменения) бинарного отношения  $R$  (в этом контексте уместнее было бы говорить о *соответствии  $R$  из  $A$  в  $B$* , а не об отношении, чтобы подчеркнуть несимметричность отношения  $R$  относительно  $A$  и  $B$ ).

**Определение 2.4.** Областью определения бинарного отношения  $R$  называется следующее множество:

$$\{x \mid \text{существует } v \text{ такое, что } \langle x, v \rangle \in R\},$$

обозначаемое через  $\delta(R)$ .

**Определение 2.5.** Областью значений бинарного отношения  $R$  называется следующее множество:

$$\{y \mid \text{существует } x \text{ такое, что } \langle x, y \rangle \in R\},$$

обозначаемое через  $\rho(R)$ .

Ясно, что для любого бинарного отношения  $R$ :

$$R \subseteq \delta(R) \times \rho(R)$$

и множества  $\delta(R)$  и  $\rho(R)$  минимальны в том смысле, что если

$$R \subseteq A \times B$$

то  $\delta(R) \subseteq A$  и  $\rho(R) \subseteq B$ .

**Определение 2.6.** С каждым бинарным отношением  $R$  естественным образом связывается бинарное отношение  $R^c$ , называемое **обращением отношения  $R$**  (или **обратным отношением** для бинарного отношения  $R$ )

$$R^c \Rightarrow \{\langle x, y \rangle \mid \langle y, x \rangle \in R\}.$$

Ясно, что

$$\delta(R^c) = \rho(R), \quad \rho(R^c) = \delta(R), \quad (R^c)^c = R.$$

Над бинарными отношениями, как и над любыми множествами, можно производить теоретико-множественные операции объединения  $\cup$ , пересечения  $\cap$ , вычитания и т.д.

Однако можно ввести более важную операцию над бинарными отношениями, называемую *умножением отношений*, а именно по отношениям  $R$  и  $S$  можно следующим образом определить новое отношение, называемое *произведением отношений  $R$  и  $S$* .

**Определение 2.7.** Произведением отношений  $R$  и  $S$  называется следующее отношение

$$R \circ S \Rightarrow \{\langle x, y \rangle \mid \text{существует } v \text{ такое, что } xSv \text{ и } vRy\}.$$

Ясно, что

$$\delta(R \circ S) \subseteq \delta(S), \quad \rho(R \circ S) \subseteq \rho(R).$$



**Определение 2.8.** Бинарное отношение  $R$  называется **отображением** или **функцией**, если для любых  $x, y, z$  из того, что

$$x R y \quad \text{и} \quad x R z$$

следует, что  $y = z$ .

Итак, по нашей терминологии **отображение (функция)** — это любое бинарное отношение, обладающее указанным в определении свойством. Это свойство называется **функциональностью** отношения  $R$ .

Если  $R$  — отображение,  $A = \delta(R)$ ,  $B \supseteq \rho(R)$ , то будем говорить, что  $R$  — отображение  $A$  в  $B$ .

Запись

$$R : A \rightarrow B$$

будет служить сокращением для утверждения “ $R$  — отображение  $A$  в  $B$ ”.

Множество всех отображений  $A$  в  $B$  обозначается через  $B^A$ .

Если  $R$  — отображение  $A$  в  $B$ , то для любого  $x \in A = \delta(R)$  найдется единственный элемент  $y \in B$  такой, что  $\langle x, y \rangle \in R$  (или в других обозначениях  $x R y$ ), этот элемент  $y$  обозначается через  $R(x)$  и называется **значением** отображения  $R$  на элементе  $x$  или **в точке**  $x$ .

Рассмотрим теперь следующий вопрос: в каком случае обращение  $R^c$  функции  $R$  само является функцией?

Для ответа на этот вопрос введем важное понятие **1-1-отображения**.

**Определение 2.9.** Отображение (функция)  $R$  называется **1-1-отображением (1-1-функцией)**, если для любых  $x_1$  и  $x_2$  из  $\delta(R)$  равенство  $R(x_1) = R(x_2)$  влечет равенство  $x_1 = x_2$ .

**Замечание.** 1-1-отображение называется еще **инъективным отображением** или **инъекцией**.

**Теорема 2.3.** Для того, чтобы обращение  $R^c$  отображения (функции) само было отображением (функцией), необходимо и достаточно, чтобы отображение (функция)  $R$  было 1-1-функцией.

*Доказательство.* Пусть  $R^c$  — функция. Покажем, что  $R$  — 1-1-отображение. Если  $x_1, x_2 \in \delta(R)$  и

$$R(x_1) = R(x_2) = y,$$

то  $x_1 R y$  и  $x_2 R y$ , значит,  $y R^c x_1$  и  $y R^c x_2$ , но по предположению  $R^c$  — функция, поэтому  $x_1 = x_2$ , значит,  $R$  — инъекция.

Обратно, пусть  $R$  — инъекция. Покажем, что  $R^c$  — функция. Если  $y, x_1, x_2$  — такие элементы, что

$$y R^c x_1 \quad \text{и} \quad y R^c x_2,$$

то

$$x_1 R y \quad \text{и} \quad x_2 R y,$$

что в силу инъективности  $R$  влечет равенство  $x_1 = x_2$ , т.е.  $R^c$  — функция.  $\square$



**Теорема 2.4.** Если  $R$  и  $S$  — отображения (функции), то  $R \circ S$  — отображение (функция).

*Доказательство.* Если  $x, y, z$  — такие элементы, что

$$x(R \circ S)y, \quad x(R \circ S)z,$$

то найдутся такие элементы  $u, v$ , что

$$xSu, \quad uRy,$$

$$xSv, \quad vRz.$$

Так как  $S$  — отображение, то из  $xSu, xSv$  следует, что  $u = v$ .

Тогда, так как  $R$  — отображение, то из  $uRy, uRz$  следует, что  $y = z$ .  $\square$

**Замечание 1.** Если  $\rho(S) \subseteq \delta(R)$ , то  $\delta(R \circ S) = \delta(S)$ . Если же  $\rho(S) = \delta(R)$ , то  $\rho(R \circ S) = \rho(R)$ .

**Замечание 2.** Если  $R$  и  $S$  — отображения, то, как только что доказано,  $R \circ S$  тоже является отображением. Пусть  $x \in \delta(R \circ S)$ , рассмотрим вопрос о вычислении значения  $(R \circ S)(x)$ . Так как  $\langle x, (R \circ S)(x) \rangle \in R \circ S$ , то найдется элемент  $v$ , такой что  $\langle x, v \rangle \in S$ ,  $\langle v, (R \circ S)(x) \rangle \in R$ , но тогда  $v = S(x)$  и  $(R \circ S)(x) = R(v)$ , поэтому получаем равенство

$$(R \circ S)(x) = R(S(x)),$$

которое показывает, что в случае, когда  $R$  и  $S$  — функции,  $R \circ S$  — это хорошо известная из курса математического анализа их суперпозиция или, как часто говорят, сложная функция.

**Теорема 2.5.** Если  $R$  и  $S$  — инъективные отображения, то  $R \circ S$  — инъективное отображение.

*Доказательство.* По теореме 2.4  $R \circ S$  — отображение, значит, остается доказать его инъективность. Если  $u, v$  — такие элементы из  $\delta(R \circ S)$ , что

$$(R \circ S)(u) = (R \circ S)(v).$$

По замечанию 2 последнее равенство можно переписать в следующем виде

$$R(S(u)) = R(S(v)).$$

Так как  $R$  — инъекция, то из последнего равенства получаем равенство

$$S(u) = S(v),$$

которое в свою очередь дает нужное нам равенство

$$u = v.$$

$\square$

Рассмотрим наиболее важные для дальнейшего виды отображений.

**Определение 2.10.** *Отображение  $f$  множества  $A$  во множество  $B$  называется **инъективным отображением** (инъекцией, вложением), если для любых  $u$  и  $v$  из  $A$  из того, что  $u \neq v$  следует, что  $f(u) \neq f(v)$ .*

Часто бывает удобно использовать определение инъективного отображения в следующей форме, конечно, равносильной предыдущей форме

**Определение 2.11.** *Отображение  $f$  множества  $A$  во множество  $B$  называется **инъективным отображением** (инъекцией, вложением), если для любых  $u$  и  $v$  из  $A$  из того, что  $f(u) = f(v)$  следует, что  $u = v$ .*

В дальнейшем запись  $f : A \mapsto B$  будет служить для сокращенного обозначения утверждения “ $f$  — инъективное отображение множества  $A$  во множество  $B$ ”.

**Определение 2.12.** *Отображение  $f$  множества  $A$  во множество  $B$  называется **сюръективным отображением** (сюръекцией, отображением на), если  $\rho(f) = B$ , т.е. если для любого элемента  $y \in B$  найдется такой элемент  $x$  в  $A$ , что  $y = f(x)$ .*

В дальнейшем запись  $f : A \rightarrow B$  будет служить для сокращенного обозначения утверждения  $f$  — сюръективное отображение множества  $A$  на множество  $B$ .

**Теорема 2.6.** *Если  $S$  — сюръективное отображение множества  $A$  на множество  $B$ , а  $R$  — сюръективное отображение множества  $B$  на множество  $C$ , то  $R \circ S$  — сюръективное отображение множества  $A$  на множество  $C$ .*

*До к а з а т е л ь с т в о.* Ясно, что  $R \circ S$  — отображение множества  $A$  во множество  $C$ . Остается доказать его сюръективность. Пусть  $z$  — произвольный элемент множества  $C$ . Так как  $R$  — сюръективное отображение множества  $B$  на множество  $C$ , то во множестве  $B$  найдется элемент  $y$  такой, что  $z = R(y)$ . Но  $S$  — сюръективное отображение множества  $A$  на множество  $B$ , поэтому во множестве  $A$  найдется такой элемент  $x$ , что  $y = S(x)$ .

Окончательно получаем

$$z = R(y) = R(S(x)) = (R \circ S)(x).$$

□

**Определение 2.13.** *Отображение  $f$  множества  $A$  во множество  $B$  называется **биективным**, если оно одновременно является инъективным и сюръективным отображением множества  $A$  на множество  $B$ .*

В дальнейшем запись  $f : A \rightarrow B$  будет служить для сокращенного обозначения утверждения  $f$  — биективное отображение множества  $A$  на множество  $B$ .

**Замечание.** Если  $R$  — биективное отображение множества  $A$  на множество  $B$ , то будем говорить, что  $R$  осуществляет **взаимнооднозначное соответствие** между множествами  $A$  и  $B$ .

**Теорема 2.7.** Если  $S$  — биективное отображение множества  $A$  на множество  $B$ , а  $R$  — биективное отображение множества  $B$  на множество  $C$ , то  $R \circ S$  — биективное отображение множества  $A$  на множество  $C$ .

*Доказательство* сразу следует из теоремы 2.5 и теоремы 2.6.  $\square$

Теперь мы рассмотрим важный вопрос об обратимости отображений (функций).

**Определение 2.14.** Для произвольного множества  $X$  обозначим через  $i_X$  следующее отображение

$$i_X : X \rightarrow X, \quad i_X(u) = u \quad \text{при любом } u \in X.$$

Легко понять, что  $i_X$  — биективное отображение множества  $X$  на себя.  $i_X$  называется **тождественным отображением** множества  $X$ .

**Определение 2.15.** Отображение  $R : A \rightarrow B$  множества  $A$  во множество  $B$  называется **обратимым**, если существует такое отображение  $S : B \rightarrow A$  множества  $B$  во множество  $A$ , что

$$S \circ R = i_A, \quad R \circ S = i_B.$$

**Замечание.** Нетрудно доказать, что если для отображения  $R : A \rightarrow B$  множества  $A$  во множество  $B$  существует такое отображение  $S : B \rightarrow A$  множества  $B$  во множество  $A$ , что

$$S \circ R = i_A, \quad R \circ S = i_B,$$

то отображение  $S$  определено однозначно, оно называется **обратным отображением** для отображения  $R$  и обозначается через  $R^{-1}$ .

**Теорема 2.8.** Отображение  $R : A \rightarrow B$  множества  $A$  во множество  $B$  является **обратимым** тогда и только тогда, когда  $R$  — **биекция** множества  $A$  на множество  $B$  и в случае обратимости отображения  $R$  обратным для него отображением является  $R^c$ , т.е.  $R^{-1} = R^c$ .

*Доказательство.* Пусть отображение  $R : A \rightarrow B$  множества  $A$  во множество  $B$  является *обратимым* и  $S$  — такое отображение  $S : B \rightarrow A$  множества  $B$  во множество  $A$ , что

$$S \circ R = i_A, \quad R \circ S = i_B.$$

Покажем, что  $R$  — *биекция*.

Прежде всего убедимся в инъективности  $R$ .

Если  $u, v$  — такие элементы из множества  $A$ , что  $R(u) = R(v)$ .

Применяя к обеим частям последнего равенства отображение  $S$ , получим равенство

$$S(R(u)) = S(R(v)),$$

из которого получаем равенства

$$(S \circ R)(u) = (S \circ R)(v), \quad i_A(u) = i_A(v), \quad u = v.$$

Значит,  $R$  — инъективное отображение.

Чтобы убедиться в сюръективности отображения  $R$ , возьмем произвольный элемент  $y$  во множестве  $B$ , а через  $x$  обозначим элемент  $S(y)$  из множества  $A$ . Тогда получим

$$R(x) = R(S(y)) = (R \circ S)(y) = i_B(y) = y,$$

поэтому  $R$  — сюръекция, а значит,  $R$  — биективное отображение множества  $A$  на множество  $B$ .

Для доказательства обратного утверждения предположим, что  $R : A \rightarrow B$  — биективное отображение множества  $A$  на множество  $B$ .

Рассмотрим соответствие  $R^c$  из множества  $B$  во множество  $A$ .

По теореме 2.3  $R^c$  — *отображение*, а так как

$$\delta(R^c) = \rho(R) = B,$$

то  $R^c$  — отображение множества  $B$  во множество  $A$ . Проверка выполнимости равенств

$$R \circ S = i_B, \quad S \circ R = i_A$$

предоставляется читателю в качестве легкого упражнения. □

В качестве некоторого дополнения к только что доказанной теореме 2.8 может рассматриваться следующая теорема.

**Теорема 2.9.** *Для того, чтобы отношение  $R$  между элементами множеств  $A$  и  $B$  осуществляло взаимнооднозначное соответствие между  $A$  и  $B$ , необходимо и достаточно, чтобы выполнялись равенства*

$$R \circ R^c = i_B, \quad R^c \circ R = i_A.$$

*Доказательство.* Если отношение  $R$  между элементами множеств  $A$  и  $B$  осуществляет **взаимнооднозначное соответствие между  $A$  и  $B$** , т.е.  $R$  является **биективным** отображением множества  $A$  на множество  $B$ , то легко доказать, что выполняются равенства

$$R \circ R^c = i_B, \quad R^c \circ R = i_A.$$

Чтобы доказать обратное утверждение, предположим, что выполняются равенства

$$R \circ R^c = i_B, \quad R^c \circ R = i_A.$$

Покажем, что  $R$  — биективное отображение множества  $A$  на множество  $B$ . Если  $u \in A, v, w \in B$  и

$$u R v, \quad u R w,$$

то

$$v R^c u, \quad w R^c u.$$

В частности,

$$v R^c u, \quad u R w,$$

поэтому

$$v R \circ R^c w,$$

но  $R \circ R^c = i_B$ , значит,  $v i_B w$ , т.е.  $i_B(v) = w$ . Но  $i_B(v) = v$ , следовательно,  $v = w$ , т.е.  $R$  — **отображение**.

Так как  $\delta(R_c \circ R) \subseteq \delta(R)$ , то  $\delta(i_A) \subseteq \delta(R)$ . Но  $\delta(i_A) = A$ , значит,  $A \subseteq \delta(R)$ , что вместе с  $\delta(R) \subseteq A$  дает равенство  $\delta(R) = A$ .

Поэтому  $R$  — **отображение** множества  $A$  во множество  $B$ .

Совершенно аналогично доказывается, что  $R^c$  — **отображение** множества  $B$  во множество  $A$ .

Так как по предположению выполняются равенства

$$R \circ R^c = i_B, \quad R^c \circ R = i_A,$$

то  $R$  — **обратимое** отображение множества  $A$  во множество  $B$ , поэтому по теореме 2.8  $R$  — **биекция**.  $\square$

**Теорема 2.10.** Для любых бинарных отношений  $R, S$  и  $U$  выполняются следующие равенства

$$(1) \quad (R \circ S) \circ U = R \circ (S \circ U),$$

$$(2) \quad (R \circ S)^c = S^c \circ R^c.$$

*Доказательство.* Докажем равенство (1).

$$\begin{aligned}
 x((R \circ S) \circ U)y &\iff (\exists v)(xUv \& v(R \circ S)y) \iff \\
 &\iff (\exists v)(xUv \& (\exists w)vSw \& wRy) \iff (\exists v)(\exists w)(xUv \& vSw \& wRy) \iff \\
 &\iff (\exists w)(\exists v)(xUv \& vSw \& wRy) \iff \\
 &\iff (\exists w)\big((\exists v)(xUv \& vSw) \& wRy\big) \iff \\
 &\iff (\exists w)\big((x(U \circ S)w) \& wRy\big) \iff \\
 &\iff x(R \circ (S \circ U))y.
 \end{aligned}$$

Докажем равенство (2).

$$\begin{aligned}
 x(R \circ S)^c y &\iff y(R \circ S)x \iff \\
 &\iff (\exists v)(ySv \& vRx) \iff \\
 &\iff (\exists v)(xR^c v \& vS^c y) \iff \\
 &\iff x(R^c \circ S^c)y.
 \end{aligned}$$

□

**Определение 2.16.** Пусть  $R$  — бинарное отношение, а  $X$  — произвольное множество. **Образом** множества  $X$  относительно  $R$  называется следующее множество

$$R(X) = \{y \mid \text{существует } x \in X \text{ такой, что } xRy\}.$$

**Прообразом** множества  $X$  относительно  $R$  называется следующее множество

$$R^{-1}(X) = \{x \mid \text{существует } y \in X \text{ такой, что } xRy\}.$$

**Замечание.** Нетрудно понять, что **прообраз** множества  $X$  относительно  $R$  — это просто **образ** множества  $X$ , но относительно  $R^c$ , т.е. имеет место равенство

$$R^{-1}(X) = R^c(X).$$

**Теорема 2.11.** Для любого отношения  $R$  имеют место следующие равенства и включения:

- (1)  $R(\bigcup_{i \in I} A_i) = \bigcup_{i \in I} R(A_i);$
- (2)  $R(\bigcap_{i \in I} A_i) \subseteq \bigcap_{i \in I} R(A_i);$
- (3)  $R^{-1}(\bigcup_{i \in I} A_i) = \bigcup_{i \in I} R^{-1}(A_i);$
- (4) если  $R$  — функция, то  $R^{-1}(\bigcap_{i \in I} A_i) = \bigcap_{i \in I} R^{-1}(A_i);$
- (5) если  $A \subseteq B$ , то  $R(A) \subseteq R(B);$
- (6) если  $A \subseteq B$ , то  $R^{-1}(A) \subseteq R^{-1}(B).$

*Доказательство.* (1) Если  $x \in R(\bigcup_{i \in I} A_i)$ , то в  $\bigcup_{i \in I} A_i$  найдется элемент  $v$  такой, что  $vRx$ . Так как  $v \in \bigcup_{i \in I} A_i$ , то найдется такое  $i \in I$ , что  $v \in A_i$ , поэтому  $x \in R(A_i)$ , а значит,  $x \in \bigcup_{i \in I} R(A_i)$ .

Следовательно, имеет место включение

$$R(\bigcup_{i \in I} A_i) \subseteq \bigcup_{i \in I} R(A_i). \quad (*)$$

Пусть  $x \in \bigcup_{i \in I} R(A_i)$ , тогда при некотором  $i \in I$   $x \in R(A_i)$ , значит, есть такой элемент  $v$  в  $A_i$ , что  $vRx$ , но тогда  $v \in \bigcup_{i \in I} A_i$ , значит,  $x \in R(\bigcup_{i \in I} A_i)$ , поэтому

$$\bigcup_{i \in I} R(A_i) \subseteq R(\bigcup_{i \in I} A_i). \quad (**)$$

Из включений (\*) и (\*\*) в силу принципа объемности следует равенство (1).

(2) Если  $x \in R(\bigcap_{i \in I} A_i)$ , то найдется элемент  $v \in \bigcap_{i \in I} A_i$  такой, что  $vRx$ . Так как при любом  $i \in I$ :  $v \in A_i$ , то можно утверждать, что для любого  $i \in I$  найдется элемент  $v$  в  $A_i$  такой, что  $vRx$ , значит,  $x \in R(A_i)$  для любого  $i$ , поэтому  $x \in \bigcap_{i \in I} R(A_i)$ .

(3) сразу следует из (1), если вспомнить, что  $R^{-1}(X) = R^c(X)$ .

(4) Включение

$$R^{-1}(\bigcap_{i \in I} A_i) \subseteq \bigcap_{i \in I} R^{-1}(A_i)$$

сразу следует из (2), так как  $R^{-1}(X) = R^c(X)$ .

Докажем обратное включение. Пусть

$$x \in \bigcap_{i \in I} R^{-1}(A_i),$$

тогда при любом  $i \in I$ :  $x \in R^{-1}(A_i)$ , значит,  $R(x) \in A_i$ , поэтому  $R(x) \in \bigcap_{i \in I} A_i$ , что вместе с  $x$   $RR(x)$  влечет

$$x \in R^{-1}(\bigcap_{i \in I} A_i).$$

Включение (6) сразу следует из (3).

(5) Если  $x \in R(A)$ , то найдется элемент  $v$  такой, что  $v \in A$ ,  $vRx$ , но тогда в силу включения  $A \subseteq B$   $v \in B$ , значит,  $x \in R(B)$ . □

Как уже отмечалось выше, множество всех функций из  $A$  в  $B$  обозначается через  $B^A$ .

Пусть  $(A_i)_{i \in I}$  — произвольное семейство множеств.



**Определение 2.17.** Декартовым произведением семейства множеств  $(A_i)_{i \in I}$  называется следующее множество:

$$\prod_{i \in I} A_i = \{ f \mid f : I \rightarrow \bigcup_{i \in I} A_i \text{ и для каждого } i \in I \quad f(i) \in A_i \}.$$

В качестве одного из важных принципов канторовской теории множеств примем следующий.

**Аксиома мультипликативности.** Декартово произведение непустого семейства непустых множеств непусто, т.е. если  $I \neq \emptyset$  и при любом  $i \in I$   $A_i \neq \emptyset$ , то и  $\prod_{i \in I} A_i \neq \emptyset$ .

**Замечание.** Данное выше определение понятия семейства элементов является недостаточно четким, однако его можно уточнить, используя уже введенное понятие функции.

Пусть  $I$  — любое множество, называемое *множеством индексов*, а  $X$  — любое множество.

**Определение 2.18.** Семейством элементов множества  $X$  с множеством индексов  $I$  называется любая функция  $f : I \rightarrow X$ .

**Определение 2.19.**  $n$ -местным отношением на множестве  $A$  назовем любое подмножество множества  $A^n$ .

Любая функция  $f : A^n \rightarrow B$  называется  $n$ -местной функцией из  $A$  в  $B$ . При этом пишут  $b = f(a_1, \dots, a_n)$  вместо  $b = f(\langle a_1, \dots, a_n \rangle)$ ,  $b$  называют значением функции  $f$  при значениях аргументов  $a_1, \dots, a_n$  или в точке  $\langle a_1, \dots, a_n \rangle$ .

**Определение 2.20.**  $n$ -местным предикатом, определенном на множестве  $A$ , называется любая  $n$ -местная функция из множества  $A$  во множество  $\{И, Л\}$ , состоящее из двух элементов И — “истина”, Л — “ложь”.

Между  $n$ -местными предикатами, определенными на множестве  $A$ , и  $n$ -местными отношениями на  $A$  естественным образом устанавливается взаимно однозначное соответствие, если каждому  $n$ -местному предикату  $P$  поставить в соответствие отношение

$$R_P = \{ \langle a_1, \dots, a_n \rangle \mid a_1, \dots, a_n \in A \text{ и } P(a_1, \dots, a_n) = И \}.$$

### У п р а ж н е н и я

1. Доказать, что  $(\bigcap_{i \in I} A_i) \times (\bigcap_{i \in I} B_i) = \bigcap_{i \in I} (A_i \times B_i)$ .



2. Доказать, что

$$\left( \bigcup_{i \in I} R_i \right) \circ Q = \bigcup_{i \in I} (R_i \circ Q), \quad Q \circ \left( \bigcup_{i \in I} R_i \right) = \bigcup_{i \in I} (Q \circ R_i).$$

3. Если  $U$  — непустое множество, то для произвольного его подмножества  $A$  обозначим через  $\chi_A^U$  *характеристическую функцию множества  $A$* , заданную следующим образом:

$$\chi_A^U = 1, \text{ если } x \in A \quad \text{и } 0, \text{ если } x \in U \setminus A.$$

Определим отображение

$$F : P(U) \rightarrow \{0, 1\}^U$$

следующим образом:

$$F(A) \equiv \chi_A^U \quad \text{для любого } A \in P(U).$$

Доказать, что  $F$  — биективное отображение  $P(U)$  на  $\{0, 1\}^U$ .

4. Доказать, что

$$(1) \quad \chi_U^U(x) \equiv 1,$$

$$(2) \quad \chi_\emptyset^U(x) \equiv 0,$$

$$(3) \quad \chi_{U \setminus A}^U(x) = 1 - \chi_A^U(x),$$

$$(4) \quad \chi_{A \cap B}^U(x) = \chi_A^U(x) \cdot \chi_B^U(x),$$

$$(5) \quad \chi_{A \cup B}^U(x) = \chi_A^U(x) + \chi_B^U(x) - \chi_A^U(x) \cdot \chi_B^U(x),$$

$$(6) \quad \chi_{\bigcup_{i \in I} A_i}^U(x) = \max_{i \in I} \chi_{A_i}^U(x),$$

$$(7) \quad \chi_{\bigcap_{i \in I} A_i}^U(x) = \min_{i \in I} \chi_{A_i}^U(x).$$

5. Задать биективное отображение  $A^n$  на  $A^I$ , где  $I = \{1, 2, \dots, n\}$ .

6. Доказать, что если при любых различных  $i, j$  из  $I$  множества  $A_i$  и  $A_j$  не пересекаются, то можно задать биективное отображение множества

$$B^{\left(\bigcup_{i \in I} A_i\right)}$$

на множество

$$\prod_{i \in I} B^{A_i}.$$

7. Доказать, что если для любых множеств  $A$ ,  $B$  и  $C$  можно задать биективное отображение множества

$$A^{B \times C} \quad \text{на множество} \quad (A^B)^C.$$

8. Задать биективное отображение множества

$$\left( \prod_{i \in I} A_i \right)^A$$

на множество

$$\prod_{i \in I} A_i^A.$$

9. Задать биективное отображение множества

$$\prod_{i \in I} A_i$$

на множество

$$\left( \prod_{i \in I_1} A_i \right) \times \left( \prod_{i \in I_2} A_i \right),$$

если

$$I = I_1 \cup I_2 \quad I_1 \cap I_2 = \emptyset.$$

Можно ли задать соответствующее биективное отображение при  $I_1 \cap I_2 \neq \emptyset$ ?

10. Пусть  $(A_i)_{i \in I}$  — семейство множеств, а  $\varphi$  — биективное отображение множества  $I$  на себя. Доказать, что выполняется равенство

$$\bigcup_{i \in I} A_i = \bigcup_{i \in I} A_{\varphi(i)}.$$

Задать биективное отображение множества

$$\prod_{i \in I} A_i$$

на множество

$$\prod_{i \in I} A_{\varphi(i)}.$$

### 3. Некоторые специальные отношения

Одним из важнейших двуместных отношений является *отношение эквивалентности*.

**Определение 3.1.** *Отношением эквивалентности или просто эквивалентностью на множестве  $A$  называется каждое двуместное отношение  $R$  на множестве  $A$ , удовлетворяющее следующим трем условиям:*

- (1) **рефлексивность:** для любого элемента  $a \in A$ :  $aRa$ ;
- (2) **симметричность:** для любых элементов  $a, b \in A$ :  
если  $aRb$ , то  $bRa$ ;
- (3) **транзитивность:** для любых элементов  $a, b, c \in A$ :  
если  $aRb$  и  $bRc$ , то  $aRc$ .

**Замечание.** Обозначим через  $\Delta_A$  так называемую *диагональ* множества  $A$ , положив

$$\Delta_A = \{ \langle a, a \rangle \mid a \in A \}.$$

Тогда рефлексивность отношения  $R$  означает, что  $\Delta_A \subseteq R$ .

Симметричность отношения  $R$  означает, что  $R^c = R$ .

Транзитивность отношения  $R$  означает, что  $R \circ R \subseteq R$ .

Приведем наиболее распространенные обозначения для отношений эквивалентности:  $=, \equiv, \sim, \approx$ .

В дальнейшем произвольное отношение эквивалентности мы обычно будем обозначать через  $\equiv$ .

Пусть  $\equiv$  — отношение эквивалентности на множестве  $A$ , а  $a$  — элемент этого множества.

**Определение 3.2.** *Классом эквивалентности (смежным классом) элемента  $a$  по отношению эквивалентности  $\equiv$  называется множество*

$$[a]_{\equiv} = \{ x \mid x \in A \text{ \& } a \equiv x \}.$$

Обычно индекс  $\equiv$  опускается, т.е. вместо записи  $[a]_{\equiv}$  используется запись  $[a]$ .

**Определение 3.3.** *Множество всех классов эквивалентности по отношению эквивалентности  $\equiv$ , определенному на множестве  $A$ , называется **фактормножеством** множества  $A$  по отношению эквивалентности  $\equiv$ .*

Фактормножество множества  $A$  по отношению эквивалентности  $\equiv$  обозначается через  $A / \equiv$ .

Следующая теорема устанавливает важнейшие свойства классов эквивалентности.

**Теорема 3.1.** (1) Для любого  $a \in A$ :  $a \in [a]$ .

(2) Если  $b \in [a]$ , то  $[a] = [b]$ .

(3) Если  $[a] \cap [b] \neq \emptyset$ , то  $[a] = [b]$ , т.е. любые два различных смежных класса не пересекаются.

(4)  $A = \bigcup_{a \in A} [a]$ .

*Доказательство.* (1) В силу рефлексивности имеем  $a \equiv a$ , значит,  $a \in [a]$ .

(2) Пусть  $b \in [a]$ , тогда  $a \equiv b$ , поэтому в силу симметричности  $b \equiv a$ , значит,  $a \in [b]$ .

Если  $x \in [b]$ , то  $b \equiv x$ , откуда используя  $a \equiv b$  в силу транзитивности получаем  $b \equiv x$ , значит,  $[b] \subseteq [a]$ .

Аналогичным образом из  $a \in [b]$  следует, что  $[a] \subseteq [b]$ . Значит,  $[a] = [b]$ .

(3) Если  $[a] \cap [b] \neq \emptyset$ , то пусть  $c \in [a] \cap [b]$ . Тогда в силу (2)  $[a] = [c] = [b]$ .

(4) сразу следует из (1). □

В определении класса эквивалентности участвовал элемент  $a$ . Следующая теорема показывает, что без этого можно обойтись.

**Теорема 3.2.** Непустое подмножество  $B$  множества  $A$  является классом эквивалентности по отношению эквивалентности  $\equiv$  тогда и только тогда, когда

(1) для любых элементов  $a$  и  $b$  из  $B$   $a \equiv b$ ,

(2) для любых элементов  $a$  и  $b$  из условий  $a \in B$  и  $a \equiv b$  следует, что  $b \in B$ .

*Доказательство.* Пусть  $B$  — класс эквивалентности по отношению эквивалентности  $\equiv$ , тогда найдется такой элемент  $c$ , что  $B = [c]$ .

Если  $a$  и  $b$  из  $B = [c]$ , то  $a \equiv c$ ,  $b \equiv c$ , значит,  $a \equiv b$ .

Если  $a \in B = [c]$ , то  $[a] = [c]$ . Если к тому же  $a \equiv b$ , то  $[a] = [b]$ . Поэтому  $b \in [b] = B$ .

Теперь предположим, что непустое подмножество  $B$  множества  $A$  удовлетворяет условиям:

(1) для любых элементов  $a$  и  $b$  из  $B$   $a \equiv b$ ,

(2) для любых элементов  $a$  и  $b$  из условий  $a \in B$  и  $a \equiv b$  следует, что  $b \in B$ .

Пусть  $a \in B$ . Покажем, что  $[a] = B$ . Если  $x \in [a]$ , то  $a \equiv x$ , что вместе с  $a \in B$  дает  $x \in B$ , значит,  $[a] \subseteq B$ .

Если  $x \in B$ , то из  $a \in B$  следует, что  $a \equiv x$ , значит,  $x \in [a]$ , поэтому  $B \subseteq [a]$ .

Значит,  $[a] = B$ . □

**Определение 3.4.** Непустое множество  $\mathcal{U}$  непустых попарно непересекающихся подмножеств множества  $A$ , объединение которого совпадает со всем  $A$ , называется **разбиением** множества  $A$ .

В следующих теоремах доказывается, что изучать отношения эквивалентности на множестве  $A$  то же самое, что изучать разбиения этого множества.

**Теорема 3.3.** Если  $\mathcal{U}$  — разбиение множества  $A$ , то отношение  $R_{\mathcal{U}}$ , определяемое следующим образом

$$x R_{\mathcal{U}} y \iff \text{существует множество } X \in \mathcal{U} \text{ такое, что } x, y \in X,$$

является отношением эквивалентности на  $A$ .

*Д о к а з а т е л ь с т в о.* Пусть  $\mathcal{U}$  — разбиение множества  $A$ . Покажем, что определенное в формулировке теоремы отношение  $R_{\mathcal{U}}$  является отношением эквивалентности, т.е. обладает свойствами рефлексивности, симметричности и транзитивности.

(1) Рефлексивность. Если  $a \in A$ , то в силу равенства  $A = \bigcup_{X \in \mathcal{U}} X$ , найдется такое множество  $X \in \mathcal{U}$ , что  $a \in X$ , значит,  $a R_{\mathcal{U}} a$ .

(2) Симметричность отношения  $R_{\mathcal{U}}$  сразу следует из его определения.

(3) Транзитивность. Пусть  $a R_{\mathcal{U}} b$  и  $b R_{\mathcal{U}} c$ . Тогда найдутся в  $\mathcal{U}$  такие множества  $X$  и  $Y$ , что  $a, b \in X$  и  $b, c \in Y$ . Тогда  $b \in X \cap Y$ . Отсюда по определению разбиения получаем, что  $X = Y$ , значит,  $a, c \in X$ , поэтому  $a R_{\mathcal{U}} c$ .  $\square$

**Теорема 3.4.** Если  $\mathcal{U}, \mathcal{V}$  — различные разбиения множества  $A$ , то  $R_{\mathcal{U}}$  и  $R_{\mathcal{V}}$  — различные отношения эквивалентности.

*Д о к а з а т е л ь с т в о.* Пусть  $\mathcal{U}, \mathcal{V}$  — различные разбиения множества  $A$ , покажем, что  $R_{\mathcal{U}}$  и  $R_{\mathcal{V}}$  — различные отношения эквивалентности. Для этого покажем, что равенство  $R_{\mathcal{U}} = R_{\mathcal{V}}$  влечет равенство  $\mathcal{U} = \mathcal{V}$ .

Пусть  $X \in \mathcal{U}$ . Возьмем  $x \in X$ . Так как  $A = \bigcup_{Y \in \mathcal{V}} Y$ , то найдется такое множество  $Y \in \mathcal{V}$ , что  $x \in Y$ .

Покажем, что  $X = Y$ . Если  $u \in X$ , то  $x R_{\mathcal{U}} u$ , значит, и  $x R_{\mathcal{V}} u$ . Но  $x \in Y$ , поэтому  $u \in Y$ . Значит,  $X \subseteq Y$ .

По той же схеме устанавливается справедливость включения  $Y \subseteq X$ , значит,  $X = Y$  и  $\mathcal{U} \subseteq \mathcal{V}$ .

Так как разбиения  $\mathcal{U}$  и  $\mathcal{V}$  равноправны, то имеет место и включение  $\mathcal{V} \subseteq \mathcal{U}$ , значит,  $\mathcal{U} = \mathcal{V}$ .  $\square$

**Теорема 3.5.** Для каждого отношения эквивалентности  $R$  на множестве  $A$  существует такое разбиение  $\mathcal{U}$  этого множества, что  $R_{\mathcal{U}} = R$ .

*Д о к а з а т е л ь с т в о.* Рассмотрим введенное выше разбиение

$$\mathcal{U} = \{[a] \mid a \in A\}$$

на классы эквивалентности по отношению эквивалентности  $R$ . Покажем, что  $R_{\mathcal{U}} = R$ .

Докажем включение  $R \subseteq R_{\mathcal{U}}$ . Если  $\langle a, b \rangle \in R$ , то  $aRb$ , поэтому  $a, b \in [a]_R$ . Значит,  $aR_{\mathcal{U}}b$ , поэтому  $\langle a, b \rangle \in R_{\mathcal{U}}$ . Следовательно,  $R \subseteq R_{\mathcal{U}}$ .

Пусть  $\langle a, b \rangle \in R_{\mathcal{U}}$ . Тогда найдется такое множество  $Y \in \mathcal{U}$ , что  $a, b \in Y$ . Но по определению разбиения  $\mathcal{U}$  его элементами являются классы эквивалентности, значит, найдется элемент  $c \in A$  такой, что  $Y = [c]_R$ . Поэтому  $a, b \in [c]_R$ . Значит,  $aRb$ , т.е.  $\langle a, b \rangle \in R$ . Тем самым доказано, что  $R_{\mathcal{U}} \subseteq R$ .

Окончательно получаем, что  $R_{\mathcal{U}} = R$ . □

Доказанные теоремы утверждают, что между отношениями эквивалентности на множестве  $A$  и разбиениями этого множества существует естественное взаимно однозначное соответствие.

Отношения эквивалентности встречаются во всех разделах математики. Приведем некоторые примеры.

Обычное отношение равенства на произвольном множестве является отношением эквивалентности.

Отношение подобия фигур — важный пример отношения эквивалентности в геометрии евклидовой плоскости. Отношение параллельности прямых на плоскости — другой важный пример отношения эквивалентности в геометрии при условии, что мы считаем каждую прямую параллельной самой себе.

Обозначим через  $\mathbb{R}$  множество всех действительных чисел, а через  $\mathbb{Q}$  — множество всех рациональных чисел. Определим на множестве  $\mathbb{R}$  действительных чисел следующее важное отношение эквивалентности: пусть  $\alpha, \beta \in \mathbb{R}$ , полагаем

$$\alpha \equiv \beta \pmod{(\mathbb{Q})} \iff \alpha - \beta \in \mathbb{Q}.$$

Читателю в качестве упражнения предоставляется проверка выполнимости условий рефлексивности, симметричности и транзитивности. Построенное отношение эквивалентности используется в математическом анализе при построении примера неизмеримого по А. Лебегу множества.

Пусть  $\mathbb{Z}$  — множество всех целых чисел. Определим на множестве  $\mathbb{R}$  действительных чисел еще одно отношение эквивалентности: пусть  $\alpha, \beta \in \mathbb{R}$ , полагаем

$$\alpha \equiv \beta \pmod{(\mathbb{Z})} \iff \alpha - \beta \in \mathbb{Z}.$$

И вновь читателю в качестве упражнения предлагается проверить, что мы действительно получаем отношение эквивалентности.

Важную роль отношения эквивалентности и фактормножества по ним играют в алгебре — на их использовании основано построение всех “факторобъектов”: факторгрупп, факторколец, фактормодулей и т.д.

Не менее важна роль этих понятий и при построении числовых систем.

Пусть

$$\mathbb{N} = \{1, 2, \dots, n, \dots\} —$$

множество натуральных чисел.



Покажем, как, отправляясь от множества  $\mathbb{N}$  натуральных чисел, можно построить множество  $\mathbb{Z}$  целых чисел.

Для построения множества  $\mathbb{Z}$  целых чисел рассмотрим на множестве  $\mathbb{N} \times \mathbb{N}$  следующее отношение  $\equiv$

$$\langle a, b \rangle \equiv \langle c, d \rangle \iff a + d = c + b.$$

Читателю предоставляется в качестве упражнения проверить, что отношение  $\equiv$  является отношением эквивалентности.

Обозначим через  $\mathbb{Z}$  фактормножество  $\mathbb{N} \times \mathbb{N} / \equiv$ . Определим на множестве  $\mathbb{Z}$  операции сложения  $+$  и умножения  $\cdot$ .

$$\begin{aligned} [\langle a, b \rangle] + [\langle c, d \rangle] &= [\langle a + c, b + d \rangle], \\ [\langle a, b \rangle] \cdot [\langle c, d \rangle] &= [\langle ac + bd, bc + ad \rangle]. \end{aligned}$$

Читателю предоставляется в качестве упражнения проверить, что множество  $\mathbb{Z}$  вместе с так определенными операциями сложения  $+$  и умножения  $\cdot$  является кольцом, причем отображение  $f : a \mapsto [\langle a + 1, 1 \rangle]$  задает изоморфное вложение множества натуральных чисел с операциями сложения и умножения в это кольцо. При этом для любого элемента  $z \in \mathbb{Z}$  найдутся такие натуральные числа  $a$  и  $b$ , что  $z = f(a) - f(b)$ , где  $-$  — операция вычитания в кольце  $\mathbb{Z}$ .

Система  $\langle \mathbb{Z}, +, \cdot \rangle$  называется кольцом целых чисел.

Покажем, как, отправляясь от множества  $\mathbb{Z}$  целых чисел, можно построить множество  $\mathbb{Q}$  рациональных чисел.

Для построения множества  $\mathbb{Q}$  рациональных чисел рассмотрим на множестве  $\mathbb{Z} \times \mathbb{N}$  следующее отношение  $\equiv$

$$\langle a, b \rangle \equiv \langle c, d \rangle \iff ad = cb.$$

Читателю предоставляется в качестве упражнения проверить, что отношение  $\equiv$  является отношением эквивалентности.

Обозначим через  $\mathbb{Q}$  фактормножество  $\mathbb{Z} \times \mathbb{N} / \equiv$ . Определим на множестве  $\mathbb{Q}$  операции сложения  $+$  и умножения  $\cdot$ :

$$\begin{aligned} [\langle a, b \rangle] + [\langle c, d \rangle] &= [\langle ad + cb, bd \rangle], \\ [\langle a, b \rangle] \cdot [\langle c, d \rangle] &= [\langle ac, bd \rangle]. \end{aligned}$$

Читателю предоставляется в качестве упражнения проверить, что множество  $\mathbb{Q}$  вместе с так определенными операциями сложения  $+$  и умножения  $\cdot$  является полем, причем отображение  $f : a \mapsto [\langle a, 1 \rangle]$  задает изоморфное вложение кольца целых чисел в это поле. При этом для любого элемента  $r \in \mathbb{Q}$  найдутся такие целые числа  $a$  и  $b$ , что  $r = f(a)/f(b)$ , где  $/$  — операция деления в поле  $\mathbb{Q}$ .

Система  $\langle \mathbb{Q}, +, \cdot \rangle$  называется полем рациональных чисел.

Построение поля  $\mathbb{R}$  действительных чисел можно провести по следующей схеме. Предварительно напомним два определения из математического анализа — понятия **фундаментальной последовательности** и **последовательности сходящейся к нулю**.

**Определение 3.5.** Последовательность  $(r_n)_{n \in \mathbb{N}}$  рациональных чисел называется **фундаментальной**, если для любого положительного рационального числа  $\varepsilon$  существует такое натуральное число  $n_0$ , что для любых натуральных чисел  $n$  и  $m$  больших, чем  $n_0$ , выполняется неравенство  $|r_n - r_m| < \varepsilon$ .

**Определение 3.6.** Последовательность  $(r_n)_{n \in \mathbb{N}}$  рациональных чисел называется **сходящейся к нулю**, если для любого положительного рационального числа  $\varepsilon$  существует такое натуральное число  $n_0$ , что для любого натурального числа  $n$  большего, чем  $n_0$ , выполняется неравенство  $|r_n| < \varepsilon$ .

Фундаментальные последовательности еще называются последовательностями, сходящимися в себе. Сходящиеся к нулю последовательности иногда называются бесконечно малыми последовательностями.

Обозначим через  $\mathcal{F}(\mathbb{Q})$  множество всех фундаментальных последовательностей рациональных чисел, а через  $\mathcal{O}(\mathbb{Q})$  — множество всех сходящихся к нулю последовательностей рациональных чисел.

Определим на множестве  $\mathcal{F}(\mathbb{Q})$  отношение  $\equiv$

$$(a_n)_{n \in \mathbb{N}} \equiv (b_n)_{n \in \mathbb{N}} \iff (a_n - b_n)_{n \in \mathbb{N}} \in \mathcal{O}(\mathbb{Q}).$$

Читателю предоставляется в качестве упражнения проверить, что отношение  $\equiv$  является отношением эквивалентности.

Обозначим через  $\mathbb{R}$  фактормножество  $\mathcal{F}(\mathbb{Q}) / \equiv$ . Это множество обозначается еще через  $\mathcal{F}(\mathbb{Q}) / \mathcal{O}(\mathbb{Q})$ .

Определим на множестве  $\mathbb{R}$  естественным образом операции сложения  $+$  и умножения  $\cdot$

$$(a_n)_{n \in \mathbb{N}} + (b_n)_{n \in \mathbb{N}} \rightleftharpoons (a_n + b_n)_{n \in \mathbb{N}},$$

$$(a_n)_{n \in \mathbb{N}} \cdot (b_n)_{n \in \mathbb{N}} \rightleftharpoons (a_n b_n)_{n \in \mathbb{N}}.$$

Читателю предоставляется в качестве упражнения проверить, что множество  $\mathbb{R}$  вместе с так определенными операциями сложения  $+$  и умножения  $\cdot$  является полем, причем отображение  $f: r \mapsto (r)_{n \in \mathbb{N}}$  задает изоморфное вложение поля рациональных чисел в это поле, где через  $(r)_{n \in \mathbb{N}}$  обозначена постоянная последовательность, все члены которой равны  $r$ .

При этом любой элемент  $\alpha \in \mathbb{R}$  будет пределом некоторой последовательности вида  $(f(r_n))_{n \in \mathbb{N}}$ .

Система  $\langle \mathbb{R}, +, \cdot \rangle$  называется полем действительных чисел. Кроме того, это поле можно упорядочить таким образом, что оно станет непрерывно архимедовски упорядоченным полем. Детали можно найти в книгах по математическому анализу.

В теории чисел важную роль играют следующие отношения эквивалентности на множестве  $\mathbb{Z}$  целых чисел. Фиксируем целое число  $m$ . Для целых чисел  $a$  и  $b$  полагаем

$$a \equiv b \pmod{m} \iff a - b \text{ делится на } m.$$



Легко проверить, что это отношение является отношением эквивалентности. Оно называется *отношением сравнимости* или *равноостаточности по модулю  $m$* .

Другой важный класс двуместных отношений образуют отношения **частичного порядка**.

**Определение 3.7.** *Отношением частичного порядка или просто частичным порядком на множестве  $A$  называется любое двуместное отношение  $R$  на этом множестве, удовлетворяющее условиям*

- (1) **рефлексивность**: для любого элемента  $a$  из  $A$ :  $aRa$ ,
- (2) **антисимметричность**: для любых элементов  $a$  и  $b$  из  $A$ : если  $aRb$  и  $bRa$ , то  $a = b$ ,
- (3) **транзитивность**: для любых элементов  $a, b, c \in A$ : если  $aRb$  и  $bRc$ , то  $aRc$ .

Обычно отношение частичного порядка обозначается через  $\leq$  и в таком случае вместо  $\langle a, b \rangle \in \leq$  пишут  $a \leq b$ .

Система  $\langle A, \leq \rangle$ , состоящая из непустого множества  $A$  и отношения частичного порядка  $\leq$  на нем, называется **частично упорядоченным множеством** и обычно обозначается тоже через  $A$ .

Примерами отношений частичного порядка являются обычные отношения порядка на множествах натуральных, целых, рациональных и действительных чисел. Важный пример частично упорядоченного множества дает множество  $P(A)$  всех подмножеств произвольного фиксированного множества  $A$  с отношением включения  $\subseteq$  как отношением частичного порядка.

Если  $\langle A, \leq \rangle$  — частично упорядоченное множество, то на множестве  $A^n$  тоже можно ввести отношение частичного порядка, которое мы будем обозначать тем же символом  $\leq$ . Полагаем

$$\langle a_1, \dots, a_n \rangle \leq \langle b_1, \dots, b_n \rangle \iff a_1 \leq b_1 \& \dots \& a_n \leq b_n.$$

Нетрудно проверить, что так определенное отношение является отношением частичного порядка.

Если  $a$  и  $b$  — элементы частично упорядоченного множества  $\langle A, \leq \rangle$  и либо  $a \leq b$ , либо  $b \leq a$ , то элементы  $a$  и  $b$  называются **сравнимыми**.

Рассмотренное выше отношение частичного порядка  $\leq$  еще называют отношением *нестрогого частичного порядка*, так как оно обладает свойством рефлексивности. Полагая

$$a < b \iff a \leq b \& a \neq b,$$

мы получим отношение  **$<$  строгого частичного порядка**. Заметим, всегда  $a \not\leq a$ , это свойство можно назвать антирефлексивностью. Кроме того, если

$a < b$ , то  $b \not\leq a$ . Для отношения строгого частичного порядка выполняется свойство транзитивности.

Можно начинать рассмотрение с отношения строгого частичного порядка  $<$ , как произвольного двуместного отношения, обладающего свойством транзитивности и антирефлексивности, и получить отношение  $\leq$  нестрогого частичного порядка путем определения

$$a \leq b \iff a < b \vee a = b.$$

Важным примером отношения строгого частичного порядка является отношение **лексикографического** порядка на множестве  $\bigcup_{n=1}^{\infty} A^n$  всех конечных последовательностей, составленных из элементов упорядоченного множества  $A$ . Оно вводится следующим определением

$$\begin{aligned} \langle a_1, \dots, a_n \rangle < \langle b_1, \dots, b_m \rangle &\iff n < m \vee \\ &\vee (n = m \ \& \ \text{найдется такое число } k, \text{ что } 0 \leq k < n \text{ и} \\ &\quad a_1 = b_1 \ \& \dots \& \ a_k = b_k \ \& \ a_{k+1} < b_{k+1}). \end{aligned}$$

**Определение 3.8.** Элемент  $a$  частично упорядоченного множества  $\langle A, \leq \rangle$  называется **максимальным** (**минимальным**), если для любого элемента  $b$  множества  $A$  из неравенства  $b \geq a$  (соответственно из неравенства  $b \leq a$ ) следует равенство  $a = b$ .

Частично упорядоченное множество может вообще не иметь максимальных (минимальных) элементов, а может иметь и несколько максимальных (минимальных) элементов. Построение соответствующих примеров предоставляется читателю в качестве упражнения.

**Определение 3.9.** Элемент  $a$  частично упорядоченного множества  $\langle A, \leq \rangle$  называется **наибольшим** (**наименьшим**), если для любого элемента  $b$  этого множества выполняется неравенство  $b \leq a$  (соответственно неравенство  $a \leq b$ ).

Ясно, что если в частично упорядоченном множестве есть наибольший (наименьший) элемент, то он будет единственным максимальным (минимальным) элементом этого множества.

**Определение 3.10.** Элемент  $a$  частично упорядоченного множества  $\langle A, \leq \rangle$  называется **верхней** (**нижней**) **гранью** подмножества  $B$  множества  $A$ , если для любого элемента  $b$  из  $B$  выполняется неравенство  $b \leq a$  (соответственно  $a \leq b$ ).

**Определение 3.11.** Точной верхней (нижней) гранью подмножества  $B$  частично упорядоченного множества  $A$  называется наименьшая верхняя (наибольшая нижняя) грань для этого подмножества  $B$ .

Точная верхняя грань подмножества  $B$ , если она существует, определена однозначно и обозначается через  $\sup B$ .

Аналогично точная нижняя грань подмножества  $B$ , если она существует, определена однозначно и обозначается через  $\inf B$ .

**Определение 3.12.** Частично упорядоченное множество  $\langle A, \leq \rangle$  называется **решеткой** или **структурой**, если для любых ее двух элементов  $a$  и  $b$  множество  $B = \{a, b\}$  имеет точную верхнюю и точную нижнюю грани.

Традиционно  $\sup\{a, b\}$  обозначается через  $a \cup b$ , а  $\inf\{a, b\}$  — через  $a \cap b$ .

Важный пример решетки дает множество  $P(A)$  всех подмножеств произвольного множества  $A$ , частично упорядоченное отношением  $\subseteq$  включения.

Понятие частично упорядоченного множества является слишком общим, чтобы можно было надеяться доказать какие-либо глубокие теоремы относительно класса всех частично упорядоченных множеств. Любое множество  $A$  можно частично упорядочить, положив для произвольных ее элементов  $a$  и  $b$

$$a \leq b \iff a = b.$$

И все же есть одно очень важное утверждение, справедливое для произвольного частично упорядоченного множества, оно носит название **Лемма Цорна**.

Для его формулировки нам понадобится понятие **цепи**.

**Определение 3.13.** Подмножество  $B$  частично упорядоченного множества  $\langle A, \leq \rangle$  называется **цепью**, если для любых двух элементов  $a$  и  $b$  из  $B$  либо  $a \leq b$ , либо  $b \leq a$ .

**Лемма Цорна.** Частично упорядоченное множество  $\langle A, \leq \rangle$ , каждая цепь которого имеет верхнюю грань, содержит максимальный элемент.

Доказательство Леммы Цорна по ряду причин будет дано несколько позже. Заметим, что в этом доказательстве будет использован пока еще не введенный нами принцип теории множеств — **Аксиома выбора**. Более того, будет доказано, что Лемма Цорна эквивалентна Аксиоме выбора, поэтому ее можно было бы принять в качестве одного из принципов теории множеств. Однако по ряду причин часто предпочитают брать в качестве одного из принципов теории множеств Аксиому выбора, а Лемму Цорна и ряд других ей эквивалентных утверждений выводить из нее.

**Определение 3.14.** Отношение  $\leq$  частичного порядка на множестве  $A$  называется **линейным порядком** или просто **порядком**, если любые два элемента  $a$  и  $b$  этого множества сравнимы, т.е. либо  $a \leq b$ , либо  $b \leq a$ .

Система  $\langle A, \leq \rangle$ , состоящая из множества  $A$  и линейного порядка  $\leq$  на нем, называется **линейно упорядоченным множеством** или просто **упорядоченным множеством**.

В качестве примеров линейно упорядоченных множеств можно привести множества натуральных, целых, рациональных и действительных чисел с обычными отношениями порядка на них. Другую серию примеров дают множества конечных последовательностей, составленных из элементов линейно упорядоченного множества, с отношением лексикографического порядка.

## 4. Равномощность множеств

Понятие *равномощности множеств* является одним из важнейших понятий теории множеств.

Для того, чтобы ответить на вопрос, содержат ли два конечных множества одинаковое число элементов, достаточно пересчитать элементы этих множеств и сравнить полученные числа. Ясно, что для бесконечных множеств такой метод принципиально не годится. Г. Кантором был предложен следующий метод “сравнения по величине” произвольных множеств, в том числе и бесконечных.

**Определение 4.1.** *Множества  $A$  и  $B$  называются равномощными, если существует биективное отображение множества  $A$  на множество  $B$ .*

Запись  $\overline{A} = \overline{B}$  будет служить обозначением утверждения “множества  $A$  и  $B$  равномощными”. При этом, если  $f$  — биекция множества  $A$  на множество  $B$ , то будем говорить, что  $f$  устанавливает равномощность множеств  $A$  и  $B$ .

Если  $A$  и  $B$  — конечные множества, то они равномощны тогда и только тогда, когда состоят из одного и того же числа элементов. Таким образом, понятие равномощности можно рассматривать как естественное обобщение на произвольные множества понятия равночисленности конечных множеств.

**Пример.** Пусть  $\mathbb{N}$  — множество всех натуральных чисел, а  $B$  — множество всех четных натуральных чисел. Тогда функция  $f(x) = 2x$  устанавливает равномощность множеств  $\mathbb{N}$  и  $B$ . Из этого примера видно, что бесконечное множество может быть равномощно своему собственному подмножеству. Что невозможно для конечных множеств.

**Теорема 4.1.** *Для любых множеств  $A$  и  $B$  выполняются следующие утверждения:*

- (1)  $\overline{A} = \overline{A}$  (рефлексивность отношения равномощности);
- (2) Если  $\overline{A} = \overline{B}$ , то  $\overline{B} = \overline{A}$  (симметричность отношения равномощности);
- (3) Если  $\overline{A} = \overline{B}$  и  $\overline{B} = \overline{C}$ , то  $\overline{A} = \overline{C}$  (транзитивность отношения равномощности).

*До к а з а т е л ь с т в о.* (1) Равномощность множества  $A$  самому себе устанавливает функция  $i_A$ .

(2) Если равномощность множеств  $A$  и  $B$  устанавливает функция  $f$ , то равномощность множеств  $B$  и  $A$  устанавливает функция  $f^{-1}$ .

(3) Если равномощность множеств  $A$  и  $B$  устанавливает функция  $f$ , а равномощность множеств  $B$  и  $C$  — функция  $g$ , то равномощность множеств  $A$  и  $C$  устанавливает функция  $g \circ f$ .  $\square$

Если множества  $A$  и  $B$  равномощны, то будем говорить, что  $A$  и  $B$  имеют *одинаковую мощность* или одно и то же *кардинальное число*. Заметим, что мы не определяем ни понятие *мощности* множества, ни понятие его *кардинального числа*, а только лишь вводим новый термин для понятия равномощности. Сам Г. Кантор определял *мощность* или *кардинальное число* множества  $A$  как такое его свойство, которое остается после абстрагирования от качества элементов множества и от их порядка. Чтобы подчеркнуть этот двойной акт абстрагирования, Г. Кантор ввел символ  $\overline{A}$  для обозначения мощности множества. Конечно, приведенное только что определение понятия *мощности* множества не может рассматриваться в качестве математического определения. Можно попытаться дать и более точное определение понятия *мощности* множества. Например, под мощностью множества  $A$  можно понимать *класс* всех множеств, равномощных множеству  $A$ . Однако такой подход к понятию мощности наталкивается на ряд трудностей, например, как доказать, что любое множество имеет мощность, т.е. что для любого множества  $A$  существует класс множеств, ему равномощных. Кроме того, рассмотрение “слишком больших” множеств может привести к противоречиям.

С другой стороны, термин *мощность* не обязательно использовать, так как теоремы теории множеств можно формулировать так, чтобы в них речь шла не о свойствах мощностей или кардинальных чисел, а об отношениях между ними, справедливость же этих отношений можно доказать при помощи понятия равномощности. Однако многие теоремы теории множеств становятся более лаконичными, если их формулировать как теоремы о мощностях или о кардинальных числах. Это служит оправданием введения в теорию множеств кардинальных чисел. Будем считать, что с каждым множеством  $A$  связан некоторый объект  $\overline{A}$ , называемый *кардинальным числом* или *мощностью* множества  $A$ , причем множества  $A$  и  $B$  равномощны тогда и только тогда, когда  $\overline{A} = \overline{B}$ .

Если  $A$  — бесконечное множество, то  $\overline{A}$  называется *бесконечным кардинальным числом*, а если  $A$  — конечное множество, то  $\overline{A}$  называется *конечным кардинальным числом*.

**Определение 4.2.** *Мощность множества  $A$  не больше мощности множества  $B$ , если существует инъективное отображение множества  $A$  во множество  $B$ .*

Запись  $\overline{A} \leq \overline{B}$  будет служить сокращением для утверждения “*мощность множества  $A$  не больше мощности множества  $B$* ”.



**Теорема Кантора – Шредера – Бернштейна.** Если  $\overline{\overline{A}} \leq \overline{\overline{B}}$  и  $\overline{\overline{B}} \leq \overline{\overline{A}}$ , то  $\overline{\overline{A}} = \overline{\overline{B}}$ .

*Доказательство.* Пусть  $f$  — инъективное отображение множества  $A$  во множество  $B$ , а  $g$  — инъективное отображение множества  $B$  во множество  $A$ . Докажем, что существует некоторое биективное отображение  $h$  множества  $A$  на множество  $B$ .

Полагаем

$$A_0 \Leftarrow A \setminus g(B), \quad B_0 \Leftarrow f(A_0), \\ A_{n+1} \Leftarrow g(B_n), \quad B_{n+1} \Leftarrow f(A_{n+1}).$$

Докажем, что при  $i \neq j$   $A_i \cap A_j = \emptyset$  и  $B_i \cap B_j = \emptyset$ . Доказательство проведем индукцией по  $i + j$ . Ясно, что  $i + j \geq 1$ . Можно считать, что  $i < j$ .

(1) Пусть  $i + j = 1$ . Тогда  $i = 0$ ,  $j = 1$  и надо доказать, что

$$A_0 \cap A_1 = \emptyset, \quad B_0 \cap B_1 = \emptyset.$$

Докажем, что при  $j \geq 1$

$$A_0 \cap A_j = \emptyset, \quad B_0 \cap B_j = \emptyset.$$

Но при  $j \geq 1$   $A_j = g(B_{j-1}) \subseteq g(B)$ , а  $A_0 = A \setminus g(B)$ , поэтому  $A_0 \cap A_j = \emptyset$ .

Докажем, что  $B_0 \cap B_j = \emptyset$ . Предположим противное и пусть  $b \in B_0 \cap B_j = f(A_0) \cap f(A_j)$ . Тогда найдутся такие элементы  $a_0 \in A_0$ ,  $a_j \in A_j$ , что  $b = f(a_0) = f(a_j)$ . Так как  $f$  — инъективное отображение, то  $a_0 = a_j$ , значит,  $a_0 \in A_0 \cap A_j = \emptyset$ . Полученное противоречие показывает, что  $B_0 \cap B_j = \emptyset$ .

(2) Сделаем индуктивное предположение:

при любых  $i \neq j$   $i + j < k$

$$A_i \cap A_j = \emptyset, \quad B_i \cap B_j = \emptyset.$$

(3) Пусть  $i + j = k \geq 2$  и  $i < j$ . Случай  $i = 0$  уже рассмотрен выше, поэтому можно считать, что  $1 \leq i < j < k$ . Допустим, что  $A_i \cap A_j \neq \emptyset$ . Пусть  $a \in A_i \cap A_j$ . Так как  $A_i = g(B_{i-1})$ ,  $A_j = g(B_{j-1})$ , то найдутся такие элементы  $b_{i-1} \in B_{i-1}$ ,  $b_{j-1} \in B_{j-1}$ , что  $a = g(b_{i-1}) = g(b_{j-1})$ . Так как  $g$  — инъективное отображение, то  $b_{i-1} = b_{j-1}$ , поэтому  $b_{i-1} = b_{j-1} \in B_{i-1} \cap B_{j-1}$ . Но  $(i-1) + (j-1) < i + j = k$ , поэтому по индуктивному предположению  $B_{i-1} \cap B_{j-1} = \emptyset$ . Полученное противоречие показывает, что  $A_i \cap A_j = \emptyset$ .

Допустим, что  $B_i \cap B_j \neq \emptyset$ . Пусть  $b \in B_i \cap B_j$ . Так как  $B_i = f(A_i)$ ,  $B_j = f(A_j)$ , то найдутся элементы  $a_i \in A_i$ ,  $a_j \in A_j$  такие, что  $b = f(a_i) = f(a_j)$ . В силу инъективности  $f$   $a_i = a_j$ , значит,  $a_i \in A_i \cap A_j = \emptyset$ . Полученное противоречие показывает, что  $B_i \cap B_j = \emptyset$ .

Полагаем

$$C \Leftarrow \bigcup_{n=0}^{\infty} A_n, \quad D \Leftarrow \bigcup_{n=0}^{\infty} B_n.$$



Определим отображение  $h$  из  $A$  в  $B$ :  $h(x) = f(x)$ , если  $x \in C$  и  $h(x) = g^{-1}(x)$ , если  $x \in A \setminus C$ .

Так как  $A \setminus g(B) = A_0 \subseteq C$ , то  $A \setminus C \subseteq g(B)$ , значит, определение отображения  $h$  корректно.

Покажем, что  $h$  — сюръективное отображение. Пусть  $b \in B$ .

Если  $b \in D$ , то найдется такое  $n$ , что  $b \in B_n$ . Но  $B_n = f(A_n)$ . Значит, найдется элемент  $a \in A_n$  такой, что  $b = f(a_n)$ . Так как  $a \in A_n \subseteq C$ , то  $h(a_n) = f(a_n) = b$ .

Если  $b \notin D$ , то  $g(b) \notin C$ , так как в противном случае при некотором  $n \geq 1$   $g(b) \in A_n$  и тогда  $b \in g^{-1}(A_n) = B_{n-1} \subseteq D$ . Значит,  $h(g(b)) = g^{-1}(g(b)) = b$ .

Покажем, что  $h$  — инъективное отображение. Пусть  $x_1, x_2 \in A$  и  $h(x_1) = h(x_2)$ . Если  $x_1, x_2 \in C$  или  $x_1, x_2 \in A \setminus C$ , то из инъективности  $f$  и  $g^{-1}$  сразу следует, что  $x_1 = x_2$ .

Остается показать, что случай  $h(x_1) = h(x_2)$ ,  $x_1 \in C$  и  $x_2 \in A \setminus C$  невозможен.

Предположим противное, пусть  $h(x_1) = h(x_2)$ ,  $x_1 \in C$  и  $x_2 \in A \setminus C$ . Тогда  $f(x_1) = g^{-1}(x_2)$ , значит,  $g(f(x_1)) = x_2$ . Пусть  $x_1 \in A_n$ , тогда  $f(x_1) \in f(A_n) = B_n$ ,  $g(f(x_1)) \in g(B_n) = A_{n+1}$ . Значит,  $x_2 \in A_{n+1} \subseteq C$ , что противоречит предположению  $x_2 \in A \setminus C$ .

Тем самым доказано, что  $h$  — биективное отображение множества  $A$  на множество  $B$ , поэтому  $\overline{A} = \overline{B}$ . □

Дадим еще одно доказательство этой важной теоремы, следуя пособию Е.И. Гордона и Г.М. Полотовского [8]. Предварительно докажем интересное и важное утверждение, носящее название **Лемма А. Тарского**.

**Определение 4.3.** Отображение  $\varphi$  в себя множества  $P(X)$  всех подмножеств произвольного множества  $X$  называется **монотонным**, если для любых двух подмножеств  $A$  и  $B$  множества  $X$  включение  $A \subseteq B$  влечет включение  $\varphi(A) \subseteq \varphi(B)$ .

**Определение 4.4.** Если  $\varphi$  — отображение в себя произвольного множества  $W$ , а  $A^*$  — такой элемент этого множества, что  $\varphi(A^*) = A^*$ , то  $A^*$  называется **неподвижной точкой** отображения  $\varphi$ .

**Лемма А. Тарского о неподвижной точке.** Любое монотонное отображение  $\varphi$  в себя множества  $P(X)$  всех подмножеств произвольного множества  $X$  имеет неподвижную точку.

*До к а з а т е л ь с т в о.* Обозначим через  $M$  следующее семейство подмножеств множества  $X$ :

$$\{U \mid U \subseteq X \wedge \varphi(U) \subseteq U\}.$$

Ясно, что само множество  $X$  входит в  $M$ . Если  $B \in M$ , то по определению  $\varphi(B) \subseteq B$ , что в силу монотонности отображения  $\varphi$  дает включение  $\varphi(\varphi(B)) \subseteq \varphi(B)$ . Значит,  $\varphi(B) \in M$ .

Полагаем

$$A^* = \bigcap_{B \in M} B.$$

Покажем, что  $A^*$  — неподвижная точка отображения  $\varphi$ . Если  $B$  — произвольное множество из  $M$ , то  $A^* \subseteq B$ , откуда в силу монотонности отображения  $\varphi$  получаем  $\varphi(A^*) \subseteq \varphi(B)$ . Из определения семейства  $M$  имеем включение  $\varphi(B) \subseteq B$ , что вместе с предыдущим включением дает  $\varphi(A^*) \subseteq B$ . Но тогда

$$\varphi(A^*) \subseteq \bigcap_{B \in M} B = A^*,$$

т.е.  $A^* \in M$ . Но тогда и  $\varphi(A^*) \in M$ . Последнее в силу определения множества  $A^*$  влечет включение  $A^* \subseteq \varphi(A^*)$ . Последнее вместе с ранее установленным включением дает нужное равенство  $\varphi(A^*) = A^*$ . Лемма доказана.  $\square$

*Доказательство теоремы Кантора – Шредера – Бернштейна.* Пусть  $f: A \rightarrow B$  и  $g: B \rightarrow A$  — инъективные отображения. Нам необходимо построить биективное отображение  $h: A \rightarrow B$ . Докажем, что существует такое подмножество  $A^*$  множества  $X$ , что  $A^* = A \setminus g(B \setminus f(A^*))$ .

Рассмотрим отображение  $\varphi$  в себя множества  $P(X)$  всех подмножеств множества  $X$ , заданное равенством

$$\varphi(U) = A \setminus g(B \setminus f(U)).$$

Нетрудно проверить, что  $\varphi$  — монотонное отображение. По лемме А. Тарского о неподвижной точке существует подмножество  $A^*$  множества  $A$ , удовлетворяющее равенству  $A^* = \varphi(A^*) = A \setminus g(B \setminus f(A^*))$ . Ясно, что  $f$  биективно отображает множество  $A^*$  на  $f(A^*)$ . Кроме того, так как  $A \setminus A^* = g(B \setminus f(A^*))$ , то  $g$  биективно отображает множество  $B \setminus f(A^*)$  на  $A \setminus A^*$ , поэтому  $g^{-1}$  биективно отображает множество  $A \setminus A^*$  на  $B \setminus f(A^*)$ . Значит,  $f \cup g^{-1}$  биективно отображает множество  $A$  на  $B$ .  $\square$

**Определение 4.5.** *Мощность  $\overline{\overline{A}}$  множества  $A$  меньше мощности  $\overline{\overline{B}}$  множества  $B$ , если  $\overline{\overline{A}} \leq \overline{\overline{B}}$ , но  $\overline{\overline{A}} \neq \overline{\overline{B}}$ .*

Запись  $\overline{\overline{A}} < \overline{\overline{B}}$  будет служить сокращением для утверждения “мощность  $\overline{\overline{A}}$  множества  $A$  меньше мощности  $\overline{\overline{B}}$  множества  $B$ ”.

Заметим, что в соответствии с определением мощность  $\overline{\overline{A}}$  множества  $A$  меньше мощности  $\overline{\overline{B}}$  множества  $B$ , если существует инъективное отображение множества  $A$  во множество  $B$ , но не существует биективного отображения множества  $A$  на множество  $B$ , т.е. множество  $A$  равномощно некоторому подмножеству множества  $B$ , но неравномощно всему множеству  $B$ .

В качестве упражнения читателю предлагается проверить, что справедливы следующие утверждения:

- (1) для любого множества  $A$   $\overline{\overline{A}} \not\prec \overline{\overline{A}}$  (антирефлексивность отношения  $<$ );
- (2) для любых множеств  $A, B$  и  $C$ : если  $\overline{\overline{A}} < \overline{\overline{B}}$  и  $\overline{\overline{B}} < \overline{\overline{C}}$ , то  $\overline{\overline{A}} < \overline{\overline{C}}$  (транзитивность отношения  $<$ ).

Г. Кантору принадлежит заслуга открытия существования бесконечных множеств, имеющих различную мощность.

**Теорема Кантора.** Если  $A$  — произвольное множество, а  $P(A)$  — множество всех его подмножеств, то  $\overline{\overline{A}} < \overline{\overline{P(A)}}$ .

*Доказательство.* Отображение

$$f : a \mapsto \{a\}$$

является инъективным вложением множества  $A$  во множество  $P(A)$ , поэтому  $\overline{\overline{A}} \leq \overline{\overline{P(A)}}$ .

Остается показать, что  $\overline{\overline{A}} \neq \overline{\overline{P(A)}}$ , т.е. что не существует биективного отображения множества  $A$  на множество  $P(A)$ . Мы докажем, что даже не существует сюръективного отображения множества  $A$  на множество  $P(A)$ . Пусть  $\varphi$  — произвольное отображение множества  $A$  во множество  $P(A)$ . Рассмотрим следующее подмножество  $D_\varphi$  множества  $A$ :

$$D_\varphi = \{x \mid x \in A \text{ \& } x \notin \varphi(x)\}.$$

Покажем, что не существует такого элемента  $a \in A$ , что  $D_\varphi = \varphi(a)$ . Предположим противное, пусть найдется такой элемент  $a \in A$ , что  $D_\varphi = \varphi(a)$ .

Допустим, что  $a \in \varphi(a)$ , тогда  $a \in D_\varphi$ , откуда по определению множества  $D_\varphi$  получаем  $a \notin \varphi(a)$ . А так как по предположению  $a \in \varphi(a)$ , то полученное противоречие показывает, что  $a \notin \varphi(a)$ .

Из последнего по определению множества  $D_\varphi$  получаем, что  $a \in D_\varphi$ , но тогда  $a \in \varphi(a)$ .

Итак, мы доказали, что  $a \notin \varphi(a)$  и  $a \in \varphi(a)$ . Полученное противоречие показывает, что не существует такого элемента  $a \in A$ , что  $D_\varphi = \varphi(a)$ . Значит, отображение  $\varphi$  не является сюръективным.

Это завершает доказательство теоремы Г. Кантора. □

**Замечание.** Если  $A$  — конечное множество, состоящее из  $n$  элементов, то  $P(A)$  — конечное множество, состоящее из  $2^n$  элементов. Это делает оправданным введение следующего обозначения: полагаем

$$2^{\overline{\overline{A}}} = \overline{\overline{P(A)}}.$$

Тогда по теореме Г. Кантора  $\overline{\overline{A}} < 2^{\overline{\overline{A}}}$ .

Для произвольного множества  $A$  определим бесконечную возрастающую последовательность кардинальных чисел, полагая

$$\alpha_0 \equiv \overline{A}, \quad \alpha_{n+1} \equiv 2^{\alpha_n}.$$

По теореме Г. Кантора

$$\alpha_0 < \alpha_1 < \dots < \alpha_n < \alpha_{n+1} < \dots$$

Взяв в качестве исходного множества  $A$  множество натуральных чисел или любое другое бесконечное множество, получим бесконечную возрастающую последовательность бесконечных кардинальных чисел. Уже это свидетельствует о плодотворности предложенного Г. Кантором способа сравнения бесконечных множеств по мощности. Дальнейшее изучение мира кардинальных чисел не входит в наши планы. Заметим лишь, что этот мир чрезвычайно богат, и далеко не на все связанные с ним вопросы получены окончательные ответы.

В дальнейшем будет полезна следующая, интуитивно очевидная, теорема

**Теорема 4.2.** *Если существует сюръективное отображение множества  $A$  на множество  $B$ , то мощность  $B$  не превосходит мощности  $A$ .*

*Доказательство.* Пусть  $f : A \rightarrow B$  — сюръективное отображение множества  $A$  на множество  $B$ . Для произвольного элемента  $b \in B$  полагаем

$$A_b \equiv \{a | f(a) = b\}.$$

При  $b \neq c$  множества  $A_b$  и  $A_c$  не пересекаются и все они непусты. Для каждого  $b \in B$  выберем во множестве  $A_b$  некоторый элемент  $a_b$  и зафиксируем этот выбор (возможность такого выбора нам гарантирует аксиома выбора). Тогда легко понять, что отображение  $\varphi$ , заданное равенством  $\varphi(b) \equiv a_b$ , является вложением множества  $B$  во множество  $A$ . Это завершает доказательство теоремы.  $\square$

## 5. Конечные и счетные множества

Для произвольного натурального числа  $m$  обозначим через  $\mathbb{N}_m$  следующее множество натуральных чисел  $\{1, 2, \dots, m\}$ . Нетрудно доказать, что при  $m \neq n$  множества  $\mathbb{N}_m$  и  $\mathbb{N}_n$  неравномощны.

**Определение 5.1.** *Множество  $A$  называется конечным, если найдется такое натуральное число  $n$ , что  $A$  равномощно множеству  $\mathbb{N}_n$ . При этом  $n$  называется числом элементов множества  $A$ .*

Следующие утверждения легко следуют из определения конечного множества.

**Теорема 5.1.** Подмножество конечного множества само является конечным множеством.

**Теорема 5.2.** Объединение конечного числа конечных множеств само является конечным множеством.

**Теорема 5.3.** Если  $A$  — конечное множество из  $n$  элементов, а  $B$  — конечное множество из  $m$  элементов, то  $A \times B$  — конечное множество из  $nm$  элементов.

**Теорема 5.4.** Если  $A$  — конечное множество из  $n$  элементов и существует сюръективное отображение этого множества на множество  $B$ , то  $B$  — конечное множество из  $m$  элементов и  $m \leq n$ .

**Определение 5.2.** Множество  $A$ , не являющееся конечным, называется бесконечным.

Простейшим примером бесконечного множества является множество  $\mathbb{N}$  натуральных чисел. Его мощность обозначается через  $\aleph_0$ .

**Определение 5.3.** Множество  $A$ , равномощное множеству  $\mathbb{N}$  натуральных чисел, называется **счетным**. Его мощность обозначается через  $\aleph_0$ .

**Теорема 5.5.** Множество  $\mathbb{N} \times \mathbb{N}$  пар натуральных чисел — счетное множество. При любом натуральном  $n$  множество  $\mathbb{N}^n$   $n$ -ок натуральных чисел — счетное множество.

**Д о к а з а т е л ь с т в о.** Рассмотрим отображение  $c_2(n, m) \Rightarrow 2^{n-1}(2m - 1)$ . Ясно, что  $c_2$  — биекция множества  $\mathbb{N} \times \mathbb{N}$  на  $\mathbb{N}$ .

Индукцией по  $n$  строим биективное отображение  $c_n$  множества  $\mathbb{N}^n$   $n$ -ок натуральных чисел на множество  $\mathbb{N}$  натуральных чисел. Полагаем

$$c_1(n) \Rightarrow n, \quad c_{n+1}(a_1, \dots, a_n, a_{n+1}) \Rightarrow c_2(c_n(a_1, \dots, a_n), a_{n+1}).$$

□

**Следствие.** Прямое произведение конечного числа счетных множеств само является счетным множеством.

**Теорема 5.6.** Любое бесконечное множество содержит счетное подмножество.

**Д о к а з а т е л ь с т в о.** Заметим, во-первых, что бесконечное множество непусто, а во-вторых, что при удалении из бесконечного множества конечного подмножества мы получаем бесконечное множество. Это позволяет нам по индукции определить счетную последовательность  $a_1, a_2, \dots$ , состоящую из попарно различных элементов бесконечного множества  $A$ :

$$a_1 \in A, \quad a_{n+1} \in A \setminus \{a_1, \dots, a_n\}.$$

Ясно, что  $\{a_1, \dots, a_n, \dots\}$  — счетное подмножество бесконечного множества  $A$ .

□



**Теорема 5.7.** *Бесконечное подмножество счетного множества само является счетным множеством.*

*Д о к а з а т е л ь с т в о.* Пусть  $B$  — бесконечное подмножество счетного множества  $A$ . В силу предыдущей теоремы  $B$  имеет некоторое счетное подмножество  $C$ . Тогда

$$\overline{\overline{B}} = \overline{\overline{C}} \leq \overline{\overline{B}} \leq \overline{\overline{A}} = \overline{\overline{N}}.$$

В силу теоремы Кантора – Шредера – Бернштейна из этих неравенств следует равенство  $\overline{\overline{A}} = \overline{\overline{N}}$ .  $\square$

**Следствие.** *Подмножество счетного множества является конечным или счетным множеством.*

**Теорема 5.8.** *Если  $A$  — бесконечное множество, а  $B$  — конечное или счетное множество, то  $\overline{\overline{A \cup B}} = \overline{\overline{A}}$ .*

*Д о к а з а т е л ь с т в о.* Достаточно доказать теорему для случая, когда  $A \cap B = \emptyset$ . Пусть  $C$  — счетное подмножество бесконечного множества  $A$ . Покажем, что  $\overline{\overline{C \cup B}} = \overline{\overline{C}}$ . Пусть  $f$  — биекция  $\mathbb{N}$  на  $C$ . Если  $B$  — счетное множество, а  $g$  — биекция  $\mathbb{N}$  на  $B$ , то функция  $h$ , определенная равенствами  $h(2n-1) = f(n)$ ,  $h(2n) = g(n)$ , задает биекцию  $\mathbb{N}$  на  $C \cup B$ , значит,  $\overline{\overline{C \cup B}} = \overline{\overline{N}} = \overline{\overline{C}}$ . Поэтому для завершения доказательства достаточно воспользоваться равенствами

$$A = (A \setminus C) \cup C, \quad A \cup B = (A \setminus C) \cup (C \cup B).$$

$\square$

**Следствие.** *Объединение конечного числа счетных множеств само является счетным множеством.*

**Теорема 5.9.** *Любое бесконечное множество содержит собственное подмножество, ему равномощное.*

*Д о к а з а т е л ь с т в о.* Пусть  $A$  — бесконечное множество и  $a \in A$ . Тогда множество  $A$  равномощно, например, своему собственному подмножеству  $A \setminus \{a\}$ .  $\square$

**Замечание.** Так как никакое конечное множество не может быть равномощно никакому своему собственному подмножеству, то установленное в теореме свойство бесконечных множеств могло быть положено в основу определения бесконечных множеств, а именно, бесконечным можно было бы назвать множество, содержащее собственное подмножество, равномощное всему множеству.

**Теорема 5.10.** *Если существует сюръективное отображение множества натуральных чисел на множество  $A$ , то  $A$  — конечное или счетное множество.*



*Доказательство.* Пусть  $f: \mathbb{N} \rightarrow A$  — сюръективное отображение множества  $\mathbb{N}$  натуральных чисел на множество  $A$ . Если  $A$  — конечное множество, то утверждение теоремы доказано. Пусть  $A$  — бесконечное множество. Для произвольного элемента  $a$  множества  $A$  полагаем

$$\mathbb{N}_a = \{n \mid f(n) = a\}.$$

Ясно, что  $\mathbb{N}_a$  — непустые, попарно непересекающиеся подмножества множества  $\mathbb{N}$ , объединение которых совпадает со всем  $\mathbb{N}$ . Пусть при любом  $a$   $n_a$  — наименьший элемент множества  $\mathbb{N}_a$ . Полагаем  $\varphi(a) = n_a$ . Нетрудно проверить, что  $\varphi$  — инъективное отображение множества  $A$  во множество  $\mathbb{N}$ . И остается воспользоваться одной из предыдущих теорем.  $\square$

**Теорема 5.11.** *Объединение счетного множества счетных множеств само является счетным множеством.*

*Доказательство.* Пусть при любом  $n \in \mathbb{N}$   $A_n$  — счетное множество и

$$A = \bigcup_{n \in \mathbb{N}} A_n.$$

При любом  $n \in \mathbb{N}$  существует сюръективное отображение  $f_n$  множества  $\mathbb{N}$  на  $A_n$ . Построим сюръективное отображение множества  $\mathbb{N}$  на  $A$ .

Полагаем  $f(n, k) = f_n(k)$ . Ясно, что  $f$  — сюръективное отображение множества  $\mathbb{N} \times \mathbb{N}$  на  $A$ . Если  $c_2^{-1}$  — сюръективное отображение множества  $\mathbb{N}$  на  $\mathbb{N} \times \mathbb{N}$ , то  $f \circ c_2^{-1}$  — сюръективное отображение множества  $\mathbb{N}$  на  $A$ . Значит,  $\overline{A} \leq \overline{\mathbb{N}}$ . Для завершения доказательства остается заметить, что  $\overline{\mathbb{N}} = \overline{A_1} \leq \overline{A}$  и воспользоваться теоремой Кантора — Шредера — Бернштейна.  $\square$

**Теорема 5.12.** *Множество всех конечных последовательностей, составленных из элементов счетного множества, само является счетным множеством.*

*Доказательство.* Достаточно доказать счетность множества

$$\mathbb{N}^* = \bigcup_{n \in \mathbb{N}} \mathbb{N}^n.$$

А это сразу следует из теорем 5.10 и 5.11.  $\square$

**Следствие.** *Множество всех конечных подмножеств счетного множества само является счетным множеством.*

Закончим параграф доказательством одной интересной теоремы из теории чисел.

**Определение 5.4.** *Комплексное число называется алгебраическим, если оно является корнем некоторого ненулевого многочлена с целыми коэффициентами. В противном случае оно называется трансцендентным.*

Каждое рациональное число  $m/n$  является алгебраическим, так как оно — корень многочлена  $nx - m$ . Множество  $A$  алгебраических чисел по своим алгебраическим свойствам не отличается от множества  $C$  комплексных чисел:  $A$  — алгебраически замкнутое поле.

Еще в XVIII веке Л. Эйлер высказал предположение о существовании трансцендентных чисел. Но только в 1844 г. Ж. Лиувиллю удалось это предположение доказать. Большим математическим достижением было доказательство Ш. Эрмитом в 1873 г. трансцендентности числа  $e$ . Выдающимся математическим результатом стало доказательство Ф. Линдеманном в 1882 г. трансцендентности числа  $\pi$ , откуда следовала невозможность построения с помощью циркуля и линейки квадрата, равного по площади данному кругу (задача о квадратуре круга). В конце XIX века Г. Кантору удалось, используя методы созданной им теории множеств, доказать, что в некотором, точно определенном им смысле, “трансцендентных чисел столько же, сколько всех действительных чисел”, точнее доказать, что “множество трансцендентных чисел равномощно множеству всех действительных чисел”. Это было поразительное математическое открытие конца XIX века — получается, что сто лет математики искали примеры трансцендентных чисел, ценой значительных усилий строили отдельные примеры таких чисел, ценой еще больших усилий доказывали трансцендентность конкретных чисел, а оказалось, что “почти все числа трансцендентны, возьми случайным образом действительное число и оно с очень большой вероятностью окажется трансцендентным”. Это яркий пример мощности теоретико-множественных методов, что и позволило им, на наш взгляд, в первой половине XX века пронизать (“захватить”) значительную часть математики. Однако доказательство Г. Кантора — это и яркий пример “неконструктивного” доказательства: чтобы доказать, что трансцендентные числа существуют, доказывалось, что их “очень много”, однако доказательство не позволяет, по крайней мере без значительных дополнительных усилий, строить конкретные примеры трансцендентных чисел. Доказательство Ж. Лиувилля все же позволяет строить конкретные примеры трансцендентных чисел, хотя это построение и требует некоторых дополнительных усилий, доказательство же Г. Кантора требует еще больших усилий. Можно было бы сказать, что доказательство Г. Кантора не позволяет строить примеры трансцендентных чисел, однако это утверждение, как и большинство излишне категоричных утверждений может быть оспорено.

Первым шагом на пути доказательства теоремы Г. Кантора о мощности множества трансцендентных чисел является следующая теорема, доказанная Г. Кантором в работе, опубликованной в 1874 году. Это была первая публикация Г. Кантора по теории множеств. В этой же работе Г. Кантор доказал, что множество действительных чисел не является счетным. Общее же определение равномощности множеств было дано Г. Кантором лишь в 1877 году.

**Теорема 5.13.** *Множество всех алгебраических чисел счетно.*

*Доказательство.* Счетность множества  $\mathbb{Z}$  целых чисел следует из равенства  $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup (-\mathbb{N})$ , где  $-\mathbb{N} = \{-n \mid n \in \mathbb{N}\}$ . Сопоставив каждому ненулевому многочлену с целыми коэффициентами  $f = a_0 + a_1x + \dots + a_nx^n$ ,  $a_n \neq 0$  последовательность  $\langle a_0, a_1, \dots, a_n \rangle$  целых чисел, получим вложение множества  $(\mathbb{Z}[x])^+$  ненулевых многочленов с целыми коэффициентами во множество  $(\mathbb{Z})^*$  всех конечных последовательностей целых чисел. А так как последнее множество счетно, то счетно и множество  $(\mathbb{Z}[x])^+$  всех ненулевых многочленов с целыми коэффициентами. Для ненулевого многочлена  $f$  через  $\mathbb{C}_f$  обозначим множество его комплексных корней. Из курса алгебры хорошо известно, что  $\mathbb{C}_f$  — конечное множество, число элементов которого не превосходит степени многочлена  $f$ . Теперь счетность множества  $\mathcal{A}$  следует из равенства

$$\mathcal{A} = \bigcup_{f \in (\mathbb{Z}[x])^+} \mathbb{C}_f.$$

□

**Теорема 5.14.** *Множество всех действительных чисел не является счетным.*

*Доказательство.* Докажем, что не является счетным даже множество чисел из интервала  $(0, 1)$ . Отсюда в силу следствия теоремы 5.7 мы получим, что множество всех действительных чисел тоже не является счетным.

Покажем, что для любой счетной последовательности

$$\alpha_1, \dots, \alpha_n, \dots \quad (*)$$

действительных чисел из интервала  $(0, 1)$  в этом интервале существует число, которое не входит в эту последовательность, т.е. *никакая последовательность (\*) не может содержать все числа интервала  $(0, 1)$* . Представим каждое число последовательности (\*) в виде бесконечной десятичной дроби, не содержащей 9 в периоде, для обеспечения однозначности представления

$$\alpha_n = 0, a_{n1}a_{n2} \dots a_{nk} \dots$$

Полагаем  $a_n$  равным 0, если  $a_{nn}$  отлично от 0, и равным 1, если  $a_{nn}$  равно 0. Ясно, что  $a_n$  не равно  $a_{nn}$ , поэтому число

$$\alpha = 0, a_1a_2 \dots a_n \dots$$

из интервала  $(0, 1)$  не содержится в последовательности (\*).

□

**Замечание.** Метод, использованный нами для построения числа  $\alpha$ , был изобретен Г. Кантором и носит название *диагональный метод Г. Кантора*. Он позволяет, по крайней мере в принципе, по любой последовательности, содержащей все

алгебраические числа, построить действительное число из интервала  $(0, 1)$ , не входящее в эту последовательность. Значит, это число будет трансцендентным. Однако, чтобы построить по этой схеме конкретное трансцендентное число, надо иметь в распоряжении (считать уже построенной) последовательность всех алгебраических чисел. Не будем пока эту тему развивать, так как это увело бы нас слишком далеко от основной цели. Диагональный метод Г. Кантора находит многочисленные применения при доказательстве фундаментальных теорем математической логики.

**Теорема 5.15.** Если  $\mathbb{R}$  — это множество всех действительных чисел, а  $\mathcal{A}$  — это множество всех алгебраических чисел, то  $\overline{\mathbb{R} \setminus \mathcal{A}} = \overline{\mathbb{R}}$ .

Заметим, что  $\mathbb{R} \setminus \mathcal{A}$  — это множество всех трансцендентных чисел.

*Доказательство.* Так как  $\mathbb{R} = (\mathbb{R} \setminus \mathcal{A}) \cup \mathcal{A}$ , то множество  $\mathbb{R} \setminus \mathcal{A}$  бесконечно в силу теорем 5.13, 5.8 и 5.14, поэтому нужное равенство следует из теорем 5.13 и 5.8.  $\square$

## 6. Множества мощности континуума

В этом параграфе рассматриваются некоторые свойства множеств, равно-мощных множеству всех действительных чисел.

**Определение 6.1.** Множество  $A$ , равномощное множеству  $\mathbb{R}$  всех действительных чисел, называется **континуальным** множеством. Его мощность обозначается через  $\mathfrak{c}$  и называется **мощностью континуума**.

**Теорема 6.1.**  $\overline{(0, 1)} = \mathfrak{c}$ . Для любых действительных чисел  $a$  и  $b$ , если  $a < b$ , то  $\overline{(a, b)} = \mathfrak{c}$  и  $\overline{[a, b]} = \mathfrak{c}$ .

*Доказательство.* Функция  $f(x) = \operatorname{tg}(\pi x - \pi/2)$  задает биективное отображение интервала  $(0, 1)$  на множество  $\mathbb{R}$  всех действительных чисел.

Функция  $g(x) = (b - a)x + a$  задает биективное отображение интервала  $(0, 1)$  на интервал  $(a, b)$ .

Остается заметить, что  $[a, b] = (a, b) \cup \{a, b\}$  и сослаться на теорему 5.8.  $\square$

**Теорема 6.2.** Для любого натурального числа  $n$  выполняются равенства  $\overline{(0, 1)^n} = \mathfrak{c}$  и  $\overline{\mathbb{R}^n} = \mathfrak{c}$ .

Для любых действительных чисел  $a$  и  $b$ , если  $a < b$ , то  $\overline{(a, b)^n} = \mathfrak{c}$  и  $\overline{[a, b]^n} = \mathfrak{c}$ .

*Доказательство.* Доказательство проведем индукцией по  $n$ . Очевидно, что  $\mathfrak{c} = \overline{(0, 1)} \leq \overline{(0, 1)^2}$ .

Г. Кантор придумал весьма остроумный способ вложения интервала  $(0, 1)$  в квадрат  $(0, 1)^2$ . Напомним, что каждое действительное число однозначно представимо в виде бесконечной десятичной дроби, не содержащей 9 в периоде. Точке  $(a, b)$  квадрата  $(0, 1)^2$ , где

$$a = 0, a_1 a_2 a_3 \dots a_n \dots, \quad b = 0, b_1 b_2 b_3 \dots b_n \dots$$

Г. Кантор сопоставил действительное число

$$\varphi(a, b) = 0, a_1 b_1 a_2 b_2 a_3 b_3 \dots a_n b_n \dots$$

и получил вложение  $\varphi$  квадрата  $(0, 1)^2$  в интервал  $(0, 1)$ . Значит,  $\overline{\overline{(0, 1)^2}} \leq \overline{\overline{(0, 1)}}$ . Поэтому  $\overline{\overline{(0, 1)^2}} = \overline{\overline{(0, 1)}}$ . Теперь индукцией по  $n$  легко получить равенство  $\overline{\overline{(0, 1)^n}} = \overline{\overline{(0, 1)}}$ .

Откуда сразу следуют остальные утверждения теоремы.  $\square$

**Следствие.** Если при любом  $i$  ( $i = 1, \dots, n$ )  $A_i$  — множество мощности  $\mathfrak{c}$ , то и их прямое произведение  $A_1 \times \dots \times A_n$  имеет мощность  $\mathfrak{c}$ .

**Теорема 6.3.** Множество  $P(\mathbb{N})$  всех подмножеств множества натуральных чисел  $\mathbb{N}$  имеет мощность  $\mathfrak{c}$ , т.е. выполняется равенство  $\mathfrak{c} = 2^{\aleph_0}$ .

*Д о к а з а т е л ь с т в о.* Пусть  $\chi_A$  — характеристическая функция подмножества  $A$  множества  $\mathbb{N}$  натуральных чисел, т.е.

$$\chi_A = 1, \text{ если } x \in A \quad \text{и} \quad 0, \text{ если } x \in \mathbb{N} \setminus A.$$

Сопоставив произвольному подмножеству  $A$  множества  $\mathbb{N}$  натуральных чисел действительное число из интервала  $(0, 1)$

$$0, \chi_A(0) \chi_A(1) \chi_A(2) \chi_A(3) \dots \chi_A(n) \dots,$$

получим вложение множества  $P(\mathbb{N})$  всех подмножеств множества  $\mathbb{N}$  в интервал  $(0, 1)$ . Значит,

$$\overline{\overline{P(\mathbb{N})}} \leq \overline{\overline{(0, 1)}}.$$

Каждое число  $\alpha$  из интервала  $(0, 1)$  представимо в виде бесконечной двоичной дроби  $(0, a_1 a_2 \dots a_n)_2$ , где  $a_n \in \{0, 1\}$ , т.е.  $\alpha = a_1/2 + a_2/2^2 + a_3/2^3 + \dots + a_n/2^n + \dots$ . Причем, если исключить из рассмотрения двоичные дроби, содержащие 1 в периоде, то указанное представление однозначно. Это позволяет задать вложение интервала  $(0, 1)$  в  $P(\mathbb{N})$ , сопоставляя числу  $\alpha = a_1/2 + a_2/2^2 + a_3/2^3 + \dots + a_n/2^n + \dots$  подмножество  $\{a_1, a_2, a_3, \dots, a_n, \dots\}$ . Значит,

$$\overline{\overline{(0, 1)}} \leq \overline{\overline{P(\mathbb{N})}}.$$

И остается сослаться на теорему Кантора — Шредера — Бернштейна.  $\square$



Из доказанной теоремы и теоремы Г. Кантора (см. стр. 45) о мощности множества всех подмножеств данного множества сразу получаем

**Следствие.**  $\aleph_0 < \mathfrak{c}$ . Множество всех действительных чисел не является счетным.

**Следствие.** Множество трансцендентных чисел равномощно множеству всех действительных чисел.

*Доказательство.* Пусть  $\mathcal{A}$  — множество всех трансцендентных действительных чисел. Так как множество  $\mathbb{R}$  всех действительных чисел не является счетным и  $\mathbb{R} = (\mathbb{R} \setminus \mathcal{A}) \cup \mathcal{A}$ , то в силу теоремы 5.8 и множество  $\mathbb{R} \setminus \mathcal{A}$  не является конечным или счетным (в противном случае счетным было бы и множество  $\mathbb{R}$  всех действительных чисел), поэтому по теореме 5.8  $\overline{\mathbb{R}} = \overline{(\mathbb{R} \setminus \mathcal{A}) \cup \mathcal{A}} = \overline{\mathbb{R} \setminus \mathcal{A}}$ .  $\square$

**Теорема 6.4.** Множество всех бесконечных последовательностей, составленных из двух чисел 0 и 1, имеет мощность  $\mathfrak{c}$ .

Множество всех последовательностей, составленных из двух чисел 0 и 1, имеет мощность  $\mathfrak{c}$ .

*Доказательство.* Покажем, что множество  $S(0, 1)$  всех бесконечных последовательностей, составленных из двух чисел 0 и 1, равномощно множеству  $P(\mathbb{N})$  всех подмножеств множества натуральных чисел  $\mathbb{N}$ , которое имеет мощность  $\mathfrak{c}$ .

Сопоставим произвольному подмножеству  $A$  множества  $\mathbb{N}$  натуральных чисел последовательность

$$\chi_A(0), \chi_A(1), \chi_A(2), \chi_A(3), \dots, \chi_A(n), \dots,$$

где  $\chi_A$  — характеристическая функция подмножества  $A$  множества  $\mathbb{N}$  натуральных чисел, т.е.

$$\chi_A = 1, \text{ если } x \in A \text{ и } 0, \text{ если } x \in \mathbb{N} \setminus A.$$

Получим биективное отображение множества  $P(\mathbb{N})$  всех подмножеств множества  $\mathbb{N}$  на  $S(0, 1)$ . Значит,

$$\overline{P(\mathbb{N})} = \overline{S(0, 1)}.$$

Для завершения доказательства остается воспользоваться теоремой 6.3.  $\square$

**Теорема 6.5.** Множество всех бесконечных последовательностей натуральных чисел имеет мощность  $\mathfrak{c}$ .

Множество всех последовательностей натуральных чисел имеет мощность  $\mathfrak{c}$ .



*Д о к а з а т е л ь с т в о.* Покажем, что множество  $\mathbb{N}^{\mathbb{N}}$  всех бесконечных последовательностей натуральных чисел равномощно множеству  $S(0, 1)$  всех бесконечных последовательностей, составленных из двух чисел 0 и 1.

Для произвольного натурального числа  $n$  обозначим через  $0^n$  последовательность  $0, 0, \dots, 0$ , состоящую из  $n$  нулей.

Сопоставив произвольной бесконечной последовательности

$$a_1, a_2, \dots, a_n, \dots$$

натуральных чисел последовательность

$$0^{a_1}, 1, 0^{a_2}, 1, \dots, 1, 0^{a_n}, 1, \dots,$$

получим неравенство

$$\overline{\mathbb{N}^{\mathbb{N}}} \leq \overline{S(0, 1)}.$$

А так как обратное неравенство очевидно, то получаем равенство

$$\overline{\mathbb{N}^{\mathbb{N}}} = \overline{S(0, 1)}.$$

Для завершения доказательства остается воспользоваться теоремой 6.4.  $\square$

**Теорема 6.6.** *Объединение счетного множества множеств мощности  $\mathfrak{c}$  само имеет мощность  $\mathfrak{c}$ .*

*Д о к а з а т е л ь с т в о.* Пусть при любом  $n \in \mathbb{N}$  множество  $A_n$  имеет мощность  $\mathfrak{c}$ .

Полагаем

$$B_1 \Leftarrow A_1, \quad B_{n+1} \Leftarrow A_{n+1} \setminus (A_1 \cup A_2 \cup \dots \cup A_n).$$

Тогда при любом  $n$ :  $B_n \subseteq A_n$  и при  $n \neq m$  множества  $B_n$  и  $B_m$  не пересекаются

$$\bigcup_{n \in \mathbb{N}} A_n = \bigcup_{n \in \mathbb{N}} B_n.$$

При каждом  $n \in \mathbb{N}$  существует вложение  $\varphi_n$  множества  $B_n$  в сегмент  $[1/n + 1, 1/n)$ . Тогда

$$\varphi \Leftarrow \bigcup_{n \in \mathbb{N}} \varphi_n$$

служит вложением множества

$$\bigcup_{n \in \mathbb{N}} A_n = \bigcup_{n \in \mathbb{N}} B_n$$

в интервал  $(0, 1)$ . Поэтому

$$\overline{\bigcup_{n \in \mathbb{N}} A_n} \leq \overline{(0, 1)}.$$

Это вместе с неравенством

$$\overline{(0, 1)} = \overline{A_1} \leq \overline{\bigcup_{n \in \mathbb{N}} A_n}$$

дает нужное равенство

$$\overline{\bigcup_{n \in \mathbb{N}} A_n} = \overline{(0, 1)}.$$

$\square$

**Теорема 6.7.** *Объединение континуального множества множеств мощности  $\mathfrak{c}$  само имеет мощность  $\mathfrak{c}$ .*

*Доказательство.* Пусть при любом  $\alpha \in (0, 1)$  множество  $A_\alpha$  имеет мощность  $\mathfrak{c}$ . Обозначим через  $\varphi_\alpha$  некоторое биективное отображение интервала  $(0, 1)$  на множество  $A_\alpha$ , имеющее по условию мощность  $\mathfrak{c}$ . Полагаем  $\varphi(\alpha, t) \doteq \varphi_\alpha(t)$ . Тогда  $\varphi$  — сюръективное отображение единичного квадрата  $(0, 1) \times (0, 1)$  на множество

$$\bigcup_{\alpha \in (0, 1)} A_\alpha.$$

Это дает неравенство

$$\overline{\bigcup_{\alpha \in (0, 1)} A_\alpha} \leq \overline{(0, 1) \times (0, 1)} = \overline{(0, 1)}.$$

Обратное неравенство очевидно. □

**Теорема 6.8.** *Множество всех бесконечных последовательностей действительных чисел имеет мощность  $\mathfrak{c}$ .*

*Множество всех последовательностей действительных чисел имеет мощность  $\mathfrak{c}$ .*

*Доказательство.* Покажем, что множество  $\mathbb{R}^{\mathbb{N}}$  всех бесконечных последовательностей действительных чисел имеет мощность  $\mathfrak{c}$ . Используя теоремы 6.4 и 5.5, получаем равенства

$$\overline{\mathbb{R}^{\mathbb{N}}} = \overline{(\{0, 1\}^{\mathbb{N}})^{\mathbb{N}}} = \overline{\{0, 1\}^{\mathbb{N} \times \mathbb{N}}} = \overline{\{0, 1\}^{\mathbb{N}}} = \overline{\mathbb{R}}.$$

□

## 7. Операции над кардинальными числами

Как уже было сказано выше, мы считаем, что каждому множеству  $A$  сопоставлено **кардинальное число**  $\mathfrak{n}$ , которое обозначается часто через  $\overline{A}$ , называемое *мощностью* множества  $A$ , причем  $\overline{A} = \overline{B}$  тогда и только тогда, когда множества  $A$  и  $B$  равномощны, т.е. существует биективное отображение одного из них на другое. При этом, если соответствующее множество  $A$  — конечно, то и кардинальное число называется конечным, а если бесконечно — то бесконечным кардинальным числом.

**Определение 7.1.** *Суммой кардинальных чисел  $\mathfrak{n}_1$  и  $\mathfrak{n}_2$  называется кардинальное число  $\mathfrak{n} = \overline{A_1 \cup A_2}$ , где  $A_1$  и  $A_2$  — такие непересекающиеся множества, что  $\mathfrak{n}_i = \overline{A_i}$  ( $i = 1, 2$ ).*

Нетрудно проверить, что определение суммы двух кардинальных чисел не зависит от выбора множеств  $A_1$  и  $A_2$ .

Сумма кардинальных чисел  $n_1$  и  $n_2$  обозначается через  $n_1 + n_2$ .

Читателю в качестве упражнения предлагается доказать, что для операции сложения кардинальных чисел выполняются свойства *коммутативности*, *ассоциативности* и кардинальное число  $\overline{\emptyset}$  играет роль *нейтрального элемента*.

Аналогичным образом можно определить сумму любого семейства кардинальных чисел.

**Определение 7.2.** Суммой семейства кардинальных чисел  $(n_i)_{i \in I}$  называется кардинальное число  $n = \overline{\bigcup_{i \in I} A_i}$ , где  $(A_i)_{i \in I}$  — такое семейство попарно непересекающихся множеств, что при любом  $i \in I$ :  $n_i = \overline{A_i}$ .

Нетрудно проверить, что определение суммы семейства кардинальных чисел не зависит от выбора семейства множеств  $(A_i)_{i \in I}$ .

Сумма семейства кардинальных чисел  $(n_i)_{i \in I}$  обозначается через  $\sum_{i \in I} n_i$ .

Аналогичным образом определяется произведение двух кардинальных чисел и произведение семейства кардинальных чисел.

**Определение 7.3.** Произведением кардинальных чисел  $n_1$  и  $n_2$  называется кардинальное число  $n = \overline{A_1 \times A_2}$ , где  $A_1$  и  $A_2$  — такие множества, что  $n_i = \overline{A_i}$  ( $i = 1, 2$ ).

Нетрудно проверить, что определение произведения двух кардинальных чисел не зависит от выбора множеств  $A_1$  и  $A_2$ .

Произведение кардинальных чисел  $n_1$  и  $n_2$  обозначается через  $n_1 \cdot n_2$ .

Читателю в качестве упражнения предлагается доказать, что для операции умножения кардинальных чисел выполняются свойства *коммутативности*, *ассоциативности* и кардинальное число  $\{\overline{\emptyset}\}$  играет роль *нейтрального элемента*.

Аналогичным образом можно определить произведение любого семейства кардинальных чисел.

**Определение 7.4.** Произведением семейства кардинальных чисел  $(n_i)_{i \in I}$  называется кардинальное число  $n = \overline{\prod_{i \in I} A_i}$ , где  $(A_i)_{i \in I}$  — такое семейство множеств, что при любом  $i \in I$   $n_i = \overline{A_i}$ .

Нетрудно проверить, что определение произведения семейства кардинальных чисел не зависит от выбора семейства множеств  $(A_i)_{i \in I}$ .

Произведение семейства кардинальных чисел  $(n_i)_{i \in I}$  обозначается через  $\prod_{i \in I} n_i$ .

Введем обозначения  $0 \hat{=} \emptyset$ ,  $1 \hat{=} \{\emptyset\}$ .

Хотя для кардинальных чисел выполняются равенства

$$1.1) \quad n_1 + n_2 = n_2 + n_1,$$

$$1.2) \quad (n_1 + n_2) + n_3 = n_1 + (n_2 + n_3),$$

$$1.3) \quad n_1 + 0 = n_1,$$

$$2.1) \quad n_1 \cdot n_2 = n_2 \cdot n_1,$$

$$2.2) \quad (n_1 \cdot n_2) \cdot n_3 = n_1 \cdot (n_2 \cdot n_3),$$

$$2.3) \quad n_1 \cdot 1 = n_1,$$

$$3.1) \quad (n_1 + n_2) \cdot n_3 = n_1 \cdot n_3 + n_2 \cdot n_3,$$

как и для натуральных чисел, но на этом аналогия с натуральными числами, пожалуй, и заканчивается.

Из теоремы 5.7 следует, что для любого бесконечного кардинального числа  $n$  выполняется равенство  $\aleph_0 + n = n$ , в частности,  $\aleph_0 + \aleph_0 = \aleph_0$  и  $\aleph_0 + c = c$ .

Так как  $[0, 1) \cup [1, 2] = [0, 2]$ , то  $c + c = c$ .

Из теоремы 5.5 следует, что выполняется равенство  $\aleph_0 \cdot \aleph_0 = \aleph_0$ , а из теоремы 6.6 — равенство  $\aleph_0 \cdot c = c$ .

По теореме 6.7  $c \cdot c = c$ .

Более того, в следующем параграфе будет доказано, что для любого бесконечного кардинального числа  $n$  выполняются равенства  $\aleph_0 \cdot n = n$ ,  $n + n = n$  и  $n \cdot n = n$ .

Напомним, что для произвольных множеств  $A$  и  $B$  через  $B^A$  обозначается множество всех отображений множества  $B$  во множество  $A$ . Читателю предлагается в качестве упражнения доказать, что если множества  $A$  и  $B$  конечные, причем множество  $A$  состоит из  $a$  элементов, а множество  $B$  — из  $b$ , то множество  $B^A$  состоит из  $b^a$  элементов. Это делает оправданным следующее определение.

**Определение 7.5.** Степенью кардинальных чисел  $n_1$  и  $n_2$  называется кардинальное число  $n = \overline{A_1^{A_2}}$ , где  $A_1$  и  $A_2$  — такие множества, что  $n_i = \overline{A_i}$  ( $i = 1, 2$ ).

Степень кардинальных чисел  $n_1$  и  $n_2$  обозначается через  $n_1^{n_2}$ .

Читателю предоставляется в качестве упражнения доказать, что для степеней кардинальных чисел выполняются обычные равенства:

$$m^n \cdot m^l = m^{n+l},$$

$$(m \cdot n)^l = m^l \cdot n^l,$$

$$(m^n)^l = m^{n \cdot l},$$

$$m^1 = m,$$

$$1^n = 1.$$

## 8. Вполне упорядоченные множества

Стандартное отношение порядка на множестве  $\mathbb{N}$  натуральных чисел обладает одним принципиально важным свойством, часто используемым в доказательствах вместо метода математической индукции, — *любое непустое подмножество множества натуральных чисел имеет наименьший элемент*. Стандартные упорядочивания множества рациональных и множества действительных чисел подобным свойством уже не обладают.

**Определение 8.1.** *Линейный порядок  $\leq$  на множестве  $A$  называется полным, а само множество  $A$  вместе с этим порядком — вполне упорядоченным, если любое непустое подмножество множества  $A$  имеет наименьший элемент.*

**Замечание.** Иногда мы будем обозначать вполне упорядоченное множество через  $\langle A, \leq \rangle$ , чтобы подчеркнуть, что это понятие включает в себя не только множество  $A$ , но и отношение полного порядка  $\leq$  на нем.

Не пытайтесь построить пример отношения полного порядка даже на множестве действительных чисел — сделать это трудно. Однако в этом параграфе будет доказано, что такое отношение существует, точнее будет доказано, что *любое множество можно вполне упорядочить*. Но доказательство будет неконструктивным и не позволит в “явном виде” построить пример полного порядка на множестве действительных чисел. Более того, из дальнейшего будет видно, что утверждение о возможности вполне упорядочить произвольное множество по сути дела должно рассматриваться в качестве одной из аксиом теории множеств, хотя по ряду причин, прежде всего исторического характера, поступают по-другому.

**Определение 8.2.** *Линейно упорядоченное множество  $\langle A, \leq_A \rangle$  называется подобным (изоморфным) линейно упорядоченному множеству  $\langle B, \leq_B \rangle$ , если существует такое биективное отображение  $f$  множества  $A$  на множество  $B$ , что для любых элементов  $x, y \in A$ :*

$$\text{если } x \leq_A y, \text{ то } f(x) \leq_B f(y).$$

Отображение  $f$  из предыдущего определения называется также **изоморфизмом** линейно упорядоченных множеств  $\langle A, \leq_A \rangle$  и  $\langle B, \leq_B \rangle$ .

Запись  $A \simeq B$  будет служить сокращением для утверждения: “*линейно упорядоченное множество  $A$  подобно линейно упорядоченному множеству  $B$* ”.

Ясно, что если линейно упорядоченные множества  $A$  и  $B$  подобны, то они равномощны.

В качестве упражнения читателю предоставляется возможность проверить, что так определенное отношение  $\simeq$  подобия обладает свойствами *рефлексивности, симметричности и транзитивности*.

Каждому линейно упорядоченному множеству  $A$  сопоставим символ  $\overline{A}$ , который назовем **порядковым типом** этого множества, при этом предполагаем, что *линейно упорядоченные множества  $A$  и  $B$  подобны тогда и только тогда, когда  $\overline{A} = \overline{B}$* .

Пусть множество  $A$  линейно упорядочено отношением  $\leq$ .

**Определение 8.3.** Начальным отрезком, отсекаемым элементом  $a$  множества  $A$ , называется множество

$$A_a = \{x \mid x \in A \text{ \& } x < a\}$$

Заметим, что  $a \notin A_a$  и  $A_a = \emptyset$  тогда и только тогда, когда  $a$  — наименьший элемент множества  $A$ . Если  $a, b \in A$  и  $a \leq b$ , то  $A_a \subseteq A_b$ .

Каждый отрезок  $A_a$ , как и любое непустое подмножество линейно упорядоченного множества, сам линейно упорядочен ограничением на нем отношения порядка  $\leq$  на множестве  $A$ .

Покажем, что если  $a, b \in A$  и  $a < b$ , то  $(A_b)_a = A_a$ . Пусть  $x \in A_a$ . Тогда  $x < a$ , так как  $a < b$ , то  $x < b$ , значит,  $x \in A_b$ . Но  $a \in A_b$  и  $x < a$ , поэтому  $x \in (A_b)_a$ . Значит,  $A_a \subseteq (A_b)_a$ . Обратно, пусть  $x \in (A_b)_a$  тогда  $x < a$ , значит,  $x \in A_a$ . Поэтому  $(A_b)_a \subseteq A_a$ . Тем самым доказано, что  $(A_b)_a = A_a$ .

Если  $a, b \in A$  и  $a < b$ , то  $A_a \subset A_b$ , т.к.  $a \in A_b$ , но  $a \notin A_a$ .

**Определение 8.4.** Множество всех отрезков линейно упорядоченного множества  $A$  будем обозначать через  $W(A)$ .

**Теорема 8.1.** Для любого линейно упорядоченного множества  $A$  множество  $W(A)$ , упорядоченное отношением включения  $\subseteq$ , подобно самому множеству  $A$ .

*Доказательство.* Естественным образом определим отображение  $\varphi$  множества  $A$  во множество  $W(A)$ , полагая

$$\varphi(a) = A_a.$$

Ясно, что  $\varphi$  — биекция множества  $A$  на множество  $W(A)$ .

При этом, если  $a \leq b$ , то  $A_a \subseteq A_b$ . Значит,  $\varphi$  — изоморфизм линейно упорядоченного множества  $A$  на линейно упорядоченное множество  $W(A)$ . Значит, линейно упорядоченное множество  $A$  подобно линейно упорядоченному множеству  $W(A)$ .  $\square$

**Определение 8.5.** Подмножество  $B$  линейно упорядоченного множества  $A$  называется **началом**  $A$ , если для любых элементов  $x$  и  $y$  множества  $A$  из того, что  $y \in B$  и  $x \leq y$ , следует  $x \in B$ .

**Теорема 8.2.** Если  $A$  — вполне упорядоченное множество, то его подмножество  $B$  является началом  $A$  тогда и только тогда, когда либо  $B = A$ , либо в  $A$  существует такой элемент  $a$ , что  $B = A_a$ .



*Доказательство.* Ясно, что и  $A$ , и  $A_a$  являются началами множества  $A$ .

Пусть  $B$  — начало множества  $A$  и  $B \neq A$ . Обозначим через  $a$  наименьший элемент множества  $A \setminus B$ . Нетрудно показать, что  $B = A_a$ .  $\square$

В дальнейшем через  $<$ ,  $<_A$ ,  $<_B$  и т.д. будем обозначать отношения строгого полного порядка, т.е.  $a < b \iff a \leq b \text{ \& } a \neq b$ . В частности,  $a \not< a$ .

**Определение 8.6.** *Отображение  $f$  линейно упорядоченного множества  $\langle A, <_A \rangle$  в линейно упорядоченное множество  $\langle B, <_B \rangle$  называется **монотонным**, если для любых элементов  $x, y \in A$  неравенство  $x <_A y$  влечет неравенство  $f(x) <_B f(y)$ .*

Легко понять, что любое монотонное отображение линейно упорядоченного множества в линейно упорядоченное множество является инъективным отображением.

**Теорема 8.3.** *Пусть  $f : A \rightarrow A$  — монотонное отображение вполне упорядоченного множества  $A$  в себя. Не существует элемента  $a \in A$  такого, что  $f(a) < a$ .*

*Доказательство.* Предположим противное: пусть найдутся монотонное отображение  $f : A \rightarrow A$  некоторого вполне упорядоченного множества  $A$  в себя и элемент  $a \in A$  такие, что  $f(a) < a$ . Тогда непусто следующее множество  $B$

$$B = \{x \mid x \in A \text{ \& } f(x) < x\}.$$

Пусть  $a$  — наименьший элемент множества  $B$ . Так как  $a \in B$ , то  $f(a) < a$ , откуда в силу монотонности отображения  $f$  получаем  $f(f(a)) < f(a)$ , значит,  $f(a) \in B$ . Но  $f(a) < a$ , а это противоречит предположению о минимальности элемента  $a$  во множестве  $B$ .  $\square$

**Следствие 1.** *Вполне упорядоченное множество не может быть подобно своему отрезку или его части.*

*Доказательство.* Если бы некоторое вполне упорядоченное множество  $A$  было подобно своему отрезку  $A_a$  или его части, то нашлось бы монотонное отображение  $f : A \rightarrow A_a$ . Тогда  $f(a) \in A_a$ , а значит,  $f(a) < a$ . Что противоречит теореме.  $\square$

**Следствие 2.** *Два различных отрезка вполне упорядоченного множества не могут быть подобны.*

*Доказательство.* Предположим, что два различных отрезка  $A_a$  и  $A_b$  некоторого вполне упорядоченного множества  $A$  подобны. Тогда  $a \neq b$ . Без ограничения общности можно считать, что  $a < b$ . Тогда вполне упорядоченное множество  $A_b$  подобно своему отрезку  $(A_b)_a = A_a$ . Что противоречит теореме.  $\square$

**Следствие 3.** Существует не более одного изоморфизма двух вполне упорядоченных множеств.

*Доказательство.* Допустим, что  $f$  и  $g$  — два различных монотонных отображения вполне упорядоченного множества  $A$  на вполне упорядоченное множество  $B$ . Тогда в  $A$  найдется такой элемент  $a$ , что  $f(a) \neq g(a)$ . Без ограничения общности можно считать, что  $f(a) <_B g(a)$ . Тогда  $(g^{-1} \circ f)(a) <_A a$ , но это невозможно, так как  $g^{-1} \circ f$  — монотонное отображение вполне упорядоченного множества  $A$  в себя.  $\square$

**Определение 8.7.** Ординальными или порядковыми числами называются порядковые типы  $\overline{A}$  вполне упорядоченных множеств  $A$ . При этом, если множество  $A$  конечно, то  $\overline{A}$  называется конечным ординальным числом, а если бесконечно — то бесконечным ординальным числом.

Ординальные числа часто называются просто ординалами.

Введем следующие обозначения

$$0 \equiv \overline{\emptyset}, n \equiv \overline{\mathbb{N}_n}, \omega \equiv \overline{\mathbb{N}},$$

где множество  $\mathbb{N}_n = \{1, 2, \dots, n\}$  и множество  $\mathbb{N}$  всех натуральных чисел упорядочены естественным образом в порядке возрастания элементов.

0 и  $n$  дают примеры конечных ординальных чисел, а  $\omega$  — пример бесконечного ординального числа. Других примеров бесконечных ординальных чисел у нас пока нет, они будут приведены позже.

Для ординальных чисел введем отношение строгого порядка  $<$ .

**Определение 8.8.** Для ординальных чисел  $\alpha = \overline{A}$  и  $\beta = \overline{B}$  полагаем  $\alpha < \beta$ , если множество  $A$  подобно (изоморфно) некоторому начальному отрезку множества  $B$ .

Ясно, что определение отношения  $\alpha < \beta$  не зависит от выбора множеств  $A$  и  $B$ .

Полагаем  $\alpha \leq \beta \iff (\alpha < \beta \vee \alpha = \beta)$ .

**Теорема 8.4.** Отношение  $<$  обладает всеми основными свойствами отношения линейного порядка:

- 1) иррефлексивность:  $\alpha \not< \alpha$ ;
- 2) транзитивность: если  $\alpha < \beta$  и  $\beta < \gamma$ , то  $\alpha < \gamma$ ;
- 3) сравнимость: если  $\alpha \neq \beta$ , то либо  $\alpha < \beta$ , либо  $\beta < \alpha$ .

*Доказательство.* 1) Иррефлексивность отношения  $<$  установлена в следствии 1 предыдущей теоремы.

2) Пусть  $\alpha < \beta$  и  $\beta < \gamma$ . Возьмем такие множества  $A$ ,  $B$  и  $C$ , что  $\alpha = \overline{A}$ ,  $\beta = \overline{B}$ ,  $\gamma = \overline{C}$ . Пусть  $f$  — изоморфизм  $A$  на  $B$ ,  $g$  — изоморфизм  $B$  на  $C$ . Покажем, что  $g \circ f$  — изоморфизм  $A$  на  $C_{g(b)}$ .

Ясно, что  $g \circ f$  — монотонное отображение  $A$  в  $C$ . При этом, если  $a \in A$ , то  $f(a) < b$ , значит,  $g(f(a)) < g(b)$ . Поэтому  $g \circ f$  — монотонное отображение  $A$  в  $C_{g(b)}$ . Остается доказать сюръективность этого отображения. Так как  $g(B) = C_c$ , то  $g(b) < c$ . Пусть  $e \in C_{g(b)}$ , тогда  $e < g(b)$ , а значит,  $e < c$ . Поэтому  $e \in C_c = g(B)$ , значит, найдется такой элемент  $d \in B$ , что  $e = g(d)$ . Покажем, что  $d < b$ . Если бы выполнялось неравенство  $b \leq d$ , то из монотонности отображения  $g$  мы получили бы  $g(b) \leq g(d) = e$ , что противоречит неравенству  $e < g(b)$ . Так как  $B_b = f(A)$ , то найдется в  $A$  такой элемент  $a$ , что  $d = f(a)$ . Тогда  $e = g(d) = g(f(a)) = (g \circ f)(a)$ . Значит,  $g \circ f$  — изоморфизм множества  $A$  на отрезок  $C_{g(b)}$  множества  $C$ .

Остается доказать самую сложную и наиболее важную для дальнейшего изложения часть теоремы.

3) Сравнимость. Пусть  $A$  и  $B$  — вполне упорядоченные множества. Покажем, что либо они подобны, либо одно из них подобно отрезку другого. Рассмотрим множество

$$D = \{ \langle a, b \rangle \mid a \in A \ \& \ b \in B \ \& \ A_a \simeq B_b \}.$$

Покажем, что  $D$  — функциональное, инъективное, монотонное отношение. Если  $\langle a, b \rangle \in D$ , то через  $f_{a,b}$  обозначим изоморфизм отрезка  $A_a$  на отрезок  $B_b$ . В силу следствия 3 для каждой пары  $\langle a, b \rangle$  изоморфизм  $f_{a,b}$  определен однозначно.

а) Функциональность.

Если  $\langle a, b \rangle \in D$  и  $\langle a, c \rangle \in D$ , то  $A_a \simeq B_b$  и  $A_a \simeq B_c$ , значит,  $B_b \simeq B_c$ . Откуда по следствию 2 предыдущей теоремы получаем  $b = c$ .

б) Инъективность.

Если  $\langle a, b \rangle \in D$  и  $\langle c, b \rangle \in D$ , то  $A_a \simeq B_b$  и  $A_c \simeq B_b$ , значит,  $A_a \simeq A_c$ . Откуда по следствию 2 предыдущей теоремы получаем  $a = c$ .

в) Монотонность.

Пусть  $\langle a_1, b_1 \rangle \in D$  и  $\langle a_2, b_2 \rangle \in D$ , причем  $a_1 < a_2$ . Покажем, что  $b_1 < b_2$ .  $f_{a_1, b_1}$  — изоморфизм отрезка  $A_{a_1}$  на отрезок  $B_{b_1}$ . Так как  $a_1 < a_2$ , то  $A_{a_1} \subseteq A_{a_2}$ .

Обозначим через  $f$  ограничение на  $A_{a_1}$  изоморфизма  $f_{a_2, b_2}$ . Ясно, что  $f$  — монотонное отображение отрезка  $A_{a_1}$  в отрезок  $B_{b_2}$ . Полагаем  $b = f_{a_2, b_2}(a_1)$ . Покажем, что  $f(A_{a_1}) = B_b$ .

Если  $x \in A_{a_1}$ , то  $x < a_1$ , поэтому  $f(x) = f_{a_2, b_2}(x) < f_{a_2, b_2}(a_1) = b$ . Значит,  $f(A_{a_1}) \subseteq B_b$ .

Пусть  $z \in B_b$ . Тогда  $z < b = f_{a_2, b_2}(a_1) < b_2$ , значит,  $z \in B_{b_2} = f_{a_2, b_2}(A_{a_2})$ . Поэтому в  $A_{a_2}$  найдется элемент  $c$  такой, что  $z = f_{a_2, b_2}(c)$ . Покажем, что  $c < a_1$ . Предположим противное  $a_1 \leq c$ . Тогда противоречивую систему неравенств

$$b = f_{a_2, b_2}(a_1) \leq f_{a_2, b_2}(c) = z < b.$$

Значит,  $B_b \subseteq f_{a_2, b_2}(A_{a_1}) = f(A_{a_1})$ .

Итак,  $f_{a_1, b_1}$  — изоморфное отображение отрезка  $A_{a_1}$  на отрезок  $B_{b_1}$ , а  $f$  — изоморфное отображение того же отрезка  $A_{a_1}$  на отрезок  $B_b$ . Отсюда следует, что отрезки  $B_{b_1}$  и  $B_b$  подобны. Значит, по следствию 2 теоремы 8.3

$b_1 = b = f_{a_2, b_2}(a_1)$ . Значит,  $b_1 \in B_{b_2}$ , т.е.  $b_1 < b_2$ . Кроме того, ясно, что  $f = f_{a_1, b_1}$ , т.е. ограничение  $f_{a_2, b_2} \upharpoonright_{A_{a_1}}$  на  $A_{a_1}$  изоморфизма  $f_{a_2, b_2}$  совпадает с  $f_{a_1, b_1}$ .

Из вышесказанного следует, что  $D$  — изоморфизм своей области определения  $\delta(D)$  на свою область значений  $\varrho(D)$ . Остается выяснить, что собой представляют область определения  $\delta(D)$  и область значений  $\varrho(D)$  отображения  $D$ .

Докажем, что если  $\langle a, b \rangle \in D$ , то  $f_{a, b} \subseteq D$ . Пусть  $\langle c, d \rangle \in f_{a, b}$ , значит,  $f_{a, b}(c) = d$ . Покажем, что  $f_{a, b} \upharpoonright_A$  — изоморфизм отрезка  $A_c$  на отрезок  $B_d$ .

Заметим, что  $f_{a, b} \upharpoonright_A$  — монотонное отображение отрезка  $A_c$  в отрезок  $B_b$ . При этом, если  $m \in A_c$ , то  $m < c$ , значит,  $f_{a, b} \upharpoonright_A (m) = f_{a, b}(m) < f_{a, b}(c) = d$ . Следовательно,  $f_{a, b} \upharpoonright_A (A_c) \subseteq B_d$ . Пусть  $z \in B_d$ . Тогда  $z < d < b$ . В отрезке  $A_a$  найдется элемент  $n$  такой, что  $z = f_{a, b}(n)$ . Как и выше убеждаемся, что  $n \in A_c$ . Значит,  $f_{a, b} \upharpoonright_A (A_c) = B_d$ , поэтому  $\langle c, d \rangle \in D$ . Следовательно,  $f_{a, b} \subseteq D$ .

Покажем, что область определения  $\delta(D)$  отношения  $D$  является началом множества  $A$ . Пусть  $x, y \in A$ ,  $x < y$  и  $y \in \delta(D)$ . Покажем, что  $x \in \delta(D)$ . Отрезок  $A_y$  изоморфен отрезку  $B_b$  при некотором  $b \in B$ . Пусть  $f$  — изоморфизм отрезка  $A_y$  на отрезок  $B_b$ . Покажем, что ограничение  $f \upharpoonright_{A_x}$  изоморфизма  $f$  изоморфно отображает  $A_x = (A_y)_x$  на  $(B_b)_{f(x)} = B_{f(x)}$  (так как  $x < y$ , то  $x \in A_y$ , значит,  $f(x) \in B_b$ , т.е.  $f(x) < b$ ). Полагаем  $\varphi = f \upharpoonright_{A_x}$ . Если  $z \in A_x$ , то  $z < x$ , значит,  $\varphi(z) = f(z) < f(x)$ . Поэтому  $\varphi$  — монотонное отображение отрезка  $A_x$  в отрезок  $B_{f(x)}$ . Остается убедиться в сюръективности отображения  $\varphi$ . Пусть  $c \in B_{f(x)}$ , тогда  $c \in B_b$ , поэтому в  $A_a$  найдется такой элемент  $a$ , что  $c = f(a)$ . Покажем, что  $a \in A_x$ . Предположим, что  $x \leq a$ , тогда  $f(x) \leq f(a)$ , т.е.  $f(x) \leq c$ . Но последнее неравенство противоречит выбору  $c$  —  $c \in B_{f(x)}$ . Значит,  $a \in A_x$ , поэтому  $c = f(a) = \varphi(a)$ . Поэтому  $\varphi$  — изоморфизм отрезка  $A_x$  на отрезок  $B_{f(x)}$ , значит,  $\langle x, f(x) \rangle \in D$ ,  $x \in D$ .

Совершенно аналогично доказывается, что область значений  $\varrho(D)$  отображения  $D$  является началом множества  $B$ .

По теореме 8.2 возможен один из следующих четырех случаев.

- 1)  $\delta(D) = A$ ,  $\varrho(D) = B$ . В этом случае  $A \simeq B$ .
- 2)  $\delta(D) = A$ ,  $\varrho(D) = B_b$  для некоторого  $b \in B$ . В этом случае  $A \simeq B_b$ .
- 3)  $\delta(D) = A_a$  для некоторого  $a \in A$ ,  $\varrho(D) = B$ . В этом случае  $A_a \simeq B$ .
- 4)  $\delta(D) = A_a$ ,  $\varrho(D) = B_b$  для некоторых  $a \in A$ ,  $b \in B$ .

Покажем, что случай 4) невозможен. В самом деле, в случае 4)  $D$  — изоморфизм отрезка  $A_a$  на отрезок  $B_b$ . Значит,  $\langle a, b \rangle \in D$ , но тогда  $a \in \delta(D) = A_a$ , что невозможно. Это завершает доказательство теоремы.  $\square$

Если  $A$  и  $B$  — вполне упорядоченные множества и  $\bar{A} \leq \bar{B}$ , то  $\bar{\bar{A}} \leq \bar{\bar{B}}$ .

Поэтому получаем следующее важное следствие.

**Следствие.** Если  $A$  и  $B$  — вполне упорядоченные множества, то либо  $\bar{\bar{A}} \leq \bar{\bar{B}}$ , либо  $\bar{\bar{B}} \leq \bar{\bar{A}}$ . Т.е. любые два вполне упорядоченных множества сравнимы по мощности.

Для установления дальнейших свойств операций над кардинальными числами нам потребуется привлекать ординальные числа. Связь между этими числами устанавливается с помощью *теоремы Цермело о возможности вполне упорядочить любое множество*. Однако доказательство этой теоремы опирается на специальное утверждение теории множеств, называемое *аксиомой выбора*. Представляется естественным рассмотреть некоторые утверждения эквивалентные аксиоме выбора.

**1. Аксиома выбора.** Если  $f$  — отображение множества  $X$  во множество  $Y$  и при любом  $x \in X$   $f(x)$  — непустое множество, то существует функция выбора  $g$ , определенная на множестве  $X$  со значениями во множестве  $\bigcup_{x \in X} f(x)$  такая, что для любого  $x$  из  $X$   $g(x) \in f(x)$ .

**2. Лемма Цорна.** Частично упорядоченное множество, каждое из линейно упорядоченных подмножеств которого имеет верхнюю грань, содержит максимальный элемент.

**3. Принцип максимальности Куратовского — Хаусдорфа.** Каждая цепь частично упорядоченного множества содержится в некоторой максимальной цепи.

**4. Аксиома Цермело.** Для любого множества  $\mathcal{X}$  непустых попарно непересекающихся множеств существует такое множество  $B$ , что для любого множества  $A$  из  $\mathcal{X}$  множество  $A \cap B$  состоит ровно из одного элемента.

**5. Теорема Цермело.** Каждое множество можно вполне упорядочить.

Для формулировки следующего утверждения нам потребуется понятие семейства подмножеств, имеющего конечный характер.

**Определение 8.9.** Семейство подмножеств  $\mathcal{X}$  множества  $E$  имеет **конечный характер**, если для каждого подмножества  $A$  множества  $E$  имеет место эквивалентность:

$A$  принадлежит  $\mathcal{X}$  тогда и только тогда, когда каждое конечное подмножество множества  $A$  принадлежит  $\mathcal{X}$ .

**6. Лемма Тейхмюллера — Тьюки.** Каждое семейство подмножеств  $\mathcal{X}$  множества  $E$ , имеющее конечный характер, обладает максимальным элементом.

**7.** Для любого отображения  $f$  множества  $A$  на непустое множество  $B$  существует функция  $g$  из  $B$  в  $A$  такая, что  $f \circ g = i_B$ .

Заметим, что функция  $g$  будет инъекцией.

**8. Аксиома мультипликативности.** Декартово произведение непустого семейства непустых множеств непусто.



**Теорема 8.5.** *Сформулированные выше восемь утверждений эквивалентны.*

*Доказательство.* Доказательство проведем по следующей схеме

$$\begin{array}{ccccc}
 (3) & \implies & (2) & \iff & (6) \\
 \uparrow & & \downarrow & & \\
 (5) & \implies & (1) & \iff & (8) \\
 & & \downarrow & & \\
 & & (4) & & \\
 & & \downarrow & & \\
 & & (7) & & 
 \end{array}$$

$(2) \implies (1)$ .

Пусть  $f$  — отображение множества  $X$  во множество  $Y$  и при любом  $x \in X$   $f(x)$  — непустое множество. Используя **Лемму Цорна** докажем, что существует **функция выбора**  $g$ , определенная на множестве  $X$  со значениями во множестве  $\bigcup_{x \in X} f(x)$  такая, что для любого  $x$  из  $X$   $g(x) \in f(x)$ .

Обозначим через  $T$  следующее множество

$$\{ \varphi \mid \varphi \subseteq X \times \bigcup_{x \in X} f(x) \text{ \& } \varphi \text{ — функционально} \}$$

для любого  $x$  из  $\delta(\varphi)$   $\varphi(x) \in f(x)$  },

т.е. это множество всех отображений, определенных на подмножествах множества  $X$  со значениями во множестве  $\bigcup_{x \in X} f(x)$ , обладающих свойством: если  $x \in X$  и  $\varphi(x)$  определено, то  $\varphi(x) \in f(x)$ .

Множество  $T$  непусто, так как, например,  $\{ \langle a, b \rangle \} \in T$ , где  $a$  — некоторый элемент из  $X$  ( $X \neq \emptyset$ ) и  $b \in f(a)$  ( $f(x) \neq \emptyset$ ). Множество  $T$  частично упорядочено отношением включения  $\subseteq$ . Покажем, что множество  $T$  с отношением включения  $\subseteq$  удовлетворяет условию **Леммы Цорна**.

Пусть  $A$  — линейно упорядоченное подмножество множества  $T$ , т.е. для любых  $x$  и  $y$  из  $A$  или  $x \subseteq y$ , или  $y \subseteq x$ . Полагаем  $z = \bigcup_{x \in A} x$ . Очевидно, что для любого  $x$  из  $A$ :  $x \subseteq z$ . Чтобы доказать, что  $z$  — верхняя грань  $A$  в  $T$ , остается лишь доказать, что  $z \in T$ .

Так как для любого  $v$  из  $A$   $v \subseteq X \times \bigcup_{x \in X} f(x)$ , то  $z \subseteq X \times \bigcup_{x \in X} f(x)$ . Покажем, что  $z$  — функционально.

Пусть  $\langle a, b \rangle \in z$  и  $\langle a, c \rangle \in z$ . В  $A$  найдутся такие два множества  $x$  и  $y$ , что  $\langle a, b \rangle \in x$ ,  $\langle a, c \rangle \in y$ . Так как  $A$  линейно упорядочено, то либо  $x \subseteq y$ , либо  $y \subseteq x$ . Достаточно рассмотреть лишь случай  $x \subseteq y$ . В этом случае  $\langle a, b \rangle \in y$  и  $\langle a, c \rangle \in y$ , что в силу функциональности  $y$  дает  $b = c$ , т.е.  $z$  функционально.

Пусть  $a \in \delta(z)$ . Найдется такое  $u$ , что  $\langle a, u \rangle \in z$ . Значит, в  $A$  существует такое  $x$ , что  $\langle a, u \rangle \in x$ . Поэтому  $a \in \delta(x)$ , а значит,  $x(a) \in f(a)$ . Но  $x(a)$  — это  $u$ , значит,  $u \in f(a)$ . С другой стороны,  $u$  — это  $z(a)$ , значит,  $z(a) \in f(a)$ .



Таким образом, все условия Леммы Цорна выполнены, значит,  $T$  содержит максимальный элемент  $\varphi$ .

Покажем, что  $\varphi$  можно взять в качестве функции выбора (заметим, что функция  $\varphi$  определена, конечно, неоднозначно, так как  $T$  может содержать более одного максимального элемента).

Так как  $\varphi \in T$ , то  $\varphi$  — функционально и для любого  $x$  из  $\delta(\varphi)$ :  $\varphi(x) \in f(x)$ . Остается показать, что  $\delta(\varphi) = X$ .

Если бы это было не так, то существовал бы элемент  $a \in X \setminus \delta(\varphi)$ . Пусть  $b \in f(a)$  и  $g = \varphi \cup \{\langle a, b \rangle\}$ .

Покажем, что  $g \in T$ .

$\varphi \subseteq X \times \bigcup_{x \in X} f(x)$  и  $\langle a, b \rangle \in X \times \bigcup_{x \in X} f(x)$ , значит,  $g \subseteq X \times \bigcup_{x \in X} f(x)$ .

Проверим, что  $g$  функционально. Если  $\langle x, y \rangle \in g$ ,  $\langle x, z \rangle \in g$ , то либо (1)  $\langle x, y \rangle \in \varphi$ ,  $\langle x, z \rangle \in \varphi$ , либо (2)  $\langle x, y \rangle \in \{\langle a, b \rangle\}$ ,  $\langle x, z \rangle \in \{\langle a, b \rangle\}$  (случай  $\langle x, y \rangle \in \varphi$  и  $\langle x, z \rangle \in \{\langle a, b \rangle\}$  невозможен, так как тогда из второго условия следует, что  $\langle x, y \rangle = \langle a, b \rangle$ , т.е.  $x = a$ ,  $y = b$ , а из первого условия получаем  $x \in \delta(\varphi)$ , т.е.  $a \in \delta(\varphi)$ , что противоречит выбору  $a$ ).

В случае (1) из функциональности  $\varphi$  следует, что  $y = z$ .

В случае (2) получаем  $y = b = z$ .

Если  $x \in \delta(\varphi)$ , то найдется элемент  $y = \varphi(x)$  такой, что  $\langle x, y \rangle \in \varphi \subseteq g$ . Если же  $\langle x, y \rangle \in \{\langle a, b \rangle\}$ , то  $x = a$  и  $y = b$ . Поэтому  $g(x) = y = \varphi(x) \in f(x)$ . Значит,  $g \in T$ . Однако это вместе с условиями  $\varphi \subset g$  и  $\varphi \neq g$  противоречит максимальной  $\varphi$ . Поэтому  $\delta(\varphi) = X$ .

(1)  $\implies$  (4).

Пусть  $\mathcal{X}$  — произвольное множество непустых попарно непересекающихся множеств. Используя существование функций выбора, покажем, что существует такое множество  $B$ , что для любого множества  $A$  из  $\mathcal{X}$  множество  $A \cap B$  состоит ровно из одного элемента.

Рассмотрим множество  $f = \{\langle a, a \rangle \mid a \in X\}$ , задающее тождественное отображение множества  $X$  на себя. Так как при любом  $x$  из  $X$   $f(x)$  — непустое множество, то по аксиоме выбора существует функция выбора  $g : X \rightarrow \bigcup_{x \in X} f(x)$ . Обозначим через  $B$   $g(X) = \{g(x) \mid x \in X\}$ . Покажем, что  $B$  — требуемое множество. Пусть  $A \in \mathcal{X}$ . Тогда  $g(A) \in f(A) = A$ , т.е.  $g(A) \in A \cap B$ . Если, кроме того,  $c \in A \cap B$ , то найдется множество  $C \in \mathcal{X}$  такое, что  $g(C) = c$ , поэтому  $c = g(C) \in f(C) = C$ , значит,  $c \in A \cap C$ . Но множества из  $\mathcal{X}$  попарно не пересекаются, значит,  $A = C$  и  $c = g(C) = g(A)$ . Значит, пересечение  $A \cap B$  состоит из единственного элемента  $g(A)$ .

(4)  $\implies$  (1).

Пусть  $f$  — отображение множества  $X$  во множество  $Y$  и при любом  $x \in X$   $f(x)$  — непустое множество. Пользуясь Аксиомой Цермело, покажем, что существует функция выбора  $g$ , определенная на множестве  $X$  со значениями во множестве  $\bigcup_{x \in X} f(x)$  такая, что для любого  $x$  из  $X$   $g(x) \in f(x)$ .

Рассмотрим множество  $U = \{\{x\} \times f(x) \mid x \in X\}$ . Элементами множества  $U$  служат непустые множества  $\{x\} \times f(x)$ . Покажем, что они попарно не пересекаются. Если  $\langle a, b \rangle \in (\{x\} \times f(x)) \cap (\{y\} \times f(y))$ , то  $x = a = y$ , поэтому  $\{x\} \times f(x) = \{y\} \times f(y)$ . Пусть  $B$  — множество, имеющее ровно по одному общему элементу с каждым множеством из  $U$ , существующее в соответствии с Аксиомой Цермело.

Покажем, что в качестве функции выбора  $g$  можно взять множество  $B$ . Заметим, что

$$B = B \cap \bigcup_{x \in X} (\{x\} \times f(x)) = \{\langle x, y \rangle \mid x \in X \text{ \& } \langle x, y \rangle \in B \cap (\{x\} \times f(x))\}.$$

Если  $\langle x, y \rangle \in g$  и  $\langle x, z \rangle \in g$ , то  $\langle x, y \rangle \in B \cap (\{x\} \times f(x))$  и  $\langle x, z \rangle \in B \cap (\{x\} \times f(x))$ . Отсюда по выбору множества  $B$  получаем  $\langle x, y \rangle = \langle x, z \rangle$ , значит,  $y = z$ . Итак  $g$  — функция. Если  $x \in X$  и  $y = g(x)$ , то  $\langle x, y \rangle \in B \cap (\{x\} \times f(x))$ , поэтому  $\langle x, y \rangle \in \{x\} \times f(x)$  и  $g(x) = y \in f(x)$ .

(1)  $\implies$  (5).

Пользуясь аксиомой выбора, покажем, что *каждое множество можно вполне упорядочить*. Именно для доказательства этого факта Цермело и использовал в явном виде аксиому выбора. По утверждению Френкеля, Бар-Хиллела и Леви первая явная ссылка на аксиому выбора была сделана Пеано в работе по дифференциальным уравнениям. Однако до этого Кантор уже применял неявно аксиому выбора.

Пусть  $M$  — произвольное множество,  $f$  — тождественная функция на множестве  $X = P(M) \setminus \{\emptyset\}$  всех непустых подмножеств множества  $M$ . Через  $g$  обозначим *функцию выбора*, соответствующую отображению  $f$ . Рассмотрим следующее семейство  $S$  непустых подмножеств множества  $M$ :

$$S = \{A \mid A \subset M \text{ \& } A \neq \emptyset \text{ \& }$$

А можно вполне упорядочить так, что для любого

$$a \in A : \quad g(M \setminus A_a) = a\}.$$

Семейство  $S$  непусто, так как  $\{g(M)\} \in S$  (заметим, что в этом случае, если  $a \in A = \{g(M)\}$ , то  $a = g(M)$  и  $A_a = \emptyset$ , поэтому  $g(M \setminus A_a) = g(M) = a$ ).

Покажем, что для любых двух множеств  $A$  и  $B$  из  $S$  одно из них является началом другого. Для этого заметим, что множество  $\{g(M)\}$  является началом и для  $A$ , и для  $B$ . В самом деле, пусть  $a$  и  $b$  — наименьшие элементы в  $A$  и в  $B$  соответственно, тогда  $A_a = \emptyset = B_b$ , значит,  $a = g(M \setminus A_a) = g(M) = g(M \setminus B_b) = b$ , т.е.  $a = b = g(M)$ , значит,  $g(M)$  — наименьший элемент в любом множестве  $A$  из  $S$ , поэтому  $\{g(M)\}$  — общее начало для  $A$  и  $B$ . Пусть  $C$  — общее начало для  $A$  и  $B$ . Ясно, что  $C \neq \emptyset$ . Покажем, что объединение любого множества  $D$  начал любого упорядоченного множества  $E$  является началом  $E$ . Пусть  $x \in \bigcup_{u \in D} u$ ,  $y \in E$  и  $y < x$ , тогда найдется  $z \in D$  такое, что  $x \in z$ . Но  $z$  — начало  $E$ , поэтому  $y \in z$ , а значит,  $y \in \bigcup_{u \in D} u$ . Поэтому  $C$  — общее начало для  $A$  и  $B$ . По теореме 8.2 возможен один из следующих четырех случаев:

- (1)  $C = A, C = B$ . В этом случае  $A = B$ .
- (2)  $C = A, C = B_b$  для некоторого  $b \in B$ . В этом случае  $A$  — начало  $B$ .
- (3)  $C = B, C = A_a$  для некоторого  $a \in A$ . В этом случае  $B$  — начало  $A$ .
- (4)  $C = A_a, C = B_b$  для некоторых  $a \in A, b \in B$ .

Остается показать, что случай (4) невозможен. В самом деле, в случае (4)  $a = g(M \setminus A_a) = g(M \setminus C) = g(M \setminus B_b) = b$ , т.е.  $C = A_a, C = B_a$ , но ясно, что  $C \cup \{a\}$  — общее начало для  $A$  и  $B$ , но  $C$  — объединение всех общих начал для  $A$  и  $B$ , поэтому  $C \cup \{a\} \subseteq C$ . Значит,  $a \in C = A_a$ , что невозможно.

Пусть  $L = \bigcup_{A \in S} A$ . Покажем, что  $L \in S$ . В самом деле, очевидно, что  $L \subseteq M, L \neq \emptyset$  ( $g(M) \in L$ ). Определим на  $L$  отношение  $<$  следующим образом: если  $x, y \in L$ , то найдутся множества  $A, B \in S$  такие, что  $x \in A, y \in B$ . Так как либо  $A = B$ , либо одно из них является отрезком другого, поэтому либо  $x, y \in A$ , либо  $x, y \in B$ .

Без ограничения общности считаем, что  $x, y \in A$ . Полагаем  $x < y$  тогда и только тогда, когда  $x <_A y$ . Если кроме того,  $x, y \in C$ , то так как либо  $A = C$ , либо одно из них является отрезком другого, получаем  $x <_A y$  тогда и только тогда, когда  $x <_C y$ . Поэтому отношение  $<$  определено корректно. Легко проверить, что отношение  $<$  вполне упорядочивает  $L$ . Проверим, например, что любое непустое подмножество  $K$  множества  $L$  имеет наименьший элемент. Так как  $K \neq \emptyset$ , то найдется элемент  $c \in K \subseteq L$ . Но тогда для некоторого  $A$  из  $S$   $c \in A$ . Значит,  $A \cap K \neq \emptyset$ . Пусть  $d$  — наименьший элемент в  $A \cap K$  относительно порядка  $<$  (или, что то же самое, относительно порядка  $<_A$ ). Покажем, что  $d$  — наименьший элемент и в  $K$ . Если бы это было не так, то в  $K$  нашелся бы элемент  $b$  такой, что  $b < d$ . Пусть  $b, d \in B \in S$ , тогда  $b <_B d$ . По ранее доказанному либо  $A = B$ , либо  $A$  — отрезок  $B$ , либо  $B$  — отрезок  $A$ . В первых двух случаях из того, что  $d \in A$  и  $b <_B d$  следует, что  $b \in A \cap K$  и  $b <_A d$ , что противоречит минимальности элемента  $d$  в  $A \cap K$ .

В третьем случае из того, что  $d \in A$  и  $b <_B d$  следует, что  $b \in A \cap K$  и  $b <_A d$ , что вновь противоречит минимальности элемента  $d$  в  $A \cap K$ .

Итак,  $L \in S$ . Значит,  $L$  можно вполне упорядочить.

Покажем, что  $L = M$ . Если это не так, то рассмотрим множество  $A = L \cup \{g(M \setminus L)\}$  и введем на  $A$  отношение порядка  $<:$  если  $x, y \in L$ , то  $x < y \iff x < y$  в  $L$ , если же  $x \in L, y \in \{g(M \setminus L)\}$ , то  $x < y$ .

Покажем, что  $A \in S$ . Заметим, что  $A \subseteq M$ . Далее, легко проверить, что введенное отношение  $<$  является отношением полного порядка. Кроме того, если  $a \in L$ , то  $A_a = L_a$  и  $g(M \setminus A_a) = g(M \setminus L_a) = a$ , а если  $a \in \{g(M \setminus L)\}$ , то  $A_a = L$  и  $g(M \setminus A_a) = g(M \setminus L) = a$ . Итак,  $A \in S$ . Но это невозможно, так как тогда  $A \subseteq L \subset A$ . Полученное противоречие доказывает, что  $L = M$ . Значит,  $M$  можно вполне упорядочить.

(5)  $\implies$  (3).

Покажем, что из теоремы Цермело о вполне упорядочиваемости любого множества следует **принцип максимальности Куратовского – Хаусдорфа**:

каждая цепь частично упорядоченного множества содержится в некоторой максимальной цепи.

Допустим, что множество  $M$  частично упорядочено отношением  $\leq$ , а  $L$  — цепь в  $M$ , т.е. подмножество множества  $M$  линейно упорядоченное отношением  $\leq$ .

Если  $L = M$ , то цепь  $L$  максимальна, т.е. не содержится ни в какой отличной от нее цепи.

Если  $L \neq M$ , то вполне упорядочим множество  $A = M \setminus L$  отношением  $\prec$ .

Теперь каждому элементу  $a$  из  $A$  сопоставим следующим образом некоторое множество  $L_a$ , которое является расширением относительно  $\leq$  цепи  $L$ . Если для любого элемента  $b \prec a$  множество  $L_b$  уже определено, то полагаем  $L_a$  равным  $\bigcup_{b \prec a} L_b \cup \{a\}$ , если  $a$  сравним по  $\leq$  со всеми элементами из  $\bigcup_{b \prec a} L_b$ , и равным  $\bigcup_{b \prec a} L_b$  в противном случае.

Проверим, что  $\bigcup_{a \in A} L_a$  является максимальной цепью, содержащей  $L$ .

Из построения множеств  $L_a$  следует, что  $L \subseteq L_a$  и если  $b \prec a$ , то  $L_b \subseteq L_a$ . Значит,  $L \subseteq \bigcup_{a \in A} L_a$ .

Если  $c, b \in \bigcup_{a \in A} L_a$ , то

либо (1)  $c, b \in L$  и, значит,  $c$  сравнимо с  $b$  по  $\leq$ ,

либо (2)  $c \in L, b \notin L$ , но тогда  $L_b = \bigcup_{a \prec b} L_a \cup \{b\}$  (иначе  $b \notin \bigcup_{a \in A} L_a$ ) и поэтому  $b$  сравним по  $\leq$  со всеми элементами из  $\bigcup_{a \prec b} L_a$ , в частности, с  $c$ ,

либо (3)  $c \notin L, b \notin L$ . Пусть в этом случае  $c \prec b$ . Тогда  $L_b = \bigcup_{a \prec b} L_a \cup \{b\}$  и  $b$  сравним по  $\leq$  со всеми элементами из  $\bigcup_{a \prec b} L_a$  и  $c \in \bigcup_{a \prec b} L_a$  (иначе  $c \notin \bigcup_{a \in A} L_a$ ), значит, в частности,  $b$  сравним по  $\leq$  с  $c$ .

Итак,  $\bigcup_{a \in A} L_a$  — цепь. Если бы цепь  $\bigcup_{a \in A} L_a$  не была максимальной, то нашелся бы элемент  $b$  такой, что  $b \notin \bigcup_{a \in A} L_a$  и  $b$  сравним по  $\leq$  со всеми элементами из  $\bigcup_{a \in A} L_a$ . Но в этом случае  $b \notin L$ , значит,  $b \in A = M \setminus L$  и  $b$  сравним по  $\leq$  со всеми элементами из  $\bigcup_{a \in A} L_a$  ( $\bigcup_{a \prec b} L_a \subseteq \bigcup_{a \in A} L_a$ ), поэтому  $L_b = \bigcup_{a \prec b} L_a \cup \{b\}$  и, значит,  $b \in \bigcup_{a \in A} L_a$ , что противоречит предположению  $b \notin \bigcup_{a \in A} L_a$ .

Итак,  $\bigcup_{a \in A} L_a$  — максимальная цепь, содержащая цепь  $L$ .

(3)  $\implies$  (2).

Покажем, что из принципа максимальности Куратовского — Хаусдорфа (каждая цепь частично упорядоченного множества содержится в некоторой максимальной цепи) следует **лемма Цорна**: частично упорядоченное множество, каждое из линейно упорядоченных подмножеств которого имеет верхнюю грань, содержит максимальный элемент.

Пусть частично упорядоченное отношением  $\leq$  множество  $M$  удовлетворяет условию леммы Цорна, т.е. каждое из его линейно упорядоченных подмножеств

имеет верхнюю грань. Возьмем в  $M$  произвольный элемент  $b$ . В силу принципа максимальности Куратовского – Хаусдорфа множество  $\{b\}$ , будучи цепью, содержится в некоторой максимальной цепи  $L$ , которая имеет в  $M$  верхнюю грань  $c$  (заметим, что  $c \in L$ , так как в противном случае цепь  $L$  содержалась бы в отличной от нее цепи  $L \cup \{c\}$ , что противоречит ее максимальнойности). Покажем, что  $c$  — *максимальный* элемент в  $M$ . Допустим, что это не так. Тогда в  $M$  найдется элемент  $a$  такой, что  $c < a$ . Покажем, что  $a$  сравним с любым элементом  $d$  цепи  $L$ . Это следует из неравенств  $d \leq c$  ( $c$  — верхняя грань цепи  $L$  в  $M$ ),  $c < a$ ,  $d < a$ . Так как  $L$  — цепь, то  $L \cup \{a\}$  — тоже цепь, но это противоречит максимальнойности цепи  $L$ .

Значит,  $c$  — *максимальный* элемент в  $M$ .

(2)  $\implies$  (6).

Покажем, что из леммы Цорна можно вывести **лемму Тейхмюллера – Тьюки**: *каждое семейство подмножеств  $X$  множества  $E$ , имеющее конечный характер, обладает максимальным элементом.*

Пусть семейство подмножеств  $X$  множества  $E$  имеет конечный характер. Множество  $X$  частично упорядочено отношением  $\subseteq$ . Покажем, что для него выполнено условие леммы Цорна. Пусть  $L$  — любая цепь в  $X$ . Покажем, что множество  $A \triangleq \bigcup_{y \in L} y$  является *верхней гранью* для  $L$  в  $X$ .

Во-первых, если  $y \in L$ , то  $y \subseteq A$ .

Во-вторых, покажем, что  $A \in X$ . Пусть  $C$  — конечное подмножество множества  $A$ , состоящее из элементов  $c_1, \dots, c_n$ . В  $L$  найдутся такие элементы  $y_1, \dots, y_n$ , что  $c_1 \in y_1, \dots, c_n \in y_n$ . Так как  $L$  — цепь, то можно считать, что  $y_1 \subseteq y_2 \subseteq \dots \subseteq y_n$ . Поэтому  $c_1 \in y_n, \dots, c_n \in y_n$ , т.е.  $C \subseteq y_n$ . Так как  $y_n \in X$ , а  $C$  — конечное подмножество  $y_n$ , то  $C \in X$ . Значит, каждое конечное подмножество множества  $A$  принадлежит  $X$ , поэтому и  $A \in X$ .

Итак  $A$  — *верхняя грань* цепи  $L$  в  $X$ . По лемме Цорна в  $X$  есть *максимальный* элемент.

(6)  $\implies$  (2).

Допустим, что множество  $E$  удовлетворяет условию леммы Цорна: т.е. *каждое из его линейно упорядоченных подмножеств имеет верхнюю грань*. Покажем, что  $E$  содержит *максимальный* элемент.

Обозначим через  $X$  множество всех цепей множества  $E$ . Покажем, что множество  $X$  имеет *конечный характер*.

Если  $A \in X$ , т.е.  $A$  является цепью в  $E$ , то и любое подмножество множества  $A$  является цепью, а значит, принадлежит  $X$ , в частности, это верно для конечных подмножеств множества  $A$ .

Пусть теперь  $A \subseteq E$  и каждое его конечное подмножество  $B$  принадлежит  $X$ , т.е. является цепью. Покажем, что и  $A$  принадлежит  $X$ , т.е. является цепью. Пусть  $x$  и  $y$  — произвольные элементы множества  $A$ , тогда подмножество  $\{x, y\}$  множества  $A$  принадлежит  $X$ , т.е. является цепью. Значит,  $x$  и  $y$



сравнимы. Так как сравнимы любые два элемента множества  $A$ , то  $A$  — цепь, значит,  $A \in X$ .

Итак, множество  $X$  имеет *конечный характер*. По лемме Тейхмюллера — Тьюки в  $X$  есть *максимальный* элемент  $A$ , т.е.  $A$  — *максимальная* цепь. По условию леммы Цорна найдется *верхняя грань*  $c$  для  $A$  в  $E$ .

Покажем, что  $c$  — *максимальный* элемент. Если это не так, то в  $E$  найдется такой элемент  $b$ , что  $c < b$ . А так как  $c$  больше любого элемента из  $A$ , то это верно и для  $b$ . Значит, множество  $A \cup \{b\}$  является цепью, что противоречит максимальной цепи  $A$ .

$$(1) \implies (8).$$

Пусть  $(A_i)_{i \in I}$  — непустое семейство непустых множеств,  $f$  — функция, определенная на  $I$  такая, что  $f(i) = A_i$ . По *аксиоме выбора* существует *функция выбора*  $g$ , определенная на  $I$ , такая, что при любом  $i \in I$ :  $g(i) \in f(i) = A_i$ . Но тогда  $g \in \prod_{i \in I} A_i$ , значит,  $\prod_{i \in I} A_i \neq \emptyset$ .

$$(8) \implies (1).$$

Пусть функция  $f$  удовлетворяет условию аксиомы выбора. Рассмотрим семейство  $(f(x))_{x \in X}$  множеств. По *аксиоме мультипликативности* существует функция  $g \in \prod_{x \in X} f(x)$ . Но тогда  $g$  — одна из *функций выбора*.

$$(4) \implies (7).$$

Пусть  $f$  — отображение множества  $A$  на непустое множество  $B$ . Для каждого  $y \in B$  обозначим через  $W_y$  множество  $\{y\} \times \{x \mid x \in A \text{ \& } f(x) = y\}$ . Ясно, что непустые множества  $W_y$  попарно не пересекаются. По *аксиоме Цермело* существует множество  $D$ , имеющее с каждым из множеств  $W_y$  в точности по одному общему элементу. Пусть  $g = D = (\bigcup_{y \in B} W_y) \cap D$ . Покажем, что  $g$  — *функция* из  $B$  в  $A$ .

Ясно, что  $\delta(g) \subseteq B$ . Если  $z \in B$ , то пусть  $v_z$  — такой элемент, что  $\langle z, v_z \rangle \in W_z \cap D$ . Тогда  $\langle z, v_z \rangle \in g$ , поэтому  $z \in \delta(g)$ , значит,  $\delta(g) = B$ .

Если  $\langle x, y \rangle \in g$  и  $\langle x, z \rangle \in g$ , то найдутся такие элементы  $u$  и  $v$ , что  $\langle x, y \rangle \in W_u$  и  $\langle x, z \rangle \in W_v$ . Но тогда  $u = x$  и  $v = y$ . Значит,  $\langle x, y \rangle \in W_x$  и  $\langle x, z \rangle \in W_x$ . Так как, кроме того,  $\langle x, y \rangle \in D$  и  $\langle x, z \rangle \in D$ , то  $\langle x, y \rangle = \langle x, z \rangle$ , значит,  $y = z$ . Т.е.  $g$  — *функция* из  $B$  в  $A$ .

Покажем, что  $f \circ g = i_B$ . Если  $\langle x, y \rangle \in f \circ g$ , то найдется элемент  $z$  такой, что  $\langle x, z \rangle \in g$ ,  $\langle z, y \rangle \in f$ . Но тогда  $\langle x, z \rangle \in W_x \cap D$ , значит,  $f(z) = x$ . Кроме того, из  $\langle z, y \rangle \in f$  следует, что  $f(z) = y$ . Поэтому  $x = y$ . Значит,  $f \circ g = i_B$ .

Заметим, что функция  $g$  является *инъекцией*, так как

$$\begin{aligned} g(y_1) = g(y_2) &\implies f(g(y_1)) = f(g(y_2)) \implies \\ &(f \circ g)(y_1) = (f \circ g)(y_2) \implies i_B(y_1) = i_B(y_2) \implies y_1 = y_2. \end{aligned}$$



Поэтому (7) можно сформулировать так: для любого множества  $A$  и любой определенной на нем функции  $f$  выполняется неравенство

$$\overline{f(A)} \leq \overline{A}.$$

(7)  $\implies$  (4).

Пусть множество  $X$  состоит из непустых попарно непересекающихся множеств. Рассмотрим множество  $f = \{\langle a, b \rangle \mid b \in X \text{ и } a \in b\}$ . Ясно, что  $f$  — функция, отображающая  $\bigcup_{x \in X} x$  на  $X$ .

В силу (7) существует инъективное отображение  $g: X \rightarrow \bigcup_{x \in X} x$  такое, что  $i_X = f \circ g$ . Пусть  $B = \rho(g)$ .

Покажем, что множество  $B$  имеет с каждым множеством  $A$  из  $X$  единственный общий элемент.

Пусть  $x \in X$ , тогда  $g(x) \in \rho(g)$  и  $x = f(g(x))$ , т.е.  $\langle g(x), x \rangle \in f$ , поэтому  $g(x) \in x \cap B$ . Значит,  $x \cap B \neq \emptyset$ .

Пусть теперь  $y \in x \cap B$ . Тогда  $y \in \rho(g)$ . Значит, найдется  $z \in X$  такой, что  $y = g(z)$ . Тогда, как было показано выше,  $y = g(z) \in z \cap B$ . Поэтому  $y \in x \cap z$ . Но тогда  $x = z$  и  $y = g(x)$ .  $\square$

**Теорема 8.6.** Для произвольных мощностей  $\alpha$  и  $\beta$  выполняется одно и только одно из условий

$$(1) \quad \alpha = \beta, \quad (2) \quad \alpha < \beta, \quad (3) \quad \beta < \alpha.$$

*Доказательство.* Напомним, что

$$\alpha < \beta \iff \alpha \leq \beta \text{ и } \alpha \neq \beta.$$

Значит, (1) несовместно ни с (2), ни с (3).

(2) и (3) тоже несовместны, так как из них следует, что  $\alpha \leq \beta$ ,  $\beta \leq \alpha$  и  $\alpha \neq \beta$ , однако по теореме Кантора – Бернштейна из неравенств  $\alpha \leq \beta$  и  $\beta \leq \alpha$  следует равенство  $\alpha = \beta$ .

Чтобы доказать, что по крайней мере один из этих случаев имеет место, воспользуемся теоремой Цермело. Пусть  $X$  и  $Y$  — такие множества, что  $\alpha = \overline{X}$ ,  $\beta = \overline{Y}$ . По теореме Цермело множества  $X$  и  $Y$  можно вполне упорядочить. Пусть  $\leq_X$  и  $\leq_Y$  — соответствующие отношения полного порядка.

В силу пункта 3) теоремы имеет место один из следующих двух случаев:

$$(1) \quad \overline{X} \leq \overline{Y}, \quad (2) \quad \overline{Y} \leq \overline{X}.$$

Но тогда

$$\text{либо (1) } \overline{\overline{X}} \leq \overline{\overline{Y}}, \quad \text{либо (2) } \overline{\overline{Y}} \leq \overline{\overline{X}},$$

т.е. либо  $\alpha \leq \beta$ , либо  $\beta \leq \alpha$ . Значит, имеет место одна из возможностей

$$(1) \quad \alpha = \beta, \quad (2) \quad \alpha < \beta, \quad (3) \quad \beta < \alpha.$$

□

**Следствие.** Кардинальные числа линейно упорядочены отношением  $<$  (и отношением  $\leq$ ).

Для произвольного порядкового числа  $\alpha$  через  $W(\alpha)$  обозначим множество всех порядковых чисел, меньших  $\alpha$ .

**Теорема 8.7.** Для любого порядкового числа  $\alpha$  множество  $W(\alpha)$  — вполне упорядоченное множество порядкового типа  $\alpha$ .

*Доказательство.* Пусть  $A$  — вполне упорядоченное множество порядкового типа  $\alpha$ . Тогда  $A$  изоморфно множеству  $W(A) = \{A_a \mid a \in A\}$ , упорядоченному отношением включения  $\subseteq$ . В свою очередь множество  $\{\overline{A_a} \mid a \in A\}$ , упорядоченное отношением включения, изоморфно множеству  $\{\overline{A_a} \mid a \in A\}$ . В самом деле, если  $A_a$  и  $A_b$  — различные отрезки, то они не могут быть подобны, значит,  $\overline{A_a} \neq \overline{A_b}$ .

Если же  $A_a \subset A_b$ , то  $A_a = (A_b)_a$ , значит,  $\overline{A_a} < \overline{A_b}$ .

Покажем, что  $\{\overline{A_a} \mid a \in A\} = W(\alpha)$ . Если  $a \in A$ , то  $\overline{A_a} < \overline{A} = \alpha$ , поэтому  $\overline{A_a} \in W(\alpha)$ . Если же  $\beta \in W(\alpha)$ , то  $\beta < \alpha$ . Пусть  $B$  — вполне упорядоченное множество типа  $\beta$ . Тогда найдется отрезок  $A_a$  подобный  $B$ , значит,  $\beta = \overline{B} = \overline{A_a}$ .  $\beta \in \{\overline{A_a} \mid a \in A\}$ . Поэтому  $W(\alpha) = \alpha$ . □

**Следствие 1.** Всякое множество ординальных чисел вполне упорядочено.

*Доказательство.* Пусть  $A$  — произвольное множество ординальных чисел,  $B$  — его непустое подмножество. Пусть  $\alpha \in B$ . Если  $W(\alpha) \cap B = \emptyset$ , то  $\alpha$  — наименьший элемент в  $B$ . Если же  $W(\alpha) \cap B \neq \emptyset$ , то пусть  $\beta$  — наименьший элемент подмножества  $W(\alpha) \cap B$  множества  $W(\alpha)$ . Тогда  $\beta$  будет и наименьшим элементом подмножества  $B$  множества  $A$ . □

**Следствие 2.** Для любого множества  $A$  порядковых чисел существует порядковое число, большее всех чисел из  $A$ .

*Доказательство.* Множество  $A$  само вполне упорядочено и в качестве искомого числа можно взять порядковый тип  $\overline{B}$  множества  $B = \bigcup_{\alpha \in A} W(\alpha)$ . В самом деле, множество  $B$ , будучи множеством порядковых чисел, само вполне упорядочено. Пусть  $\beta = \overline{B}$ . Если  $\alpha \in A$ , то  $\overline{W(\alpha)} = \alpha$  и  $B_\alpha = W(\alpha)$ . Так как вполне упорядоченное множество  $B$  не может быть подобно своему отрезку  $B_\alpha$ , то  $\beta = \overline{B} > \overline{B_\alpha} = \overline{W(\alpha)} = \alpha$ . □

**Следствие 3.** Не существует множества, содержащего все порядковые числа.

*Д о к а з а т е л ь с т в о.* Сразу следует из предыдущего следствия.  $\square$

**Следствие 4.** Среди порядковых чисел, не принадлежащих данному множеству  $A$  порядковых чисел, есть наименьшее.

*Д о к а з а т е л ь с т в о.* Пусть  $\alpha$  — порядковое число большее всех чисел из  $A$ , а  $\beta$  — наименьшее в  $W(\alpha) \cup \{\alpha\}$  число из  $(W(\alpha) \cup \{\alpha\}) \setminus A$ , тогда  $\beta$  — искомое число.  $\square$

**Определение 8.10.** Для порядкового числа  $\alpha$  наименьшее порядковое число  $\beta$ , не принадлежащее  $W(\alpha) \cup \{\alpha\}$ , называется **непосредственно следующим** за  $\alpha$  и обозначается через  $\alpha'$ .

Покажем, что  $\alpha' = \alpha + 1$ . В самом деле, во-первых,  $\alpha < \alpha + 1$ . Во-вторых, если  $\alpha < \beta$ , то  $W(\alpha) \subset W(\beta)$ , поэтому  $W(\alpha) \cup \{\alpha\} \subseteq W(\beta)$ . Значит, либо  $W(\alpha) \cup \{\alpha\} = W(\beta)$ , либо  $W(\alpha) \cup \{\alpha\}$  является начальным отрезком  $W(\beta)$ , поэтому  $\alpha = \overline{W(\alpha) \cup \{\alpha\}} \leq \overline{W(\beta)}$ , т.е.  $\alpha + 1 \leq \beta$ .

**Следствие 5.** Всякое множество кардинальных чисел вполне упорядочено.

*Д о к а з а т е л ь с т в о.* Пусть  $X$  — произвольное множество кардинальных чисел. Для каждого  $y \in X$  выберем множество  $Y$  такое, что  $\overline{Y} = y$ . По теореме Цермело множество  $Y$  можно вполне упорядочить. Обозначим  $\overline{Y}$  через  $\alpha_y$ . Пусть  $V = \{\alpha_y \mid y \in X\}$ . Рассмотрим отображение  $f : y \mapsto \alpha_y$  множества  $X$  на множество  $V$ . Если  $y, z \in X$ ,  $y \neq z$ ,  $\overline{Y} = y$ ,  $\overline{Z} = z$ , то по теореме 8.6 либо  $\overline{Y} < \overline{Z}$ , либо  $\overline{Z} < \overline{Y}$ . Если  $\overline{Y} < \overline{Z}$ , то невозможно, чтобы  $\overline{Z} \leq \overline{Y}$ , так как иначе  $\overline{Z} \leq \overline{Y}$ , значит,  $\overline{Y} \leq \overline{Z}$ . Поэтому  $f$  — монотонная биекция  $X$  на  $V$ . Так как любое множество ординальных чисел вполне упорядочено, то и множество  $V$  ординальных чисел вполне упорядочено, значит, вполне упорядоченно и  $X$ .  $\square$

**Следствие 6.** Для любого кардинального числа  $n$  существует непосредственно следующее за ним кардинальное число  $n^+$ , т.е. такое кардинальное число  $n^+$ , что

$$(1) \ n < n^+,$$

$$(2) \text{ если } m \text{ — кардинальное число и } n < m, \text{ то } n^+ \leq m.$$

*Д о к а з а т е л ь с т в о.* Пусть  $n^+$  — наименьшее число из множества  $\{\alpha \mid \alpha \text{ — кардинальное число, } n < \alpha \leq 2^n\}$ . Очевидно, что  $n^+$  — непосредственно следующее за  $n$  кардинальное число.  $\square$

**Замечание.** Формула  $2^{\aleph_0} = \aleph_0^+$  выражает знаменитую континуум-гипотезу Г. Кантора.

**Принцип минимальности для ординальных чисел.** Если  $Q$  — произвольное свойство ординальных чисел, которое выполняется хотя бы для одного

ординального числа, то существует *наименьшее* ординальное число, обладающее свойством  $Q$ .

Пусть для ординального числа  $\alpha$  выполняется свойство  $Q$ , тогда в качестве искомого наименьшего ординального числа можно взять наименьшее ординальное число в множестве

$$\{\gamma \mid \gamma \text{ — ординальное число из } W(\alpha) \cup \{\alpha\}, \text{ обладающее свойством } Q\}.$$

**Принцип трансфинитной индукции для ординальных чисел.** Пусть  $Q$  — такое свойство ординальных чисел, что для любого ординального числа  $\alpha$  из того, что все ординальные числа  $\beta < \alpha$  обладают свойством  $Q$ , следует, что и  $\alpha$  обладает свойством  $Q$ . Тогда все ординальные числа обладают свойством  $Q$ .

*Доказательство.* Предположим противное, и пусть  $\beta$  — одно из ординальных, не обладающих свойством  $Q$ . Пусть  $\alpha$  — наименьшее ординальное число из  $W(\beta) \cup \{\beta\}$ , не обладающее свойством  $Q$  (любое множество ординальных чисел вполне упорядочено). Тогда все ординальные числа из  $W(\alpha)$  обладают свойством  $Q$ , а значит, этим свойством обладает и  $\alpha$ . Что противоречит выбору  $\alpha$ .  $\square$

В заключение установим ряд фактов арифметики бесконечных кардинальных чисел, существенно отличающих ее от арифметики натуральных чисел (конечных кардинальных чисел). При этом будет показано, как при установлении свойств кардинальных чисел (мощностей множеств) приходится использовать свойства ординальных чисел (порядковых типов вполне упорядоченных множеств).

**Теорема 8.8.** Для произвольного бесконечного кардинального числа  $n$  выполняются равенства

- 1)  $n + n = n$ ,
- 2)  $n \cdot k = n$ , где  $k$  — конечное ненулевое кардинальное число,
- 3)  $n \cdot \aleph_0 = n$ .

*Доказательство.* Покажем, что найдется такое кардинальное число  $n_0$ , что  $n = \aleph_0 \cdot n_0$ .

Пусть  $n = \overline{A}$ . Вполне упорядочим множество  $A$  некоторым отношением  $<_A$  полного порядка. Введем на множестве  $\mathbb{N} \times A$  отношение  $<$ :

$$\langle n, a \rangle < \langle m, b \rangle \iff (a <_A b) \vee (a = b \ \& \ n < m).$$

Нетрудно проверить, что отношение  $<$  вполне упорядочивает множество  $\mathbb{N} \times A$ .

Множество  $A$  подобно подмножеству

$$\{1\} \times A = \{\langle 1, a \rangle \mid a \in A\}$$

множества  $\mathbb{N} \times A$ . Поэтому из следствия теоремы 8.3 получаем, что множество  $\mathbb{N} \times A$  не может быть подобно начальному отрезку множества  $A$ . Значит, множество  $A$  подобно либо множеству  $\mathbb{N} \times A$ , либо некоторому его начальному отрезку  $(\mathbb{N} \times A)_{\langle n_0, a_0 \rangle}$ . В первом случае получаем

$$\overline{A} = \overline{\mathbb{N} \times A}.$$

Значит,  $n \cdot \aleph_0 = n$ . Во втором случае

$$\overline{A} = \overline{(\mathbb{N} \times A)_{\langle n_0, a_0 \rangle}}.$$

Так как

$$(\mathbb{N} \times A)_{\langle n_0, a_0 \rangle} = (\mathbb{N} \times A_{a_0}) \cup (\mathbb{N}_{n_0} \times \{a_0\})$$

и  $\mathbb{N}_{n_0} \times \{a_0\}$  — конечное множество, то  $n = \aleph_0 \cdot n_0$ , где  $n = \overline{A_{a_0}}$ .

Равенство 1) следует из следующих равенств

$$n + n = \aleph_0 \cdot n_0 + \aleph_0 \cdot n_0 = (\aleph_0 + \aleph_0) \cdot n_0 = \aleph_0 \cdot n_0 = n.$$

Равенство 2) следует из следующих равенств

$$n \cdot k = (\aleph_0 \cdot n_0) \cdot k = (\aleph_0 \cdot k) \cdot n_0 = \aleph_0 \cdot n_0 = n.$$

Равенство 3)  $n \cdot \aleph_0 = n$  получаем из следующих равенств

$$\aleph_0 \cdot n = \aleph_0 \cdot \aleph_0 \cdot n_0 = \aleph_0 \cdot n_0 = n.$$

□

Следующая теорема следует из леммы Цорна и даже на самом деле ей эквивалентна.

**Теорема 8.9.** Для произвольного бесконечного кардинального числа  $n$  выполняется равенство  $n \cdot n = n$ .

*До к а з а т е л ь с т в о.* Для произвольного множества  $A$  такого, что  $\overline{A} = n$ , полагаем

$$M(A) = \{f \mid f \text{ — биективное отображение множества } B \times B \text{ на } B \\ \text{ для некоторого бесконечного подмножества } B \text{ множества } A\}.$$

Так как любое бесконечное множество  $A$  содержит счетное подмножество  $B$  и в таком случае  $\overline{B \times B} = \overline{B}$ , то множество  $M(A)$  непусто. Множество  $M(A)$  частично упорядочено отношением включения  $\subseteq$  и нетрудно проверить выполнение условия леммы Цорна. Значит, по лемме Цорна в множестве  $M(A)$  есть максимальный элемент  $g : C \times C \rightarrow C$ .

Пусть  $m = \overline{C}$ . Заметим, что  $\overline{C \times C} = \overline{C}$ , поэтому  $m \cdot m = m$ , т.е.  $m^2 = m$ .

Ясно, что  $m \leq n$ . Если  $m = n$ , то теорема доказана.

Предположим  $m < n$ .

Покажем, что выполнено неравенство  $\overline{A \setminus C} > m$ .

Предположим противное  $\overline{A \setminus C} \leq m$ .

Тогда в силу предыдущей теоремы

$$n = \overline{A} = \overline{C \cup (A \setminus C)} = \overline{C} + \overline{A \setminus C} \leq m + m = m,$$

что противоречит сделанному выше предположению  $m < n$ .

Пусть  $C_1$  — подмножество мощности  $m$  множества  $A \setminus C$ .

Для получения противоречия рассмотрим множество  $D \doteq C \cup C_1$ . Тогда

$$D \times D = (C \times C) \cup (C \times C_1) \cup (C_1 \times C) \cup (C_1 \times C_1).$$

Пусть

$$E \doteq (C \times C_1) \cup (C_1 \times C) \cup (C_1 \times C_1).$$

Тогда  $\overline{E} = m^2 + m^2 + m^2 = m + m + m = m$ . Поэтому существует биективное отображение  $h$  множества  $E$  на множество  $C_1$ .

Полагаем  $f \doteq g \cup h$ . Тогда

$$f : (C \cup C_1) \times (C \cup C_1) \rightarrow (C \cup C_1),$$

но это противоречит предположению о том, что отображение  $g : C \times C \rightarrow C$  является максимальным элементом во множестве  $M(A)$ . Полученное противоречие завершает доказательство теоремы.  $\square$

**Следствие.** Для произвольных бесконечных кардинальных чисел  $n$  и  $m$  выполняются равенства

$$1) \ n + m = \max\{n, m\},$$

$$2) \ n \cdot m = \max\{n, m\}.$$

*Доказательство.* В силу теоремы 8.6 можно считать,  $n \leq m$ , а значит,  $\max\{n, m\} = m$ .

Равенства 1) и 2) получаются из неравенств

$$m \leq n + m \leq m + m = m$$

$$m \leq n \cdot m \leq m \cdot m = m$$

на основании теоремы Кантора – Шредера – Бернштейна  $\square$

В качестве еще одного приложения аксиомы и теоремы Цермело, а значит, и эквивалентных им утверждений, рассмотрим вопрос о существовании базисов в векторных пространствах.



**Определение 8.11.** Множество векторов  $\mathcal{E}$  векторного пространства  $V$  над полем  $K$  называется **базисом** этого пространства, если любой вектор из  $V$  однозначно представим в виде линейной комбинации конечного множества векторов из  $\mathcal{E}$ .

**Теорема 8.10.** В любом векторном пространстве  $V$  над произвольным полем  $K$  существует базис.

*До к а з а т е л ь с т в о.* Напомним, что произвольная система  $S$  векторов векторного пространства называется **линейно независимой**, если линейно независимой является любая **конечная** подсистема системы  $S$ .

Обозначим через  $\mathcal{X}$  семейство всех *линейно независимых* систем векторов векторного пространства  $V$ .

Из определения линейно независимых систем векторов сразу следует, что семейство подмножеств  $\mathcal{X}$  множества  $V$  имеет *конечный характер*. Поэтому по лемме Тейхмюллера – Тьюки семейство подмножеств  $\mathcal{X}$  обладает *максимальным элементом*, т.е. в  $V$  существует *максимальная*  $\mathcal{E}$  относительно отношения включения  $\subseteq$  линейно независимая система векторов.

Покажем, что  $\mathcal{E}$  — базис векторного пространства  $V$ .

Если некоторый вектор  $v$  не представлялся бы в виде линейной комбинации векторов из  $\mathcal{E}$ , то легко убедиться, что система векторов  $\mathcal{E} \cup \{v\}$  была бы линейно независима. Что противоречило бы максимальной системе  $\mathcal{E}$ .

Однозначность представления векторов в виде линейных комбинаций векторов из системы  $\mathcal{E}$  легко следует из линейной независимости системы векторов  $\mathcal{E}$ .  $\square$

**Замечание.** Можно доказать, что любые два базиса произвольного векторного пространства  $V$  равномощны.

В качестве весьма нетривиального следствия доказанной теоремы получим ответ на следующий интересный вопрос. Очевидно, что для линейной функции  $f(x) = ax$  выполняется тождество  $f(x + u) = f(x) + f(u)$ . Можно ли привести пример нелинейной функции  $f$ , определенной на всем множестве действительных чисел и удовлетворяющей тождеству  $f(x + u) = f(x) + f(u)$ ?

Ответ оказывается положительным, но “явный” пример такой функции не известен, однако мы сейчас покажем, что такие функции существуют.

Рассмотрим множество  $\mathbb{R}$  действительных чисел как векторное пространство над полем  $\mathbb{Q}$  рациональных чисел.

В силу вышесказанного в  $\mathbb{R}$  найдется базис  $\mathcal{E}$  над  $\mathbb{Q}$ . Зафиксируем некоторый вектор  $e$  в базисе  $\mathcal{E}$ . Для произвольного  $x \in \mathbb{R}$  через  $f(x)$  обозначим коэффициент при базисном векторе  $e$  в разложении вектора  $x$  по базису  $\mathcal{E}$ . Ясно, что для функции  $f(x)$  выполняется тождество  $f(x + u) = f(x) + f(u)$ . Однако эта функция не является линейной функцией вида  $f(x) = ax$ , так как она принимает только рациональные значения.

В качестве еще одного классического применения аксиомы выбора рассмотрим теорему Х. Хана – С. Банаха о продолжении линейных функционалов.

Пусть  $L$  — линейное пространство над полем действительных чисел  $R$ . Любое отображение из  $L$  в  $R$  называется *функционалом* на  $L$ . Функционал  $f$  называется *линейным*, если для любых двух чисел  $\alpha$  и  $\beta$  из  $R$  и любых двух векторов  $v$  и  $u$  из  $L$  выполняется равенство  $f(\alpha v + \beta u) = \alpha f(v) + \beta f(u)$ .

Это условие равносильно двум условиям

- 1) *аддитивность*: для любых двух векторов  $v$  и  $u$  из  $L$  выполняется равенство  $f(v + u) = f(v) + f(u)$ ,
- 2) *однородность*: для любого числа  $\alpha$  из  $R$  и вектора  $v$  из  $L$  выполняется равенство  $f(\alpha v) = \alpha f(v)$ .

Функционал  $p$  называется *однородно выпуклым*, если для него выполняются следующие два условия

- 1) *полуаддитивность*: для любых двух векторов  $v$  и  $u$  из  $L$  выполняется неравенство  $p(v + u) \leq p(v) + p(u)$ ,
- 2) *полуоднородность*: для любого неотрицательного действительного числа  $\alpha$  и любого вектора  $v$  из  $L$  выполняется равенство  $p(\alpha v) = \alpha p(v)$ .

**Теорема 8.11.** Пусть на линейном пространстве  $L$  над полем действительных чисел задан однородно выпуклый функционал  $p$ , а на подпространстве  $U$  задан линейный функционал  $f$ , причем для любого вектора  $v$  из подпространства  $U$  выполняется неравенство  $f(v) \leq p(v)$ . Тогда существует линейный функционал  $F$ , определенный на всем пространстве  $L$ , являющийся продолжением линейного функционала  $f$ , причем для любого вектора  $v$  пространства  $L$  выполняется неравенство  $F(v) \leq p(v)$ .

*Доказательство.* Пусть  $w \in L \setminus U$ . Обозначим через  $U(w)$  линейное подпространство, полученное присоединением вектора  $w$  к  $U$ , т.е.  $U(w)$  состоит из всевозможных векторов вида  $v + tw$ , где  $t$  — произвольное действительное число. Для произвольного фиксированного действительного числа  $c$  равенство  $f_c(v + tw) = f(v) + tc$  определяет продолжение линейного функционала  $f$  с подпространства  $U$  на подпространство  $U(w)$ . Остается подобрать такое число  $c$ , чтобы при любом  $t$  выполнялось неравенство  $f_c(v + tw) \leq p(v + tw)$ , т.е.  $f(v) + tc \leq p(v + tw)$ . При  $t = 0$  неравенство, конечно, выполнено. При  $t > 0$  оно равносильно неравенству  $f(v/t) + c \leq p(v/t + w)$ , а при  $t < 0$  — неравенству  $f(-v/t) - c \leq p(-v/t - w)$ . Таким образом, достаточно доказать существование числа  $c$ , удовлетворяющего при любых положительных  $t$  и  $t'$  неравенствам

$$f(v/t') - p(v/t' - w) \leq c \leq p(v/t + w) - f(v/t).$$

А это будет верно, если мы установим, что при любых  $v'$  и  $v''$  из  $L$  выполняется неравенство

$$f(v') - p(v' - w) \leq p(v'' + w) - f(v'').$$

Последнее неравенство доказывается следующим образом: при любых  $v'$  и  $v''$  из  $L$

$$\begin{aligned} f(v') + f(v'') &= f(v' + v'') \leq p(v' + v'') = \\ &= p(v' - w + v'' + w) \leq p(v' - w) + p(v'' + w). \end{aligned}$$

Значит,

$$\sup_{v' \in L} \{f(v') - p(v' - w)\} \leq \inf_{v'' \in L} \{p(v'' + w) - f(v'')\}.$$

Рассмотрим частично упорядоченное отношением  $\leq$  множество  $\Phi$ , элементами которого являются всевозможные пары  $\langle W, F_W \rangle$ , где  $W$  — подпространство пространства  $L$ , содержащее  $U$ , а  $F_W$  — такое линейное продолжение функционала  $f$  с  $U$  на  $W$ , что при любом  $w$  из  $W$  выполняется неравенство  $F_W(w) \leq p(w)$ . При этом считаем, что  $\langle W, F_W \rangle \leq \langle W_1, F_{W_1} \rangle$  тогда и только тогда, когда  $W \subseteq W_1$  и  $F_{W_1}$  — продолжение функционала  $F_W$ . Нетрудно проверить, что отношение  $\leq$  является отношением частичного порядка, т.е. оно рефлексивно, транзитивно и антисимметрично и для него выполнено условие леммы Цорна — для каждого линейно упорядоченного подмножества  $\Sigma$  множества  $\Phi$  существует верхняя грань: если  $\Sigma = \{\langle W_i, F_{W_i} \rangle \mid i \in I\}$ , то полагаем  $W = \cup_{i \in I} W_i$ ,  $F_W = \cup_{i \in I} F_{W_i}$ . Тогда пара  $\langle W, F_W \rangle$  принадлежит  $\Phi$  и является верхней гранью для  $\Sigma$ . По лемме Цорна в  $\Phi$  имеется максимальный элемент  $\langle \bar{W}, F_{\bar{W}} \rangle$ . Остается показать, что  $\bar{W} = L$ . В противном случае берем  $w \in L \setminus \bar{W}$  и описанным выше способом строим продолжение  $F_{\bar{W}(w)}$  функционала  $F_{\bar{W}}$  на  $\bar{W}(w)$ . Тогда пара  $\langle \bar{W}(w), F_{\bar{W}(w)} \rangle$  принадлежит  $\Phi$  и  $\langle \bar{W}, F_{\bar{W}} \rangle < \langle \bar{W}(w), F_{\bar{W}(w)} \rangle$ , что противоречит максимальнойности  $\langle \bar{W}, F_{\bar{W}} \rangle$ .  $\square$

В заключение параграфа приведем пример просто формулируемой задачи Улама из теории множеств, попытки решения которой наталкиваются на непреодолимые на сегодняшний день трудности.

*Можно ли привести пример непустого множества  $\mathcal{X}$  и функции  $\mu$ , определенной на множестве  $P(\mathcal{X})$  всех его подмножеств и принимающей лишь два значения 0 и 1, такой, что значение функции  $\mu$  на каждом одноэлементном подмножестве множества  $\mathcal{X}$  равно нулю,  $\mu(\mathcal{X}) = 1$  и для любого счетного множества  $(A_n)_{n \in \mathbb{N}}$  попарно непересекающихся подмножеств множества  $\mathcal{X}$  выполняется равенство*

$$\mu\left(\bigcup_{n \in \mathbb{N}} A_n\right) = \sum_{n=1}^{+\infty} \mu(A_n)?$$

Каждая такая функция называется счетно-аддитивной двузначной мерой на множестве всех подмножеств множества  $\mathcal{X}$ .

Заметим, что если в число требований не включать условие равенства нулю значения функции  $\mu$  на каждом одноэлементном подмножестве, то пример такой функции легко привести: для произвольного множества  $\mathcal{X}$  и фиксированного в нем элемента  $a$  полагаем

$$\text{если } A \subseteq \mathcal{X}, \text{ то } \mu(A) = 1 \iff a \in A.$$

Такие функции называются  $\delta$ -мерами.

Ясно, что множество  $\mathcal{X}$  не может быть конечным или счетным. Более глубокое изучение этого вопроса показывает, что если такое множество существует, то его мощность “очень большая”. Однако вопрос о существовании такого множества  $\mathcal{X}$ , так же как и попытки решения континуум-гипотезы, неизбежно приводит нас к необходимости точной формулировки аксиом теории множеств, что в свою очередь ведет к необходимости построения соответствующего формального языка первого порядка, однако это не входит в цели настоящего пособия и составляет предмет отдельного разговора.

## 9. Натуральные числа. Системы Пеано

Выше было показано, как, отправляясь от системы натуральных чисел

$$\langle \mathbb{N}, 1, +, \cdot \rangle,$$

можно построить все остальные числовые системы — целые, рациональные, действительные и комплексные числа. При этом мы рассматривали натуральные числа, как данные нам. Т.е. в определенной мере поступали в соответствии с высказыванием Л. Кронекера: “Натуральные числа создал господь Бог, а все остальное — дело человеческих рук”.

В этом параграфе будут рассмотрены два подхода для определения множества натуральных чисел: аксиоматический и генетический. Первый из них основан на предложенной Дж. Пеано в 1889 году системе аксиом для арифметики натуральных чисел, сходную систему аксиом для натуральных чисел независимо предложил в 1888 году Р. Дедекин. Второй подход основан на предложенном Джоном фон Нейманом определении натуральных чисел в рамках теории множеств.

### 9.1. Системы Пеано

**Определение 9.1.** *Системой Пеано называется*

$$\langle P, s, c \rangle,$$

где  $P$  — непустое множество,  $s : P \rightarrow P$  — одноместная функция на множестве  $P$ , называемая функцией следования, а  $c$  — выделенный элемент в  $P$ , при условии выполнения следующих аксиом, называемых аксиомами Пеано:

- I) для любого  $a \in P$  выполняется неравенство  $c \neq s(a)$ ;
- II)  $s$  — инъективная функция, т.е. для любых  $a, b \in P$  из равенства  $s(a) = s(b)$  следует равенство  $a = b$ ;
- III) аксиома индукции: пусть  $B \subseteq P$  — произвольное подмножество множества  $P$  такое, что  $c \in B$ , и для любого элемента  $a \in P$ : если  $a \in B$ , то  $s(a) \in B$ , тогда  $B = P$ .

**Замечание.** Каждое подмножество  $B$  множества  $P$  такое, что  $c \in B$ , и для любого элемента  $a \in P$ : если  $a \in B$ , то  $s(a) \in B$ , будем называть индуктивным.

Вопрос о существовании систем Пеано мы обсудим позже. А сейчас рассмотрим вопрос об однозначности характеристики систем Пеано указанными аксиомами.

**Определение 9.2.** Системы Пеано

$$\langle P, s, c \rangle \quad \text{и} \quad \langle P', s', c' \rangle$$

называются изоморфными, если существует биективное отображение  $f : P \rightarrow P'$  такое, что  $f(c) = c'$  и для любого  $x$  из  $P$  выполняется равенство  $f(s(x)) = s'(f(x))$ .

**Теорема 9.1.** Любые две системы Пеано изоморфны.

*Доказательство.* Докажем, что существует биективное отображение  $f : P \rightarrow P'$  такое, что  $f(c) = c'$  и для любого  $x$  из  $P$  выполняется равенство  $f(s(x)) = s'(f(x))$ .

Заметим, что если такая функция  $f$  существует, то она в соответствии с данным выше определением понятия функции является подмножеством  $U$  множества  $P \times P'$  и удовлетворяет следующим двум условиям:

- I)  $\langle c, c' \rangle \in U$ ,  
и для любых  $a$  и  $b$ :
- II) если  $\langle a, b \rangle \in U$ , то  $\langle s(a), s'(b) \rangle \in U$ .

Обозначим через  $W$  множество всех подмножеств  $U$  множества  $P \times P'$ , удовлетворяющих условиям I) и II). Ясно, что  $W \neq \emptyset$ , так как, например,  $P \times P' \in W$ .

Полагаем

$$f = \bigcap_{U \in W} U.$$

Легко видеть, что  $f$  является подмножеством множества  $P \times P'$  и удовлетворяет условиям I) и II), т.е.  $f \in W$ .

Значит,  $f$  — соответствие с областью определения  $\delta(f) \subseteq P$  и множеством значений  $\rho(f) \subseteq P'$ .

Покажем, что  $f$  — функция с областью определения  $\delta(f) = P$  и множеством значений  $\rho(f) \subseteq P'$ , удовлетворяющая условиям

- 1)  $f(c) = c'$ ,
- 2)  $f(s(a)) = s'(f(a))$ .

Обозначим через  $B$  множество  $\delta(f)$ , т.е.

$$B = \{a \mid a \in P \text{ \& } (\exists b)(b \in P') \text{ \& } \langle a, b \rangle \in f\}.$$



Из условия I) следует, что  $c \in B$ . Условие II) дает: если  $a \in B$ , то  $s(a) \in P'$ .

Значит,  $B$  — индуктивное множество, поэтому по третьей аксиоме Пеано  $B = P$ , т.е.  $\delta(f) = P$ .

Проверим, что для  $f$  выполняется свойство функциональности, т.е.

$$(\forall y)(\forall z_1)(\forall z_2)((\langle y, z_1 \rangle \in f \ \& \ \langle y, z_2 \rangle \in f) \rightarrow z_1 = z_2).$$

Обозначим через  $Q$  множество

$$\{a \mid (\forall z_1)(\forall z_2)((\langle a, z_1 \rangle \in f \ \& \ \langle a, z_2 \rangle \in f) \rightarrow z_1 = z_2)\}.$$

Покажем, что  $Q$  — индуктивное множество.

Докажем, что  $c \in Q$ . Так как  $\langle c, c' \rangle \in U$ , то необходимо показать, что для любого  $z$ , если  $\langle c, z \rangle \in f$ , то  $z = c'$ . Предположим противное, т.е. что существует такое  $e$ , что  $\langle c, e \rangle \in f$ , но  $e \neq c'$ .

Рассмотрим множество  $U = f \setminus \{\langle c, e \rangle\}$ .

Так как  $e \neq c'$ , то  $\langle c, c' \rangle \in U$ , т.е. для множества  $U$  выполнено условие I).

Проверим выполнимость для множества  $U$  условия II). Если  $\langle a, b \rangle \in U$ , то  $\langle a, b \rangle \in f$ , тогда  $\langle s(a), s'(b) \rangle \in f$ . Так как  $s'(b) \neq c'$ , то  $\langle s(a), s(b) \rangle \in U$ .

Значит, для построенного множества  $U$  выполнены условия I) и II), поэтому  $f \subseteq U = f \setminus \{\langle c, e \rangle\}$ . Полученное противоречие показывает, что  $c \in Q$ .

Покажем, что если  $a \in Q$ , то  $s(a) \in Q$ .

Установим, что если  $\langle s(a), e \rangle \in f$ , то найдется такой элемент  $b$ , что  $\langle a, b \rangle \in f$  и  $e = s'(b)$ .

Предположим противное, т.е. что существует элемент  $e$  такой, что  $\langle s(a), e \rangle \in f$ , но нет такого элемента  $b$ , что  $\langle a, b \rangle \in f$  и  $e = s'(b)$ .

Рассмотрим множество  $U = f \setminus \{\langle s(a), e \rangle\}$ .

Проверим выполнимость для множества  $U$  условий I) и II).

Так как  $s(a) \neq c$ , то  $\langle c, c' \rangle \in U$ , т.е. для множества  $U$  выполнено условие I).

Проверим выполнимость для множества  $U$  условия II). Пусть  $\langle d, l \rangle \in U$ , тогда  $\langle d, l \rangle \in f$ , значит,  $\langle s(d), s'(l) \rangle \in f$ .

Если  $d \neq a$ , то по второй аксиоме Пеано  $s(d) \neq s(a)$ , поэтому  $\langle s(d), s'(l) \rangle \notin \{\langle s(a), e \rangle\}$ . Значит,  $\langle s(d), s'(l) \rangle \in U$ . Если  $d = a$ , то  $\langle a, b \rangle \in f$ . Тогда  $\langle s(a), s'(b) \rangle \in f$ .

Так как нет такого элемента  $b$ , что  $\langle a, b \rangle \in f$  и  $e = s'(b)$ , то  $e \neq s'(b)$ .

Поэтому  $\langle s(a), s'(b) \rangle \in U$ .

Значит, для построенного множества  $U$  выполнены условия I) и II), поэтому  $f \subseteq U = f \setminus \{\langle s(a), e \rangle\}$ .

Полученное противоречие показывает, что если  $\langle s(a), e \rangle \in f$ , то найдется такой элемент  $b$ , что  $\langle a, b \rangle \in f$  и  $e = s'(b)$ .

Пусть  $a \in Q$ . Чтобы доказать, что  $s(a) \in Q$ , предположим, что  $\langle s(a), e_1 \rangle \in f \ \& \ \langle s(a), e_2 \rangle \in f$ .

Тогда найдутся такие элементы  $b_i$  ( $i = 1, 2$ ), что  $\langle a, b_i \rangle \in f$  и  $e_i = s'(b_i)$ .

Так как  $a \in Q$ , то  $b_1 = b_2$ , значит,  $e_1 = e_2$ . Поэтому  $s(a) \in Q$ .



Значит,  $Q$  — индуктивное множество, поэтому по третьей аксиоме Пеано  $Q = P$ .

Значит,  $f$  — функция.

Тем самым доказано существование функции  $f$  такой, что  $\delta(f) = P$ ,  $\rho(f) \subseteq P'$ ,

$$1) f(c) = c'$$

и для любого  $a \in P$  выполняется равенство

$$2) f(s(a)) = s'(f(a)).$$

Остается доказать,  $f$  — биективное отображение, т.е. что  $\rho(f) = P'$  и  $f$  — инъекция.

Покажем, что  $\rho(f)$  — индуктивное подмножество множества  $P'$ .

$$1) c' = f(c) \in \rho(f)$$

2) Если  $b \in \rho(f)$ , то  $b = f(a)$  для некоторого  $a$  из  $P$ . Но тогда  $s'(b) = s'(f(a)) = f(s(a)) \in \rho(f)$ .

Значит,  $\rho(f) = P'$ .

Чтобы доказать, что  $f$  — инъекция, обозначим через  $B$  следующее подмножество множества  $P'$

$$B = \{b \mid (\forall u)(\forall v)(b = f(u) \ \& \ b = f(v)) \implies u = v\}.$$

Покажем, что  $B$  — индуктивное подмножество множества  $P'$ .

Сначала установим полезный для дальнейшего факт: для любого элемента  $a$  отличного от  $c$  элемента из  $P$  найдется такой элемент  $e$ , что  $a = s(e)$ . Это сразу следует из индуктивности множества

$$\{c\} \cup \{s(e) \mid e \in A\}.$$

Заметим, что из аксиомы 2) следует, что для любого элемента  $a$  отличного от  $c$  соответствующий элемент  $e$  определен однозначно.

Покажем, что  $c' \in B$ .  $c' = f(c)$ . Если кроме того,  $c' = f(a) \ \& \ a \neq c$ , то найдется  $e$  такой, что  $a = s(e)$ , но тогда  $c' = f(a) = f(s(e)) = s'(f(e))$ , что противоречит аксиоме 1).

Пусть  $b \in B$ . Если  $s'(b) = f(u)$  и  $s'(b) = f(v)$ , то  $u \neq c$  и  $v \neq c$ . Значит,  $u = s(x)$  и  $v = s(y)$ , тогда  $s'(b) = s'(f(x))$  и  $s'(b) = s'(f(y))$ . По аксиоме 2)  $b = f(x)$  и  $b = f(y)$ . Так как  $b \in B$ , то  $x = y$ . Значит,  $s(b) \in B$ . Поэтому  $B$  — индуктивное подмножество множества  $P'$ . Значит,  $B = P'$ , поэтому  $f$  — инъекция.

Итак,  $f$  — изоморфизм систем Пеано  $P$  и  $P'$ .

Можно доказать, что условиями 1) и 2) функция  $f$  определена однозначно.

В самом деле, предположим, что существуют функции  $f_1$  и  $f_2$  такие, что  $\delta(f_i) = P$ ,  $\rho(f_i) \subseteq P'$  и

$$1) f_i(c) = c',$$

и для любого  $a \in P$  выполняется равенство

$$2) f_i(s(a)) = s'(f_i(a)) \quad i = 1, 2.$$

Обозначим через  $B$  множество

$$\{a \mid f_1(a) = f_2(a)\}.$$

Так как  $f_1(c) = c' = f_2(c)$ , то  $c \in B$ .

Если  $a \in B$ , то  $f_1(a) = f_2(a)$ , значит,  $f_1(s(a)) = s'(f_1(a)) = s'(f_2(a)) = f_2(s(a))$ . Следовательно,  $s(a) \in B$ .

Значит,  $B$  — индуктивное множество, поэтому по третьей аксиоме Пеано  $B = P$ . Поэтому  $f_1 = f_2$ .  $\square$

Рассмотрим вопрос о существовании систем Пеано.

**Определение 9.3.** Для произвольного множества  $U$  полагаем  $U' \Leftarrow U \cup \{U\}$ . Множество  $U'$  называется **последователем** множества  $U$ .

**Определение 9.4.** Множество  $S$  назовем **индуктивным**, если его элементом является пустое множество  $\emptyset$  и вместе с каждым элементом  $a$  —  $a'$  также является элементом этого множества.

Следующее утверждение принимаем в качестве еще одной из аксиом теории множеств.

**Аксиома бесконечности.** Существует индуктивное множество  $S$ .

**Определение 9.5.** Множеством **натуральных чисел**  $\mathbb{N}$  называется пересечение всех индуктивных подмножеств множества  $S$ .

Множество натуральных чисел  $\mathbb{N}$  обладает следующими тремя важными свойствами:

- 1)  $\emptyset \in \mathbb{N}$ ;
- 2) если  $a \in \mathbb{N}$ , то  $a' \in \mathbb{N}$ ;
- 3) для любого подмножества  $L$  множества  $\mathbb{N}$  такого, что  $\emptyset \in L$  и если  $a \in L$ , то  $a' \in L$ , выполняется равенство  $L = \mathbb{N}$ .

**Замечание 1.** Свойства 1) и 2) означают, что  $\mathbb{N}$  — индуктивное множество, а в силу свойства 3)  $\mathbb{N}$  не имеет собственных индуктивных подмножеств, т.е. любое индуктивное подмножество множества  $\mathbb{N}$  совпадает со всем этим множеством.

**Замечание 2.** Рассмотренный способ определения понятия натурального числа через понятие множества принадлежит Джону фон Нейману:

$$0 = \emptyset, \quad n' = n \cup \{n\}.$$

Готтлоб Фреге в 1884 г. предложил другое определение натуральных чисел:

0 — это класс  $\{\emptyset\}$ ,

1 — это класс всех множеств, которые становятся пустыми при удалении из них одного элемента,

$n'$  — это класс всех множеств, которые попадают в класс  $n$  при удалении из них одного элемента.

## 9.2. Рекурсивные определения в системах Пеано

**Теорема 9.2.** Для любых двух функций  $g$  и  $h$  таких, что  $\delta(g) = \mathbb{N}^n$ ,  $\rho(g) \subseteq \mathbb{N}$ ,  $\delta(h) = \mathbb{N}^{n+2}$  и  $\rho(h) \subseteq \mathbb{N}$  существует единственная функция  $f$  такая, что  $\delta(f) = \mathbb{N}^{n+1}$ ,  $\rho(f) \subseteq \mathbb{N}$  и для любых  $a_1, \dots, a_n, b \in \mathbb{N}$  выполняются следующие равенства

$$1) f(a_1, \dots, a_n, 1) = g(a_1, \dots, a_n),$$

$$2) f(a_1, \dots, a_n, s(b)) = h(a_1, \dots, a_n, b, f(a_1, \dots, a_n, b)).$$

**Замечание.** Про функцию  $f$  говорят, что она получается с помощью примитивной рекурсии из функций  $g$  и  $h$  и пишут  $f = PR(g; h)$ .

*Д о к а з а т е л ь с т в о.* Начнем с доказательства существования функции  $f$ . Заметим, что если такая функция существует, то она в соответствии с данным выше определением понятия функции является подмножеством  $U$  множества  $\mathbb{N}^{n+1} \times \mathbb{N}$  и для любых  $a_1, \dots, a_n, b, c \in \mathbb{N}$  удовлетворяет следующим двум условиям

$$I) \langle \langle a_1, \dots, a_n, 1 \rangle, g(a_1, \dots, a_n) \rangle \in U,$$

$$II) \text{ если } \langle \langle a_1, \dots, a_n, b \rangle, c \rangle \in U, \text{ то } \langle \langle a_1, \dots, a_n, s(b) \rangle, h(a_1, \dots, a_n, b, c) \rangle \in U.$$

Обозначим через  $W$  множество всех подмножеств  $U$  множества  $\mathbb{N}^{n+1} \times \mathbb{N}$ , удовлетворяющих условиям I) и II). Ясно, что  $W \neq \emptyset$ , так как, например,  $\mathbb{N}^{n+1} \times \mathbb{N} \in W$ .

Полагаем

$$f = \bigcap_{U \in W} U.$$

Легко видеть, что  $f$  является подмножеством множества  $\mathbb{N}^{n+1} \times \mathbb{N}$  и удовлетворяет условиям I) и II), т.е.  $f \in W$ .

Значит,  $f$  — соответствие с областью определения  $\delta(f) \subseteq \mathbb{N}^{n+1}$  и множеством значений  $\rho(f) \subseteq \mathbb{N}$ .

Покажем, что  $f$  — функция с областью определения  $\delta(f) = \mathbb{N}^{n+1}$  и множеством значений  $\rho(f) \subseteq \mathbb{N}$ , удовлетворяющая условиям

- 1)  $f(a_1, \dots, a_n, 1) = g(a_1, \dots, a_n)$ ,
- 2)  $f(a_1, \dots, a_n, s(b)) = h(a_1, \dots, a_n, b, f(a_1, \dots, a_n, b))$ .

Для сокращения обозначаем набор  $a_1, \dots, a_n$  через  $\bar{a}$ .

Для произвольного фиксированного набора  $\langle a_1, \dots, a_n \rangle$  обозначим через  $P_{\bar{a}}$  множество

$$\{b \mid b \in \mathbb{N} \ \& \ (\exists c)(c \in \mathbb{N} \ \& \ \langle \langle a_1, \dots, a_n, b \rangle, c \rangle \in f)\}$$

Из условия I) следует, что  $1 \in P_{\bar{a}}$ . Условие II) дает: если  $b \in P_{\bar{a}}$ , то  $s(b) \in P_{\bar{a}}$ .

Значит,  $P_{\bar{a}}$  — индуктивное множество, поэтому по третьей аксиоме Пеано  $P_{\bar{a}} = \mathbb{N}$ . Т.е. для любого набора  $\langle a_1, \dots, a_n, b \rangle$   $\langle a_1, \dots, a_n, b \rangle \in \delta(f)$ , поэтому  $\delta(f) = \mathbb{N}^{n+1}$ .

Проверим, что для  $f$  выполняется свойство функциональности, т.е.

$$(\forall x_1) \dots (\forall x_n) (\forall y) (\forall z_1) (\forall z_2) ((\langle \langle x_1, \dots, x_n, y \rangle, z_1 \rangle \in f \ \& \ \langle \langle x_1, \dots, x_n, y \rangle, z_2 \rangle \in f) \rightarrow z_1 = z_2).$$

Для произвольного фиксированного набора  $\langle a_1, \dots, a_n \rangle$  обозначим через  $Q_{\bar{a}}$  множество

$$\{b \mid (\forall z_1) (\forall z_2) ((\langle \langle a_1, \dots, a_n, b \rangle, z_1 \rangle \in f \ \& \ \langle \langle a_1, \dots, a_n, b \rangle, z_2 \rangle \in f) \rightarrow z_1 = z_2)\}.$$

Покажем, что  $Q_{\bar{a}}$  — индуктивное множество.

Докажем, что  $1 \in Q_{\bar{a}}$ . Так как  $\langle \langle a_1, \dots, a_n, 1 \rangle, g(a_1, \dots, a_n) \rangle \in U$ , то необходимо показать, что для любого  $z$ , если  $\langle \langle a_1, \dots, a_n, 1 \rangle, z \rangle \in f$ , то  $z = g(a_1, \dots, a_n)$ . Предположим противное, т.е. что существует такое  $e$ , что  $\langle \langle a_1, \dots, a_n, 1 \rangle, e \rangle \in f$ , но  $z \neq g(a_1, \dots, a_n)$ .

Рассмотрим множество  $U = f \setminus \{\langle \langle a_1, \dots, a_n, 1 \rangle, e \rangle\}$ .

Так как  $c \neq g(a_1, \dots, a_n)$ , то  $\langle \langle a_1, \dots, a_n, 1 \rangle, g(a_1, \dots, a_n) \rangle \in U$ , т.е. для множества  $U$  выполнено условие I).

Проверим выполнимость для множества  $U$  условия II).

Если  $\langle \langle a_1, \dots, a_n, b \rangle, c \rangle \in U$ , то  $\langle \langle a_1, \dots, a_n, b \rangle, c \rangle \in f$ , тогда

$$\langle \langle a_1, \dots, a_n, s(b) \rangle, h(a_1, \dots, a_n, b, c) \rangle \in f.$$

Так как  $s(b) \neq 1$ , то  $\langle \langle a_1, \dots, a_n, s(b) \rangle, h(a_1, \dots, a_n, b, c) \rangle \in U$ .

Значит, для построенного множества  $U$  выполнены условия I) и II), поэтому  $f \subseteq U = f \setminus \{\langle \langle a_1, \dots, a_n, 1 \rangle, e \rangle\}$ . Полученное противоречие показывает, что  $1 \in Q_{\bar{a}}$ .

Покажем, что если  $b \in Q_{\bar{a}}$ , то  $s(b) \in Q_{\bar{a}}$ .

Установим, что если  $\langle \langle a_1, \dots, a_n, s(b) \rangle, e \rangle \in f$ , то найдется такой элемент  $c$ , что  $\langle \langle a_1, \dots, a_n, b \rangle, c \rangle \in f$  и  $e = h(a_1, \dots, a_n, b, c)$ .

Предположим противное, т.е. что существует элемент  $e$  такой, что  $\langle \langle a_1, \dots, a_n, s(b) \rangle, e \rangle \in f$ , но нет такого элемента  $c$ , что  $\langle \langle a_1, \dots, a_n, b \rangle, c \rangle \in f$  и  $e = h(a_1, \dots, a_n, b, c)$ .

Рассмотрим множество  $U = f \setminus \{\langle \langle a_1, \dots, a_n, s(b), \rangle, e \rangle\}$ .

Проверим выполнимость для множества  $U$  условий I) и II).

Так как  $s(b) \neq 1$ , то  $\langle \langle a_1, \dots, a_n, 1 \rangle, g(a_1, \dots, a_n) \rangle \in U$ , т.е. для множества  $U$  выполнено условие I).

Проверим выполнимость для множества  $U$  условия II).

Пусть  $\langle \langle a_1, \dots, a_n, d \rangle, c \rangle \in U$ , тогда  $\langle \langle a_1, \dots, a_n, d \rangle, c \rangle \in f$ , значит,

$$\langle \langle a_1, \dots, a_n, s(d) \rangle, h(a_1, \dots, a_n, d, c) \rangle \in f.$$

Если  $d \neq b$ , то по второй аксиоме Пеано  $s(d) \neq s(b)$ , поэтому  $\langle \langle a_1, \dots, a_n, s(d) \rangle, h(a_1, \dots, a_n, d, c) \rangle \notin \{\langle \langle a_1, \dots, a_n, s(b) \rangle, e \rangle\}$ . Значит,  $\langle \langle a_1, \dots, a_n, s(d) \rangle, h(a_1, \dots, a_n, d, c) \rangle \in U$ . Если  $d = b$ , то  $\langle \langle a_1, \dots, a_n, b \rangle, c \rangle \in f$ . Тогда  $\langle \langle a_1, \dots, a_n, s(b) \rangle, h(a_1, \dots, a_n, b, c) \rangle \in f$ .

Так как нет такого элемента  $c$ , что  $\langle \langle a_1, \dots, a_n, b \rangle, c \rangle \in f$  и  $e = h(a_1, \dots, a_n, b, c)$ , то  $e \neq h(a_1, \dots, a_n, b, c)$ .

Поэтому  $\langle \langle a_1, \dots, a_n, s(b) \rangle, h(a_1, \dots, a_n, b, c) \rangle \in U$ .

Значит, для построенного множества  $U$  выполнены условия I) и II), поэтому  $f \subseteq U = f \setminus \{\langle \langle a_1, \dots, a_n, s(b) \rangle, e \rangle\}$ .

Полученное противоречие показывает, что если  $\langle \langle a_1, \dots, a_n, s(b) \rangle, e \rangle \in f$ , то найдется такой элемент  $c$ , что  $\langle \langle a_1, \dots, a_n, b \rangle, c \rangle \in f$  и  $e = h(a_1, \dots, a_n, b, c)$ .

Пусть  $b \in Q_{\bar{a}}$ . Чтобы доказать, что  $s(b) \in Q_{\bar{a}}$ , предположим, что  $\langle \langle a_1, \dots, a_n, s(b) \rangle, e_1 \rangle \in f$  &  $\langle \langle a_1, \dots, a_n, s(b) \rangle, e_2 \rangle \in f$ .

Тогда найдутся такие элементы  $c_i$  ( $i = 1, 2$ ), что  $\langle \langle a_1, \dots, a_n, b \rangle, c_i \rangle \in f$  и  $e_i = h(a_1, \dots, a_n, b, c_i)$ .

Так как  $b \in Q_{\bar{a}}$ , то  $c_1 = c_2$ , значит,  $e_1 = e_2$ . Поэтому  $s(b) \in Q_{\bar{a}}$ .

Значит,  $Q_{\bar{a}}$  — индуктивное множество, поэтому по третьей аксиоме Пеано  $Q_{\bar{a}} = \mathbb{N}$ .

Значит,  $f$  — функция.

Тем самым доказано существование функции  $f$  такой, что  $\delta(f) = \mathbb{N}^{n+1}$ ,  $\rho(f) \subseteq \mathbb{N}$  и для любых  $a_1, \dots, a_n, b \in \mathbb{N}$  выполняются следующие равенства

- 1)  $f(a_1, \dots, a_n, 1) = g(a_1, \dots, a_n)$ ,
- 2)  $f(a_1, \dots, a_n, s(b)) = h(a_1, \dots, a_n, b, f(a_1, \dots, a_n, b))$ .

Для доказательства единственности, предположим, что существуют функции  $f_1$  и  $f_2$  такие, что  $\delta(f_i) = \mathbb{N}^{n+1}$ ,  $\rho(f_i) \subseteq \mathbb{N}$  и для любых  $a_1, \dots, a_n, b \in \mathbb{N}$  выполняются следующие равенства

- 1)  $f_i(a_1, \dots, a_n, 1) = g(a_1, \dots, a_n)$ ,
- 2)  $f_i(a_1, \dots, a_n, s(b)) = h(a_1, \dots, a_n, b, f_i(a_1, \dots, a_n, b)) \quad i = 1, 2$ .

Для произвольного фиксированного набора  $\langle a_1, \dots, a_n \rangle$  обозначим через  $R_{\bar{a}}$  множество

$$\{b \mid f_1(a_1, \dots, a_n, b) = f_2(a_1, \dots, a_n, b)\}.$$

Так как  $f_1(a_1, \dots, a_n, 1) = g(a_1, \dots, a_n) = f_2(a_1, \dots, a_n, 1)$ , то  $1 \in R_{\bar{a}}$ .



Если  $b \in R_{\bar{a}}$ , то  $f_1(a_1, \dots, a_n, b) = f_2(a_1, \dots, a_n, b)$ , значит,  $f_1(a_1, \dots, a_n, s(b)) = h(a_1, \dots, a_n, b, f_1(a_1, \dots, a_n, b)) = h(a_1, \dots, a_n, b, f_2(a_1, \dots, a_n, b)) = f_2(a_1, \dots, a_n, s(b))$ . Следовательно,  $s(b) \in R_{\bar{a}}$ .

Значит,  $R_{\bar{a}}$  — индуктивное множество, поэтому по третьей аксиоме Пеано  $R_{\bar{a}} = \mathbb{N}$ . Поэтому  $f_1 = f_2$ .  $\square$

### 9.3. Определение сложения и умножения натуральных чисел

Из доказанной теоремы 9.2 следует, что существует единственная функция  $+$  такая, что  $\delta(+) = \mathbb{N}^2$ ,  $\rho(+) \subseteq \mathbb{N}$  и для любых  $a, b \in \mathbb{N}$  выполняются следующие равенства

- 1)  $a + 1 = s(a)$ ,
- 2)  $a + s(b) = s(a + b)$ .

Функция  $+$  называется *сложением* натуральных чисел.

В ниже следующих теоремах, с доказательствами которых читатель может ознакомиться, например, по книге С. Фефермана “Числовые системы”, устанавливается, что для введенной операции сложения натуральных чисел выполняются хорошо известные из школьного курса математики свойства.

Сложение натуральных чисел удовлетворяет ассоциативному закону.

**Теорема 9.3.** Для любых натуральных чисел  $a, b$  и  $c$  выполняется равенство  $a + (b + c) = (a + b) + c$ .

Коммутативность операции сложения натуральных чисел устанавливает следующая теорема.

**Теорема 9.4.** Для любых натуральных чисел  $a$  и  $b$  выполняется равенство  $a + b = b + a$ .

Для операции сложения натуральных чисел выполняется закон сокращения.

**Теорема 9.5.** Для любых натуральных чисел  $a, b$  и  $c$  из равенства  $a + c = b + c$  следует равенство  $a = b$ .

**Теорема 9.6.** Для любых натуральных чисел  $a$  и  $b$  выполняется неравенство  $b \neq a + b$ .

Следующая теорема устанавливает закон трихотомии для операции сложения натуральных чисел.

**Теорема 9.7.** Для любых натуральных чисел  $a$  и  $b$  выполняется одно из трех условий

- 1)  $a = b$ ;

II) найдется  $c$  такое, что  $a = b + c$ ;

III) найдется  $c$  такое, что  $b = a + c$ .

Причем никакие два из этих утверждений не могут выполняться одновременно. Элемент  $c$  в случаях II) и III) определен однозначно.

Из доказанной выше теоремы 9.2 следует, что существует единственная функция  $\cdot$  такая, что  $\delta(\cdot) = \mathbb{N}^2$ ,  $\rho(\cdot) \subseteq \mathbb{N}$  и для любых  $a, b \in \mathbb{N}$  выполняются следующие равенства

$$1) a \cdot 1 = a,$$

$$2) a \cdot s(b) = a \cdot b + a.$$

Функция  $\cdot$  называется *умножением* натуральных чисел.

В ниже следующих теоремах, с доказательствами которых читатель может ознакомиться, например, по книге С. Фефермана “Числовые системы”, устанавливается, что для введенной операции умножения натуральных чисел выполняются хорошо известные из школьного курса математики свойства.

Левая дистрибутивность операции умножения относительно сложения.

**Теорема 9.8.** Для любых натуральных чисел  $a, b$  и  $c$  выполняется равенство  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ .

Правая дистрибутивность операции умножения относительно сложения.

**Теорема 9.9.** Для любых натуральных чисел  $a, b$  и  $c$  выполняется равенство  $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ .

Коммутативность операции умножения натуральных чисел.

**Теорема 9.10.** Для любых натуральных чисел  $a$  и  $b$  выполняется равенство  $a \cdot b = b \cdot a$ .

Ассоциативность операции умножения натуральных чисел.

**Теорема 9.11.** Для любых натуральных чисел  $a, b$  и  $c$  выполняется равенство  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ .

Закон сокращения для операции умножения натуральных чисел.

**Теорема 9.12.** Для любых натуральных чисел  $a, b$  и  $c$  из равенства  $a \cdot c = b \cdot c$  следует равенство  $a = b$ .

Из теоремы 9.2 следует, что существует единственная функция  $\uparrow$  такая, что  $\delta(\uparrow) = \mathbb{N}^2$ ,  $\rho(\uparrow) \subseteq \mathbb{N}$  и для любых  $a, b \in \mathbb{N}$  выполняются следующие равенства

- 1)  $a \uparrow 1 = a$ ,
- 2)  $a \uparrow s(b) = (a \uparrow b) \cdot a$ .

Функция  $\uparrow$  называется *возведением в степень* натуральных чисел. Вместо  $a \uparrow b$  пишем  $a^b$ .

Нетрудно доказать следующую теорему.

**Теорема 9.13.** Для любых натуральных чисел  $a, b$  и  $c$  выполняются следующие равенства

- I)  $1^b = 1$ ;
- II)  $a^b \cdot a^c = a^{b+c}$ ;
- III)  $(a^b)^c = a^{b \cdot c}$ ;
- IV)  $(a \cdot b)^c = a^c \cdot b^c$ .

## 10. Некоторые приложения аксиомы выбора

Чтобы продемонстрировать применения аксиомы выбора, рассмотрим некоторые задачи из теории измерения площадей и объемов.

**Определение 10.1.** Движением числовой прямой  $\mathbb{R}$  называется любое отображение  $f : \mathbb{R} \rightarrow \mathbb{R}$ , сохраняющее расстояние, т.е. для любых  $\alpha, \beta \in \mathbb{R}$  выполняется равенство  $|f(\alpha) - f(\beta)| = |\alpha - \beta|$ .

Примеры движений числовой прямой:

- 1)  $f_a(x) = x + a$ , где  $a$  — фиксированное действительное число; такие движения  $f_a$  называются **сдвигами**;
- 2)  $f(x) = -x$  — симметрия относительно начала координат;
- 3)  $f_a^{(-)}(x) = -x + a$ , где  $a$  — фиксированное действительное число.

Оказывается, что других движений числовой прямой нет.

**Теорема 10.1.** Если  $g$  — движение числовой прямой, то найдется такое действительное число  $a$ , что либо  $g = f_a$ , либо  $g = f_a^{(-)}$ .

*Доказательство.* Пусть  $g$  — движение числовой прямой. Полагаем  $a = g(0)$ . Тогда из определения движения следует, что для любого  $x$  выполняются равенства

$$|g(x) - a| = |g(x) - g(0)| = |x - 0| = |x|.$$

Значит,  $g(x) = (-1)^{\sigma(x)}x + a$ , где функция  $\sigma(x)$  принимает лишь два значения 0 и 1. Покажем, что функция  $\sigma(x)$  постоянна.

Пусть  $\alpha$  и  $\beta$  — два различных действительных числа, причем  $\alpha$  отлично от нуля. Тогда

$$g(\alpha) - g(\beta) = (-1)^{\sigma(\alpha)}\alpha - (-1)^{\sigma(\beta)}\beta.$$

$$g(\alpha) - g(\beta) = (-1)^{\sigma(\alpha)}(\alpha - (-1)^\rho\beta),$$

где  $\rho = \sigma(\beta) - \sigma(\alpha)$ . Заметим, что  $\rho$  может принимать одно из трех значений  $-1, 0, 1$ . Так как  $g$  движение, то  $|\alpha - (-1)^\rho\beta| = |\alpha - \beta|$ .

Значит,  $\alpha - (-1)^\rho\beta = \pm(\alpha - \beta)$ . Если  $\alpha - (-1)^\rho\beta = -(\alpha - \beta)$ , то  $2\alpha = [(-1)^\rho + 1]\beta$ . При  $\rho = \pm 1$  получаем  $\alpha = 0$ , что противоречит выбору  $\alpha$ , а при  $\rho = 0$  получаем, что  $\alpha = \beta$ , а это противоречит выбору  $\alpha$  и  $\beta$ .

Следовательно,  $\alpha - (-1)^\rho\beta = \alpha - \beta$ , а значит,  $\rho = 0$ .

Тем самым доказано, что для любых двух различных действительных чисел  $\alpha$  и  $\beta$ , из которых хотя бы одно отлично от нуля, выполняется равенство  $\sigma(\alpha) = \sigma(\beta) = \sigma$ . Поэтому для любого  $x$   $g(x) = (-1)^\sigma x + a$ .  $\square$

**Определение 10.2.** Подмножества  $A$  и  $B$  числовой прямой  $\mathbb{R}$  называются **конгруэнтными**, если существует такое движение  $f$  числовой прямой  $\mathbb{R}$ , что  $f(A) = B$ .

Легко проверить, что отношение конгруэнтности является отношением эквивалентности на множестве всех подмножеств числовой прямой  $\mathbb{R}$ .

**Определение 10.3.** Движением пространства  $\mathbb{R}^n$  называется любое отображение  $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ , сохраняющее расстояние, т.е. для любых  $v, u \in \mathbb{R}^n$  выполняется равенство  $d(f(v), f(u)) = d(v, u)$ , где  $d(x, y)$  — функция, задающая расстояние в пространстве  $\mathbb{R}^n$ .

Вопрос об описании движений пространства  $\mathbb{R}^n$  изучается в геометрии и линейной алгебре.

Следуя И.П. Натансону [31], рассмотрим две задачи — трудную и легкую задачи теории измерения в пространстве  $\mathbb{R}^n$ .

**Трудная задача теории измерения.** Требуется сопоставить каждому ограниченному подмножеству  $A$  пространства  $\mathbb{R}^n$  неотрицательное действительное число  $\mu(A)$ , называемое мерой множества  $A$ , так, чтобы выполнялись следующие условия:

$$1) \mu([0, 1]^n) = 1;$$

2) Если множества  $A$  и  $B$  конгруэнтны, то  $\mu(A) = \mu(B)$ ;

3) Если  $(A_i)_{i \in I}$  — конечное или счетное семейство ограниченных попарно не пересекающихся множеств и их объединение  $\bigcup_{i \in I} A_i$  ограничено, то

$$\mu\left(\bigcup_{i \in I} A_i\right) = \sum_{i \in I} \mu(A_i).$$

**Теорема 10.2.** Трудная задача теории измерения неразрешима даже для числовой прямой  $\mathbb{R}$ .

*Доказательство.* Предположим противное и пусть  $\mu$  — мера, определенная на всех ограниченных подмножествах числовой прямой. Рассмотрим на отрезке  $[0, 1]$  числовой прямой  $\mathbb{R}$  введенное раньше отношение сравнимости по множеству рациональных чисел  $\mathbb{Q}$ : напомним, что для действительных чисел  $\alpha$  и  $\beta$  выполнено  $\alpha \equiv \beta \pmod{(\mathbb{Q})}$  тогда и только тогда, когда разность  $\alpha - \beta$  лежит в  $\mathbb{Q}$ . Это отношение является отношением эквивалентности. По аксиоме выбора существует множество  $V$ , содержащее в точности по одному элементу из каждого класса эквивалентности отрезка  $[0, 1]$  по этому отношению.

Рассмотрим некоторую нумерацию

$$r_0 = 0, r_1, \dots, r_n, \dots$$

всех рациональных чисел отрезка  $[-1, 1]$ . Полагаем  $A_n \equiv f_{r_n}(A)$ , где  $f_{r_n}$  — сдвиг на число  $r_n$ . Каждое множество  $A_n$  конгруэнтно множеству  $A$ , поэтому  $\mu(A_n) = \mu(A)$ . Рассмотрим семейство  $(A_n)_{n \in \mathbb{N}}$  ограниченных попарно не пересекающихся множеств. Все они содержатся в отрезке  $[-1, 2]$ , поэтому их объединение ограничено и

$$[0, 1] \subseteq \bigcup_{n \in \mathbb{N}} A_n \subseteq [-1, 2].$$

Значит, в силу пункта 3) выполняются равенства

$$\mu([0, 1]) \leq \sum_{n \in \mathbb{N}} \mu(A_n) \leq \mu([-1, 2]).$$

$\mu([0, 1]) = 1$ . Каждое из множеств  $A_n$  конгруэнтно множеству  $A$ , поэтому  $\mu(A_n) = \mu(A) = \sigma$ . Получаем противоречивую систему неравенств

$$1 \leq \sum_{n \in \mathbb{N}} \sigma \leq \mu([-3/2, 3/2]).$$

Это завершает доказательство теоремы. □

Естественно возникает вопрос, насколько существенно использование аксиомы выбора в доказательстве предыдущей теоремы, т.е. можно ли доказать эту



теорему без использования аксиомы выбора или других аксиом, ей эквивалентных. Оказывается, что в определенном смысле без аксиомы выбора обойтись нельзя. Но как это можно доказать, т.е. как можно доказать, что нечто нельзя доказать. Попытки дать ответ на этот вопрос приведут нас к необходимости уточнения, казалось бы, всем хорошо известного понятия “математическое доказательство”. Это было сделано в первой половине XX века в рамках математической логики, некоторым введением в которую служит следующая глава пособия.

**Легкая задача теории измерения.** Требуется сопоставить каждому ограниченному подмножеству  $A$  пространства  $\mathbb{R}^n$  неотрицательное действительное число  $\mu(A)$ , называемое мерой множества  $A$ , так, чтобы выполнялись следующие условия:

- 1)  $\mu([0, 1]^n) = 1$ ;
- 2) Если множества  $A$  и  $B$  конгруэнтны, то  $\mu(A) = \mu(B)$ ;
- 3) Если  $(A_i)_{i \in \mathbb{N}_m}$  — конечное семейство ограниченных попарно не пересекающихся множеств, то

$$\mu\left(\bigcup_{i \in \mathbb{N}_m} A_i\right) = \sum_{i \in \mathbb{N}_m} \mu(A_i).$$

**Теорема 10.3 (Ф. Хаусдорф).** При  $n \geq 3$  легкая задача теории измерения неразрешима для пространства  $\mathbb{R}^n$ .

Доказательство этой теоремы не является слишком сложным, однако его аккуратное изложение с подробной проверкой всех деталей увело бы нас слишком далеко от основной линии пособия. Поэтому мы ограничимся лишь обсуждением основных идей доказательства.

Множества точек пространства  $\mathbb{R}^n$ , совпадающие при некотором движении этого пространства, называются *конгруэнтными*.

Множества  $A$  и  $B$  называются *конгруэнтными при конечном разбиении*, если найдется такое натуральное число  $m$ , такие попарно не пересекающиеся множества  $A_1, \dots, A_m$  и такие попарно непересекающиеся множества  $B_1, \dots, B_m$ , что

$$A = A_1 \cup A_2 \cup \dots \cup A_m, \quad B = B_1 \cup B_2 \cup \dots \cup B_m$$

$A_1$  конгруэнтно  $B_1$ , ...,  $A_m$  конгруэнтно  $B_m$ .

Запись  $A \approx B$  будет обозначать, что множества  $A$  и  $B$  являются конгруэнтными при конечном разбиении.

Конгруэнтные при конечном разбиении множества называются еще *равносоставленными*. Однако, в геометрии последний термин закреплен за фигурами, которые можно разбить на одинаковое число не имеющих общих точек подфигур, соответственно конгруэнтных.

Доказано, что прямоугольный равнобедренный треугольник конгруэнтен при конечном разбиении квадрату, но доказательство непростое. Можно показать, что отношение равносоставленности транзитивно.

Стефан Банах и Альфред Тарский доказали следующий замечательный факт: для того, чтобы два многоугольника на плоскости имели равные площади, необходима и достаточна их конгруэнтность при конечных разбиениях.

В 1924 году С. Банах и А. Тарский доказали следующее, на первый взгляд, весьма парадоксальное, утверждение: любые два ограниченных тела в пространстве  $\mathbb{R}^3$  конгруэнтны при конечном разбиении. Любой шар можно разбить на 5 непересекающихся множеств, из которых путем поворотов и переносов можно получить два непересекающихся шара, каждый из которых конгруэнтен исходному шару. Значит, в замкнутом 3-мерном шаре  $D$  существуют два таких подмножества  $X$  и  $Y$ , что  $D = X \cup Y$ ,  $X \cap Y = \emptyset$ ,  $X \approx D$  и  $Y \approx D$ . В то же время для круга это невозможно. Отсюда следует, в частности, неразрешимость при  $n \geq 3$  для пространства  $R^n$  легкой задачи теории измерения.

Однако не известно, конгруэнтен ли круг при конечном разбиении квадрату с той же площадью. В этом смысле проблема “квадратуры круга” остается открытой.

В статье Т.Дж. Йеха [44] приведен доступный для понимания вариант доказательства теоремы С. Банаха и А. Тарского, из которого легко получить доказательство теоремы Хаусдорфа. Основные идеи этого доказательства будут изложены ниже.

В пространстве  $\mathbb{R}^3$  рассматриваются две оси  $a_\varphi$  и  $a_\psi$ , расположенные в плоскости  $XOY$ , причем  $a_\psi$  — это ось  $OX$ , а ось  $a_\varphi$  составляет с ней угол  $\theta$ . Через  $\psi$  обозначим поворот на угол  $120^\circ$  относительно оси  $a_\psi$ , а через  $\varphi$  — поворот на угол  $180^\circ$  относительно оси  $a_\varphi$ . Ясно, что  $\psi^3 = 1$  и  $\varphi^2 = 1$ , где через 1 обозначено тождественное отображение пространства  $\mathbb{R}^3$  на себя. В группе всех движений пространства  $\mathbb{R}^3$  рассмотрим подгруппу, порожденную вращениями  $\psi$  и  $\varphi$ . Приведенным словом назовем любое выражение вида

$$\varphi^\alpha \psi^{\beta_1} \varphi \psi^{\beta_2} \varphi \psi^{\beta_3} \dots \varphi \psi^{\beta_t} \varphi \psi^\beta,$$

где  $t \geq 0$ ,  $\alpha \in \{0, 1\}$ ,  $\beta \in \{0, 1, 2\}$  и  $\beta_1, \dots, \beta_t \in \{1, 2\}$ .

Выписав матрицы этих преобразований в стандартном базисе, можно заметить, что если приведенное слово определяет тождественное отображение, то тангенс соответствующего угла  $\theta/2$  является корнем некоторого ненулевого полинома над полем  $\mathbb{Q}[\sqrt{3}]$ . Так как множество полиномов  $\mathbb{Q}[\sqrt{3}][x]$  счетно, а у каждого полинома множество корней конечно, то существует угол между осями  $\theta$ , для которого никакое нетривиальное приведенное слово не даст тождественное преобразование. Пусть  $\theta$  — один из таких углов, тогда любым двум различным приведенным словам соответствуют различные преобразования. Обозначим через  $\mathbb{G}$  группу, порожденную преобразованиями  $\psi$  и  $\varphi$ . Тогда выше сказанное означает, что группа  $\mathbb{G}$  имеет задание (генетический код)

$$\langle\langle \psi, \varphi \mid \psi^3 = 1, \varphi^2 = 1 \rangle\rangle$$

и является свободным произведением циклических групп  $\langle\langle \psi \mid \psi^3 = 1 \rangle\rangle$  и  $\langle\langle \varphi \mid \varphi^2 = 1 \rangle\rangle$  третьего и второго порядков.

Специальным образом разобьем множество  $\mathbb{G}$  на три попарно непересекающихся множества  $\mathcal{A}$ ,  $\mathcal{B}$  и  $\mathcal{C}$ . Для этого упорядочим все приведенные слова в порядке возрастания их длины, а слова одинаковой длины упорядочим, например, лексикографически, считая, что  $\varphi$  предшествует  $\psi$ , получим список

$$w_0 = e, w_1 = \varphi, w_2 = \psi, w_3, \dots, w_n, \dots$$

Полагаем  $w_0 = e \in \mathcal{A}$ ,  $w_1 = \varphi \in \mathcal{B}$ ,  $w_2 = \psi \in \mathcal{B}$ ,  $\varphi\psi \in \mathcal{A}$ ,  $\psi\varphi \in \mathcal{C}$  и  $\psi^2 \in \mathcal{C}$ .

Пусть для любого  $t < n$  слово  $w_t$  отнесено к одному из множеств  $\mathcal{A}$ ,  $\mathcal{B}$  или  $\mathcal{C}$ . Рассмотрим слово  $w_n$ . Можно считать, что его длина не меньше 3. Возможны три случая: 1)  $w_n = \varphi\psi u$ , 2)  $w_n = \psi\varphi u$  и 3)  $w_n = \psi\psi u$ .

Рассмотрим случай 1)  $w_n = \varphi\psi u$ .

Если  $\psi u \in \mathcal{A}$ , то  $w_n = \varphi\psi u \in \mathcal{B}$ .

Если  $\psi u \in \mathcal{B}$ , то  $w_n = \varphi\psi u \in \mathcal{A}$ .

Если  $\psi u \in \mathcal{C}$ , то  $w_n = \varphi\psi u \in \mathcal{A}$ .

Рассмотрим случай 2)  $w_n = \psi\varphi u$ .

Если  $\varphi u \in \mathcal{A}$ , то  $w_n = \psi\varphi u \in \mathcal{B}$ .

Если  $\varphi u \in \mathcal{B}$ , то  $w_n = \psi\varphi u \in \mathcal{C}$ .

Если  $\varphi u \in \mathcal{C}$ , то  $w_n = \psi\varphi u \in \mathcal{A}$ .

Рассмотрим случай 3)  $w_n = \psi\psi u$ .

Если  $u \in \mathcal{A}$ , то  $w_n = \psi\psi u \in \mathcal{C}$ .

Если  $u \in \mathcal{B}$ , то  $w_n = \psi\psi u \in \mathcal{A}$ .

Если  $u \in \mathcal{C}$ , то  $w_n = \psi\psi u \in \mathcal{B}$ .

В итоге получаем разбиение множества  $\mathbb{G}$  на три попарно непересекающихся множества  $\mathcal{A}$ ,  $\mathcal{B}$  и  $\mathcal{C}$ .

Покажем, что  $\psi^2(\mathcal{A}) = \mathcal{C}$ ,  $\psi^2(\mathcal{B}) = \mathcal{A}$ ,  $\psi^2(\mathcal{C}) = \mathcal{B}$ ,  $\psi(\mathcal{A}) = \mathcal{B}$ ,  $\psi(\mathcal{B}) = \mathcal{C}$ ,  $\psi(\mathcal{C}) = \mathcal{A}$  и  $\varphi(\mathcal{A}) = \mathcal{B} \cup \mathcal{C}$ .

Пусть  $w \in \mathcal{A}$ .

Если  $w$  — это  $\varphi u$ , то  $\psi w = \psi\varphi u \in \mathcal{B}$  и  $\psi^2 w \in \mathcal{C}$ .

Если  $w$  — это  $\psi\varphi u$ , то  $\varphi u \in \mathcal{C}$ , поэтому  $\psi w = \psi^2\varphi u \in \mathcal{B}$  и  $\psi^2 w = \varphi u \in \mathcal{C}$ .

Если  $w$  — это  $\psi^2\varphi u$ , то  $\varphi u \in \mathcal{B}$ , поэтому  $\psi w = \varphi u \in \mathcal{B}$  и  $\psi^2 w = \psi\varphi u \in \mathcal{C}$ .

Итак,  $\psi(\mathcal{A}) \subset \mathcal{B}$  и  $\psi^2(\mathcal{A}) \subset \mathcal{C}$ .

Покажем, что  $\psi(\mathcal{A}) = \mathcal{B}$ .

Допустим, что  $\psi(\mathcal{A}) \neq \mathcal{B}$  и пусть  $w$  — слово минимальной длины из  $\mathcal{B} \setminus \psi(\mathcal{A})$ . Если длина  $w$  равна 1, то  $w$  может быть лишь словом  $\varphi$ , но тогда  $\psi^2\varphi \in \psi(\mathcal{A})$ , поэтому  $\varphi = \psi(\psi^2\varphi) \in \psi(\mathcal{A})$ . Полученное противоречие показывает, что длина  $w$  не меньше 2. Для некоторого  $u$  возможен один из трех случаев

1)  $w$  — это  $\psi\varphi u$ ,

2)  $w$  — это  $\varphi\psi u$ ,

3)  $w$  — это  $\psi^2 u$ .

В случае 1)  $\varphi u \in \mathcal{A}$  и  $w = \psi(\varphi u) \in \psi(\mathcal{A})$ . Противоречие.

В случае 2)  $\psi^2 \varphi \psi u \in \mathcal{A}$  и  $w = \psi(\psi^2 \varphi \psi u) \in \psi(\mathcal{A})$ . Противоречие.

В случае 3)  $u \in \mathcal{C}$ ,  $\psi u \in \mathcal{A}$  и  $w = \psi^2 u \in \psi(\mathcal{A})$ . Противоречие.

Тем самым доказано, что  $\psi(\mathcal{A}) = \mathcal{B}$ .

По той же схеме доказываются и все остальные равенства.

Так как преобразования из группы  $\mathbb{G}$  сохраняют расстояния, то эта группа *действует* на каждой 2-мерной сфере  $\mathbb{S}$  фиксированного радиуса пространства  $\mathbb{R}^3$ . Для элемента  $g$  группы  $\mathbb{G}$  и точки  $v$  сферы  $\mathbb{S}$  через  $g \cdot v$  будем обозначать точку сферы, в которую переходит точка  $v$  при повороте  $g$ . Получаем отображение  $\cdot : \mathbb{S} \times \mathbb{G} \rightarrow \mathbb{G}$ , для которого выполняются следующие свойства:

$$1) \quad (gh) \cdot v = g \cdot (h \cdot v), \quad 2) \quad 1 \cdot v = v.$$

На сфере  $\mathbb{S}$  пространства  $\mathbb{R}^3$  введем отношение эквивалентности

$$v \equiv_{\mathbb{S}} u \iff (\exists g \in \mathbb{G})(u = g \cdot v).$$

Нетрудно проверить, что введенное отношение  $\equiv_{\mathbb{S}}$  действительно является отношением эквивалентности, т.е. для него выполняются свойства рефлексивности, симметричности и транзитивности. Для произвольной точки  $v$  сферы  $\mathbb{S}$  через  $\mathbb{G}(v)$  обозначим соответствующий *класс эквивалентности*, т.е. множество  $\{g \cdot v \mid g \in \mathbb{G}\}$ , которое называется *орбитой* точки  $v$ .

Каждое непустое приведенное слово определяет нетождественное, сохраняющее расстояния и ориентацию линейное преобразование пространства  $\mathbb{R}^3$ , биективно отображающее единичную сферу на себя. По теореме Л. Эйлера оно является поворотом относительно некоторой оси, поэтому у него на сфере в точности две неподвижные точки. Значит, если два различных приведенных слова  $W(\psi, \varphi)$  и  $U(\psi, \varphi)$  переводят точку  $x$  сферы в одну и ту же точку, т.е.  $W(\psi, \varphi)(x) = U(\psi, \varphi)(x)$ , то эта точка  $x$  является *неподвижной точкой неединичного приведенного слова*  $W^{-1}(\psi, \varphi)U(\psi, \varphi)$ . Такие точки назовем “циклическими”. Из счетности множества приведенных слов и конечности числа неподвижных точек у каждого такого преобразования следует счетность множества “циклических” точек. Заметим, что если в орбите имеется хотя бы одна циклическая точка, то все точки орбиты - циклические: если  $W(\varphi, \psi)(v) = v$  и  $u = U(\varphi, \psi)(v)$ , то  $U(\varphi, \psi)W(\varphi, \psi)U^{-1}(\varphi, \psi)(u) = u$ . Орбиты, содержащие циклические точки, назовем *циклическими*. В силу сказанного выше множество циклических орбит счетно. А так как каждая орбита счетна, то счетным будет и объединение  $Q_1$  всех циклических орбит. Используя *аксиому выбора*, “построим” множество  $M$ , содержащее из каждой нециклической орбиты по одной точке. Для произвольного подмножества  $H$  группы  $\mathbb{G}$  и подмножества  $X$  сферы  $\mathbb{S}$  через  $H \cdot X$  обозначим следующее множество

$$\{h \cdot v \mid h \in H \wedge v \in X\}.$$

Полагаем

$$A = A \cdot M, B = B \cdot M, C = C \cdot M.$$

Тогда  $S = A \cup B \cup C \cup Q$  и  $\psi^2(A) = C$ ,  $\psi^2(B) = A$ ,  $\psi^2(C) = B$  и  $\varphi(A) = B \cup C$ .

Обозначим через  $D$  шар пространства  $\mathbb{R}^3$  с центром в начале координат. Для произвольного подмножества  $E$  сферы  $S$ , ограничивающей шар  $D$ , через  $E$  обозначим подмножество этого шара, состоящее из всех отличных от начала координат точек всех отрезков, соединяющих начало координат  $O$  с точками множества  $E$ .

Тогда

$$D = A \cup B \cup C \cup Q_1 \cup \{O\}$$

и  $\psi^2(A) = C$ ,  $\psi^2(B) = A$ ,  $\psi^2(C) = B$  и  $\varphi(A) = B \cup C$ . Пусть  $Q$  — это  $Q_1 \cup \{O\}$ .

Допустим, что легкая задача теории измерения разрешима для пространства  $\mathbb{R}^3$  и пусть  $\mu$  — соответствующая мера. Тогда  $\mu(D) = \mu(A) + \mu(B) + \mu(C) + \mu(Q)$ ,  $\mu(A) = \mu(C)$ ,  $\mu(B) = \mu(A)$ ,  $\mu(C) = \mu(B)$  и  $\mu(A) = \mu(B) + \mu(C)$ .

Значит,  $\mu(A) = \mu(B) = \mu(C) = 0$ . Поэтому  $\mu(D) = \mu(Q)$ .

Для двух различных точек сферы  $v$  и  $u$  существуют лишь два поворота, переводящих  $v$  в  $u$ . Значит, существует лишь счетное число осей, повороты относительно которых переводят хотя бы одну точку счетного множества в какую-либо точку этого множества. Поэтому существует такой поворот  $f$ , для которого  $f(Q) \cap Q = \emptyset$ . Тогда  $D = Q \cup f(Q) \cup U$  и эти три множества попарно не пересекаются, поэтому  $\mu(D) \geq 2\mu(Q)$ , что вместе с равенством  $\mu(D) = \mu(Q)$  дает равенство  $\mu(D) = 0$ . Значит, мера любого подмножества шара  $D$  равна 0, поэтому мера любого ограниченного множества равна 0, т.е.  $\mu$  — нулевая мера, что противоречит требованию  $\mu([0, 1]^n) = 1$ .

В качестве еще одного применения аксиомы выбора рассмотрим теорему А.Н. Тихонова о компактности произведения компактных топологических пространств. Но вначале напомним основные, необходимые для дальнейшего, определения из топологии.

**Определение 10.4.** Топологическое пространство — это пара  $\langle U, \tau \rangle$ , где  $U$  — множество, а  $\tau$  — система его подмножеств, т.е.  $\tau \subseteq P(U)$ , удовлетворяющая следующим условиям — аксиомам топологического пространства:

- 1)  $\emptyset \in \tau$ ,  $U \in \tau$ ,
- 2) если  $A, B \in \tau$ , то  $A \cap B \in \tau$ ,
- 3) для произвольного семейства  $(A_i)_{i \in I}$  множеств  $A_i$  из  $\tau$   $\bigcup_{i \in I} A_i \in \tau$ .

Множества из  $\tau$  называются открытыми множествами, а сама система  $\tau$  — топологией на  $U$ .

Дополнения открытых множеств называются замкнутыми множествами. Система  $F$  замкнутых подмножеств топологического пространства удовлетворяет следующим условиям, которые могут выступать в качестве аксиом топологического пространства при его определении через понятие замкнутого множества:



- 1)  $\emptyset \in F, U \in F$ ,
- 2) если  $A, B \in F$ , то  $A \cup B \in F$ ,
- 3) для произвольного семейства  $(A_i)_{i \in I}$  множеств  $A_i$  из  $F$   $\bigcap_{i \in I} A_i \in F$ .

Так как топологии — это подмножества множества  $P(U)$ , то их можно сравнивать: топология  $\tau_1$  слабее топологии  $\tau_2$ , если  $\tau_1 \subseteq \tau_2$ , при этом топология  $\tau_2$  сильнее топологии  $\tau_1$ .

Так как пересечение произвольного семейства  $(\tau_i)_{i \in I}$  топологий на множестве  $U$  является топологией на этом множестве, то для произвольного подмножества  $X$  множества  $P(U)$  пересечение всех содержащих  $X$  топологий будет “слабейшей” топологией на  $U$ , порожденной  $X$ , которую мы будем обозначать через  $\tau(X)$ . Эта топология удовлетворяет следующим условиям:

- 1)  $X \subseteq \tau(X)$ ,
- 2) если  $\tau_1$  — топология на  $U$  и  $X \subseteq \tau_1$ ,  $\tau(X) \subseteq \tau_1$ .

Можно дать “более конструктивное” описание топологии  $\tau(X)$ . Из аксиом для открытых множеств топологического пространства сразу следует, что произвольное объединение конечных пересечений множеств из  $X$  принадлежит  $\tau(X)$ . Нетрудно показать, что множество, состоящее из произвольных объединений конечных пересечений множеств из  $X$ , удовлетворяет аксиомам для открытых множеств, если считать, что объединение пустого семейства множеств пусто, а пересечение пустого семейства множеств есть все  $U$ . Значит, топология  $\tau(X)$  — это всевозможные объединения конечных пересечений множеств из  $X$ .

Пусть  $\langle U, \tau \rangle$  и  $\langle U_1, \tau_1 \rangle$  — два топологических пространства. Отображение  $f: U \rightarrow U_1$  называется *непрерывным* отображением топологического пространства  $\langle U, \tau \rangle$  в топологическое пространство  $\langle U_1, \tau_1 \rangle$ , если прообраз  $f^{-1}(X)$  любого открытого подмножества  $X$  пространства  $U_1$  открыт в пространстве  $U$ .

Для произведения  $\prod_{i \in I} U_i$  семейства  $(U_i)_{i \in I}$  множеств  $U_i$  через  $pr_t$  обозначим проектирование этого произведения на  $t$ -ый сомножитель, т.е.  $pr_t((u_i)_{i \in I}) = u_t$ .

Если  $(\langle U_i, \tau_i \rangle)_{i \in I}$  — семейство топологических пространств, то на их произведении  $\prod_{i \in I} U_i$  существует *слабейшая топология*  $\tau$ , в которой непрерывны все функции проектирования  $pr_t$ . Множество  $\prod_{i \in I} U_i$  вместе с этой топологией  $\tau$  называется *произведением* семейства  $(\langle U_i, \tau_i \rangle)_{i \in I}$  топологических пространств и обозначается через  $\prod_{i \in I} \langle U_i, \tau_i \rangle$ .

Дадим “более конструктивное” описание этой топологии.

Для произвольного  $t \in I$  и произвольного открытого в  $U_t$  множества  $G_t$  его прообраз

$$pr_t^{-1}(G_t) = \prod_{i \in I \setminus \{t\}} U_i \times G_t$$

относительно отображения проектирования  $pr_t$  должен быть открытым множеством в  $U$ , а значит, открытыми в  $U$  будут и конечные пересечения этих

множеств, т.е. множества вида  $\Gamma$  вида  $\prod_{t \in I} G_t$ , где при любом  $t \in I$ :  $G_t$  — открытое множество в  $U_t$  и лишь для конечного множества индексов  $t$  множество  $G_t$  отлично от всего  $U_t$ , поэтому открытыми будут произвольные объединения множеств указанного вида. Нетрудно проверить, что семейство подмножеств в  $U$ , состоящее из произвольных объединений множеств вида  $\Gamma$  вида  $\prod_{t \in I} G_t$ , где при любом  $t \in I$ :  $G_t$  — открытое множество в  $U_t$  и лишь для конечного множества индексов  $t$  множество  $G_t$  отлично от всего  $U_t$ , удовлетворяет аксиомам топологического пространства, а значит, это и есть семейство всех открытых множеств в  $U$ . Таким образом каждое открытое множество  $W$  из  $U$  есть объединение открытых множеств  $\Gamma$  вида  $\prod_{t \in I} G_t$ , где при любом  $t \in I$ :  $G_t$  — открытое множество в  $U_t$  и лишь для конечного множества индексов  $t$  множество  $G_t$  отлично от всего  $U_t$ , поэтому открытые множества  $\Gamma$  указанного вида образуют базу топологии на  $U$ . Эта база носит название база А.Н. Тихонова.

**Определение 10.5.** Топологическое пространство  $\langle U, \tau \rangle$  называется компактным, если из любого его покрытия открытыми множествами можно выделить конечное подпокрытие, т.е. для любого семейства  $(V_i)_{i \in I}$  открытых множеств из равенства  $U = \bigcup_{i \in I} V_i$  следует, что существует такое конечное подмножество  $I_0$  множества  $I$ , что  $U = \bigcup_{i \in I_0} V_i$ .

Эквивалентное определение через понятие замкнутого множества следующее. Семейство  $\mathcal{R}$  подмножеств множества  $U$  называется *центрированным*, если пересечение любого конечного числа множеств из  $\mathcal{R}$  непусто. Читателю в качестве упражнения предлагается доказать, что топологическое пространство является компактным тогда и только тогда, когда непусто пересечение любого центрированного семейства замкнутых подмножеств.

**Теорема 10.4 (А.Н. Тихонов).** Произведение  $\prod_{i \in I} \langle U_i, \tau_i \rangle$  семейства  $(\langle U_i, \tau_i \rangle)_{i \in I}$  компактных топологических пространств компактно.

**Лемма 10.1.** Для любого центрированного семейства  $\mathcal{R}_0$  подмножеств множества  $U$  существует максимальное центрированное семейство  $\mathcal{R} \subseteq P(U)$ , содержащее  $\mathcal{R}_0$ .

**Д о к а з а т е л ь с т в о.** Напомним, что множество  $\Phi$  подмножеств множества  $U$  (т.е.  $\Phi \subseteq P(U)$ ) называется *фильтром* в  $P(U)$ , если оно удовлетворяет следующим условиям, аксиомам фильтра:

- 1)  $\emptyset \notin \Phi$ ,
- 2) если  $A \in \Phi$  и  $B \in \Phi$ , то  $A \cap B \in \Phi$ ,
- 3) если  $A \in \Phi$  и  $A \subseteq B$ , то  $B \in \Phi$ .

Так как объединение любого линейно упорядоченного отношением включения  $\subseteq$  множества фильтров из  $P(U)$  само будет фильтром в  $P(U)$ , то для любой

цепи фильтров в  $P(U)$  существует во множестве всех фильтров в  $P(U)$  верхняя грань, поэтому по лемме Цорна любой фильтр в  $P(U)$  содержится в некотором максимальном фильтре.

По центрированному семейству  $\mathcal{R}_0$  построим содержащий его фильтр  $\Phi(\mathcal{R}_0) \supseteq \mathcal{R}_0$ , полагая

$$\Phi(\mathcal{R}_0) = \{ Y \mid (\exists X_1, \dots, X_n \in \mathcal{R}_0) \left( \bigcap_{i=1}^n X_i \subseteq Y \right) \}.$$

Проверка выполнимости для  $\Phi(\mathcal{R}_0)$  аксиом фильтра предоставляется читателю в качестве простого упражнения. Ясно, что  $\Phi(\mathcal{R}_0) \supseteq \mathcal{R}_0$ . Пусть  $\Phi$  — максимальный фильтр, содержащий  $\Phi(\mathcal{R}_0)$ .

Покажем, что *каждый максимальный фильтр является максимальным центрированным семейством, а каждое максимальное центрированное семейство — максимальным фильтром.*

Пусть  $\mathcal{R}$  — максимальное центрированное семейство. Строим содержащий  $\mathcal{R}$  фильтр  $\Phi(\mathcal{R})$ . Так как фильтр  $\Phi(\mathcal{R})$  является центрированным семейством, то из максимальной семейства  $\mathcal{R}$  следует равенство  $\Phi(\mathcal{R}) = \mathcal{R}$ . Значит,  $\mathcal{R}$  — фильтр. Если фильтр  $\Phi$  содержит  $\mathcal{R}$ , то так как  $\Phi$  — центрированное семейство, выполняется равенство  $\Phi = \mathcal{R}$ . Поэтому  $\mathcal{R}$  — максимальный фильтр.

Пусть  $\mathcal{R}$  — максимальный фильтр. Покажем, что  $\mathcal{R}$  — максимальное центрированное семейство.

Так как каждый фильтр является центрированным семейством, то остается доказать максимальность семейства  $\mathcal{R}$ . Пусть  $\mathcal{R}'$  — центрированное семейство, содержащее  $\mathcal{R}$ . Строим фильтр  $\Phi(\mathcal{R}')$ . Тогда

$$\mathcal{R} \subseteq \mathcal{R}' \subseteq \Phi(\mathcal{R}').$$

Из максимальной фильтра  $\mathcal{R}$  следует равенство  $\mathcal{R} = \Phi(\mathcal{R}')$ , а значит, и равенство  $\mathcal{R} = \mathcal{R}'$ . Поэтому  $\mathcal{R}$  — максимальное центрированное семейство.  $\square$

Для любого фильтра  $\Phi$  имеет место эквивалентность

$$(A \in \Phi \wedge B \in \Phi) \longleftrightarrow A \cap B \in \Phi.$$

Покажем, что для любого максимального фильтра  $\Phi$  имеет место эквивалентность

$$(A \in \Phi \vee B \in \Phi) \longleftrightarrow A \cup B \in \Phi.$$

Если  $A \in \Phi$  или  $B \in \Phi$ , то, конечно,  $A \cup B \in \Phi$ .

Для доказательства обратной импликации, предположим, что  $A \cup B \in \Phi$ , но  $A \notin \Phi$  и  $B \notin \Phi$ . Тогда в силу максимальной центрированного семейства  $\Phi$  семейства  $\Phi \cup \{A\}$  и  $\Phi \cup \{B\}$  не являются центрированными, поэтому в  $\Phi$  найдутся такие множества  $C$  и  $D$ , что  $A \cap C = \emptyset$  и  $B \cap D = \emptyset$ , поэтому  $\emptyset = (A \cup B) \cap (C \cap D) \in \Phi$ , но это противоречит пункту 1) из определения фильтра.

Покажем, что для любого максимального фильтра  $\Phi$  и любого подмножества  $A$  множества  $U$  либо  $A \in \Phi$ , либо  $\bar{A} \in \Phi$ .

Так как  $A \cup \bar{A} = U \in \Phi$ , то из максимальности фильтра  $\Phi$  следует, что  $A \in \Phi$  либо  $\bar{A} \in \Phi$ .

Докажем, что верно и обратное: если для любого подмножества  $A$  множества  $U$  либо  $A \in \Phi$ , либо  $\bar{A} \in \Phi$ , то  $\Phi$  — максимальный фильтр.

Пусть фильтр  $\Phi'$  содержит фильтр  $\Phi$ . Если  $\Phi' \neq \Phi$ , то найдется такое  $A$ , что  $A \in \Phi'$  и  $A \notin \Phi$ . Тогда  $\bar{A} \in \Phi$ , а значит,  $\bar{A} \in \Phi'$ , поэтому  $\emptyset = A \cap \bar{A} \in \Phi'$ , что невозможно.

Если  $\Phi$  — максимальный фильтр, а  $A$  — такое подмножество множества  $U$ , что для любого  $X$  из  $\Phi$   $A \cap X \neq \emptyset$ , то  $A \in \Phi$ .

Рассмотрим семейство  $\oplus' = \Phi \cup \{A\}$ . Нетрудно показать, что семейство  $\oplus'$  является центрированным, поэтому из максимальности  $\Phi$  следует равенство  $\oplus' = \Phi$ . Поэтому  $A \in \oplus' = \Phi$ .

*Д о к а з а т е л ь с т в о.* теоремы А.Н. Тихонова. Пусть  $U = \prod_{i \in I} U_i$  — прямое произведение компактных топологических пространств, с определенной выше топологией на нем. Покажем, что  $U$  — компактное топологическое пространство. Пусть  $\mathcal{R}_0$  — центрированное семейство замкнутых подмножеств в  $U$ , а  $\mathcal{R}$  — содержащее  $\mathcal{R}_0$  максимальное центрированное семейство подмножеств пространства  $U$ . Для произвольного подмножества  $Y$  пространства  $U$  через  $\bar{Y}$  обозначим замыкание  $Y$ , т.е. пересечение всех замкнутых подмножеств в  $U$ , содержащих  $Y$ . Так как для  $X$  из  $\mathcal{R}_0$  выполняется равенство  $\bar{X} = X$ , то

$$\bigcap_{Y \in \mathcal{R}} \bar{Y} \subseteq \bigcap_{X \in \mathcal{R}_0} X.$$

Поэтому достаточно доказать, что  $\bigcap_{Y \in \mathcal{R}} \bar{Y} \neq \emptyset$ . Для произвольного подмножества  $Z \subseteq U$  и любого  $t \in I$  обозначим через  $Z^t$  образ множества  $Z$  при отображении проектирования  $pr_t$ , т.е.  $Z^t = pr_t(Z)$ .

Пусть  $\mathcal{R}^t$  обозначает множество  $\{\bar{Y}^t \mid Y \in \mathcal{R}\}$ . Покажем, что семейство  $\mathcal{R}^t$  замкнутых подмножеств в  $U_t$  является центрированным.

Пусть  $(\bar{Y}_j^t)_{1 \leq j \leq n}$  — конечное семейство элементов из  $\mathcal{R}^t$ .

Тогда  $(Y_j)_{1 \leq j \leq n}$  — конечное семейство элементов из  $\mathcal{R}$ . В силу центрированности  $\mathcal{R}$   $(\bigcap_{1 \leq j \leq n} Y_j) \neq \emptyset$ . Но  $Y_j \subseteq \prod_{t \in I} Y_j^t$  и

$$\emptyset \neq \bigcap_{1 \leq j \leq n} Y_j \subseteq \bigcap_{1 \leq j \leq n} \prod_{t \in I} Y_j^t = \prod_{t \in I} (\bigcap_{1 \leq j \leq n} Y_j^t),$$

значит,  $\bigcap_{1 \leq j \leq n} Y_j^t \neq \emptyset$ , но тогда и  $\bigcap_{1 \leq j \leq n} \bar{Y}_j^t \neq \emptyset$ .

Значит,  $\mathcal{R}^t$  — центрированное семейство замкнутых множеств в  $U_t$ . В силу компактности  $U_t$  тогда  $\bigcap_{Y \in \mathcal{R}^t} Y \neq \emptyset$ .



Покажем, что

$$\prod_{t \in I} \left( \bigcap_{X \in \mathcal{R}^t} X \right) \subseteq \bigcap_{Y \in \mathcal{R}} \bar{Y}.$$

Пусть

$$f \in \prod_{t \in I} \left( \bigcap_{X \in \mathcal{R}^t} X \right) = \prod_{t \in I} \left( \bigcap_{Y \in \mathcal{R}} \bar{Y}^t \right).$$

Тогда при любом  $t \in I$

$$f(t) \in \bigcap_{Y \in \mathcal{R}} \bar{Y}^t.$$

Пусть  $Y \in \mathcal{R}$ . Покажем, что  $f \in \bar{Y}$ . Для этого достаточно (и необходимо) установить, что для любого открытого множества  $W$ , содержащего  $f$ ,  $W \cap Y \neq \emptyset$ . Каждое открытое множество  $W$  из  $U$  есть объединение открытых множеств  $\Gamma$  вида  $\prod_{t \in I} G_t$ , где при любом  $t \in I$ :  $G_t$  — открытое множество в  $U_t$  и лишь для конечного множества индексов  $t$  множество  $G_t$  отлично от всего  $U_t$  (открытые множества  $\Gamma$  указанного вида образуют базу топологии на  $U$ ). Поэтому найдется такое открытое множество  $\Gamma$  указанного вида, что  $f \in \Gamma \subseteq W$ . Достаточно показать, что  $\Gamma \cap Y \neq \emptyset$ . Итак,  $f \in \Gamma$ ,  $\Gamma = \prod_{t \in I} G_t$ . Пусть  $S$  — такое конечное подмножество множества  $I$ , что при  $t \notin S$ :  $G_t = U_t$ .

Для произвольного  $s \in S$  полагаем

$$\Gamma_s = \left( \prod_{t \in I \setminus \{s\}} X_t \right) \times G_s.$$

Тогда  $\Gamma = \bigcap_{s \in S} \Gamma_s$  и при любом  $s \in S$ :  $f \in \Gamma_s$ . Покажем, что  $\Gamma_s \in \mathcal{R}$ .

Для этого, как было показано выше, достаточно (и необходимо) установить, что для любого  $Z$  из  $\mathcal{R}$ :  $Z \cap \Gamma_s \neq \emptyset$ . Итак, пусть  $Z \in \mathcal{R}$ . Тогда при любом  $t \in I$ :  $f(t) \in \bar{Z}^t$ , в частности, при  $s \in S$ :  $f(s) \in \bar{Z}^s$ . Но  $f(s) \in G_s$  и  $G_s$  — открытое множество, поэтому  $Z^s \cap G_s \neq \emptyset$ . Пусть при любом  $s \in S$ :  $m_s \in Z^s \cap G_s \neq \emptyset$ . Найдется такая функция  $g \in Z$ , что  $g(s) = m_s$ . Но тогда  $g(s) \in G_s$ , значит,  $g \in \Gamma_s$ , поэтому  $g \in \Gamma_s \cap Z$ . Следовательно  $\Gamma_s \cap Z \neq \emptyset$ . Ссылка на одно из выше доказанных свойств максимальных центрированных семейств множеств дает  $\Gamma_s \in \mathcal{R}$ . Но тогда в силу конечности множества  $S$  получаем  $\Gamma = \bigcap_{s \in S} \Gamma_s \in \mathcal{R}$

(напомним, что  $\mathcal{R}$  — фильтр). А так как  $Y \in \mathcal{R}$ , то  $Y \cap \Gamma \neq \emptyset$ . Значит,  $f \in \bar{Y}$ , поэтому

$$\prod_{t \in I} \left( \bigcap_{X \in \mathcal{R}^t} X \right) = \prod_{t \in I} \left( \bigcap_{Y \in \mathcal{R}} \bar{Y}^t \right) \subseteq \bigcap_{Y \in \mathcal{R}} \bar{Y}.$$

Значит,  $\bigcap_{Y \in \mathcal{R}} \bar{Y} \neq \emptyset$ . Выше уже отмечалось, что из последнего следует

$$\bigcap_{X \in \mathcal{R}_0} X \neq \emptyset.$$



Теорема А.Н. Тихонова доказана.  $\square$

Приведем несколько усовершенствованный вариант доказательства теоремы А.Н. Тихонова.

Так как объединение любого линейно упорядоченного отношением включения  $\subseteq$  множества центрированных семейств замкнутых множеств в  $U$  само будет центрированным семейством замкнутых множеств, то для любой цепи центрированных семейств замкнутых множеств в  $P(U)$  существует во множестве всех центрированных семейств замкнутых множеств в  $P(U)$  верхняя грань, поэтому по лемме Цорна любое центрированное семейство замкнутых множеств в  $P(U)$  содержится в некотором максимальном центрированном семействе замкнутых множеств.

По центрированному семейству замкнутых множеств  $\mathcal{R}_0$  построим содержащее его максимальное центрированное семейство замкнутых множеств  $\mathcal{R}$ .

Установим некоторые необходимые для дальнейшего свойства максимального центрированного семейства  $\mathcal{R}$  замкнутых множеств.

1)  $\emptyset \notin \mathcal{R}$ .

2) Докажем, что если  $A$  и  $B$  — замкнутые множества в  $U$ ,  $A \in \mathcal{R}$ ,  $A \subseteq B$ , то  $B \in \mathcal{R}$ . Рассмотрим содержащее  $\mathcal{R}$  семейство  $\mathcal{R}' = \mathcal{R} \cup \{B\}$  замкнутых множеств. Покажем, что оно является центрированным. Если бы это было не так, то в  $\mathcal{R}$  нашлись бы такие множества  $X_1, \dots, X_n$ , что  $B \cap \bigcap_{1 \leq i \leq n} X_i = \emptyset$ , но тогда и  $A \cap \bigcap_{1 \leq i \leq n} X_i = \emptyset$ , что противоречит центрированности семейства  $\mathcal{R}$ . Из максимальной семейства  $\mathcal{R}$  получаем равенство  $\mathcal{R} \cup \{B\} = \mathcal{R}' = \mathcal{R}$ , значит,  $B \in \mathcal{R}$ .

3) Докажем, что имеет место эквивалентность

$$(A \in \Phi \wedge B \in \mathcal{R}) \longleftrightarrow A \cap B \in \mathcal{R}.$$

Если  $A \cap B \in \mathcal{R}$ , то в силу пункта 2)  $A \in \mathcal{R}$  и  $B \in \mathcal{R}$ .

Для доказательства обратного предположим, что  $A \in \mathcal{R}$  и  $B \in \mathcal{R}$  и получим  $A \cap B \in \mathcal{R}$ . Рассмотрим содержащее  $\mathcal{R}$  семейство  $\mathcal{R}' = \mathcal{R} \cup \{A \cap B\}$  замкнутых множеств. Покажем, что оно является центрированным. Если бы это было не так, то в  $\mathcal{R}$  нашлись бы такие множества  $X_1, \dots, X_n$ , что  $A \cap B \cap \bigcap_{1 \leq i \leq n} X_i = \emptyset$ , но это противоречит центрированности семейства  $\mathcal{R}$ . Из максимальной семейства  $\mathcal{R}$  получаем равенство  $\mathcal{R} \cup \{A \cap B\} = \mathcal{R}' = \mathcal{R}$ , значит,  $A \cap B \in \mathcal{R}$ .

4) Докажем, что если  $A$  и  $B$  — замкнутые множества в  $U$ , то имеет место эквивалентность

$$(A \in \mathcal{R} \vee B \in \mathcal{R}) \longleftrightarrow A \cup B \in \mathcal{R}.$$

Если  $A \in \mathcal{R}$  или  $B \in \mathcal{R}$ , то в силу пункта 2)  $A \cup B \in \mathcal{R}$ .

Для доказательства обратного предположим, что  $A \cup B \in \mathcal{R}$ , но  $A \notin \mathcal{R}$  и  $B \notin \mathcal{R}$  и получим противоречие. В силу максимальной центрированного семейства

$\mathcal{R}$  семейства  $\mathcal{R} \cup \{A\}$  и  $\mathcal{R} \cup \{B\}$  замкнутых множеств не являются центрированными. Поэтому в  $\mathcal{R}$  найдутся такие множества  $X_1, \dots, X_n$  и  $Y_1, \dots, Y_m$ , что  $\bigcap_{1 \leq i \leq n} X_i = \emptyset$  и  $\bigcap_{1 \leq j \leq m} Y_j = \emptyset$ . Но тогда

$$(A \cup B) \cap \bigcap_{1 \leq i \leq n} X_i \cap \bigcap_{1 \leq j \leq m} Y_j = \\ \left( A \cap \bigcap_{1 \leq i \leq n} X_i \cap \bigcap_{1 \leq j \leq m} Y_j \right) \cup \left( B \cap \bigcap_{1 \leq i \leq n} X_i \cap \bigcap_{1 \leq j \leq m} Y_j \right) = \emptyset,$$

что противоречит предположению  $A \cup B \in \mathcal{R}$  и центрированности  $\mathcal{R}$ .

5) Докажем, что если  $A$  — замкнутое множество в  $U$ ,  $\mathcal{R}$  — максимальное центрированное семейство замкнутых множеств и для любого  $X$  из  $\mathcal{R}$   $A \cap X \neq \emptyset$ , то  $A \in \mathcal{R}$ .

Рассмотрим семейство  $\mathcal{R}' = \mathcal{R} \cup \{A\}$ . Покажем, что семейство  $\mathcal{R}'$  является центрированным семейством замкнутых множеств, тогда из максимальной  $\mathcal{R}$  получим равенство  $\mathcal{R}' = \mathcal{R}$ . Поэтому  $A \in \mathcal{R}' = \mathcal{R}$ . Если  $X_1, \dots, X_n$  из  $\mathcal{R}$ , то в силу пункта 3)  $\bigcap_{1 \leq i \leq n} X_i \in \mathcal{R}$ , поэтому  $A \cap \bigcap_{1 \leq i \leq n} X_i \neq \emptyset$ .

Пусть  $\mathcal{R}$  — максимальное центрированное семейство замкнутых множеств, содержащее исходное центрированное семейство замкнутых множеств  $\mathcal{R}_0$ .

Если  $Y \in \mathcal{R}$ , то  $CY = \bigcup_{V \in I(Y)} V$ , где  $V$  — множества из базы Тихонова. Тогда  $Y = \bigcap_{CV \in I(Y)} V$ , значит,  $Y \subseteq CV$ , поэтому в силу пункта 2)  $CV \in \mathcal{R}$ . Поэтому

$$\bigcap_{Y \in \mathcal{R}} Y = \bigcap_{\{CV \in \mathcal{R}, V \text{ — из базы топологии Тихонова}\}} CV.$$

Если  $V$  из базы топологии Тихонова, то  $V = \bigcap_{s \in S} V_s$ , где  $S$  — конечное множество, а  $V_s = \prod_{t \in I \setminus \{s\}} U_t \times G_s$ , где  $G_s$  — открытое множество в  $U_s$ . Поэтому

$$CV = \bigcup_{s \in S} CV_s, \quad CV_s = \prod_{t \in I \setminus \{s\}} U_t \times CG_s.$$

Значит,  $(CV_s)^t = U_t$  при  $t \neq s$  и  $(CV_s)^s = CG_s$ . Поэтому  $(CV_s)^t$  — замкнутое множество в  $U_t$ . Значит, замкнуто и множество  $(CV)^t = \bigcup_{s \in S} (CV_s)^t$ , так как  $S$  — конечное множество.

Полагаем

$$\mathcal{R}^t = \{(CV)^t \mid CV \in \mathcal{R} \text{ \& } V \text{ — из базы топологии Тихонова}\}.$$

Покажем, что  $\mathcal{R}^t$  — центрированное семейство замкнутых множеств в  $U_t$ . Пусть  $(CV_j)_{1 \leq j \leq n}$  — конечное семейство множеств из  $\mathcal{R}^t$ . Тогда  $(CV_j)_{1 \leq j \leq n}$  — конечное

семейство множеств из  $\mathcal{R}$ , значит,  $\bigcap_{1 \leq j \leq n} CV_j \neq \emptyset$ . Но

$$\emptyset \neq \bigcap_{1 \leq j \leq n} CV_j \subseteq \bigcap_{1 \leq j \leq n} \prod_{t \in I} (CV_j)^t = \prod_{t \in I} \left( \bigcap_{1 \leq j \leq n} (CV_j)^t \right).$$

Поэтому  $\bigcap_{1 \leq j \leq n} (CV_j)^t \neq \emptyset$ . Значит,  $\mathcal{R}^t$  — центрированное семейство замкнутых множеств в  $\bar{U}_t$ . В силу компактности  $U_t$  получаем

$$\bigcap_{\{CV \in \mathcal{R} \text{ \& } V \text{ — из базы топологии Тихонова}\}} (CV)^t \neq \emptyset.$$

Пусть

$$f \in \prod_{t \in I} \left( \bigcap_{\{CV \in \mathcal{R} \text{ \& } V \text{ — из базы топологии Тихонова}\}} (CV)^t \right).$$

Тогда при любом  $t$  из  $I$ :

$$f(t) \in \left( \bigcap_{\{CV \in \mathcal{R} \text{ \& } V \text{ — из базы топологии Тихонова}\}} (CV)^t \right).$$

Пусть  $CV \in \mathcal{R}$  и  $V$  из базы топологии Тихонова. Покажем, что  $f \in CV$ . Так как  $V = \bigcap_{s \in S} V_s$ ,  $CV = \bigcup_{s \in S} CV_s \in \mathcal{R}$ , то в силу пункта 4 найдется такое  $s \in S$ , что  $CV_s \in \mathcal{R}$ . Пусть  $V_s = \prod_{t \in I \setminus \{s\}} U_t \times G_s$ . Покажем, что

$$f \in CV_s = \prod_{t \in I \setminus \{s\}} U_t \times CG_s.$$

Но это следует из

$$f(s) \in \bigcap_{\{CV \in \mathcal{R} \text{ \& } V \text{ — из базы топологии Тихонова}\}} (CV)^t \subseteq (CV_s)^t = CG_s.$$

Значит,

$$\emptyset \neq \prod_{t \in I} \left( \bigcap_{\{CV \in \mathcal{R} \text{ \& } V \text{ — из базы топологии Тихонова}\}} (CV)^t \right) \subseteq \bigcap_{\{CV \in \mathcal{R} \text{ \& } V \text{ — из базы топологии Тихонова}\}} CV = \bigcap_{Y \in \mathcal{R}} Y \subseteq \bigcap_{X \in \mathcal{R}_0} X.$$

## 11. Дополнение

По мнению ряда специалистов по истории математики, есть достаточно убедительные основания считать, что примитивная математика существовала за 4000 лет до н.э. у египетских и вавилонских плотников и землемеров.

Первые попытки научного осмысления мира традиционно связывают с именем древнегреческого философа и математика Фалеса (Фалес Милетский около 625–547 гг. до н.э.), который первым ввел в математику понятие *доказательства* и доказал ряд геометрических теорем. В частности, ему приписывают доказательства утверждений “диаметр делит круг на две равные части” и “углы при основании равнобедренного треугольника равны”. Конечно, по современным стандартам эти теоремы и их доказательства достаточно несложны, однако заслуга Фалеса состоит в том, что он осознал необходимость доказывать такие, казалось бы “очевидные”, утверждения.

Одним из источников сведений, касающихся “доисторического” периода развития математики, является папирус Ринда, названный по имени его открывателя. Основная часть папируса хранится в Британском музее. Этот свиток представляет собой справочник землемера для решения практических задач. Составлен он примерно в 1550 г. до н.э. писцом по имени Ахмес. Ряд исследователей считает, что папирус Ринда был создан на основе более древних источников.

В папирусе Ринда содержатся решения следующих задач.

- 1) Пример расчета площади прямоугольника земли размером 10 хетов на 2 хета.
- 2) Вычисление площади “круглого поля” с периметром 9 хетов.
- 3) Вычисление площадей полей, имеющих форму треугольника и трапеции.

Математика, как и искусство, — это особый способ познания мира.

На протяжении всей 4-ех тысячелетней истории математики в ней изучались два одновременно далеких и близких понятия — понятие *числа* и понятие *геометрической фигуры*. Понятие числа и прежде всего натурального числа — основной объект изучения арифметики в широком смысле этого слова или теории чисел, а понятие геометрической фигуры — основной объект изучения геометрии. Сразу бросается в глаза принципиальное различие этих двух понятий — каждое натуральное число выступают как далее неделимый объект, в то время, как обычно геометрическая фигура состоит из бесконечного числа совершенно одинаковых точек. Впрочем, и натуральное число  $n$  можно рассматривать как состоящее из  $n$  единиц, однако они “дискретны”, в то время как для геометрических фигур характерна “непрерывность”. Несмотря на это на протяжении по крайней мере последних двух тысяч лет неоднократно предпринимались попытки объединить эти два понятия, связать геометрию с арифметикой, вывести из одного основания всю математику. Одна из первых дошедших до нас попыток объединения этих двух понятий, а значит, и объединения арифметики и

геометрии, относится к VI веку до н.э. Она была предпринята в школе древнегреческого философа и математика Пифагора и ее смысл хорошо выражает приписываемое Пифагору высказывание “Все есть число”.

Сокрушительный удар по этой точке зрения школы Пифагора был нанесен открытием одним из ее членов несоизмеримости диагонали квадрата с его стороной, или, как мы теперь говорим, доказательством несуществования такого рационального числа  $r$ , что  $r^2 = 2$ , т.е. в школе Пифагора в VI веке до н.э. была открыта иррациональность  $\sqrt{2}$  при условии, что такое число существует. Это число нельзя было отнести ни к целым числам, ни к дробям, а в те далекие времена под словом “числа” понимались целые (положительные) числа и их отношения, т.е. по современной терминологии положительные рациональные числа. Длины отрезков выражались числами и получалось, что “*диагональ квадрата не имеет длины*”. Со временем была понята невозможность построения геометрии на основе понятия натурального числа. Древними греками был найден выход — они объявили, что “*числа — это длины*”. Арифметика была сведена к геометрии. Однако это сведение на протяжении длительного времени сдерживало развитие арифметики и алгебры. Это породило идущую от древнегреческих математиков традицию выражать соотношения между любыми величинами в геометрических терминах — *сводить математику к геометрии*. Отзвуки этой традиции мы находим в выражениях *квадрат числа, куб числа, геометрическая прогрессия, среднее геометрическое* и т.д. В “Началах” Евклида была предпринята одна из первых и достаточно удачных попыток дедуктивного изложения известных к тому времени математических фактов — *аксиоматическое* изложение геометрии и части арифметики. Особую роль в развитии алгебры и теории чисел сыграл многотомный труд Диофанта “Арифметика” (III век н.э.).

Уровень развития цивилизации, как в зеркале, отражается в сложности используемых ею чисел. Древнегреческие математики, разрабатывая систему наименований для больших чисел, совершили великий скачок от конечного к бесконечному. Этот революционный переход мы теперь скромно обозначаем тремя маленькими точками после запятой обозначая бесконечный ряд  $\mathbb{N}$  натуральных чисел

$$1, 2, 3, 4, \dots$$

Для древних греков концепция бесконечного ряда натуральных чисел была важным достижением творческой мысли и вдохновения, так как она шла вразрез со всеми накопленными к тому времени естественно-научными знаниями и с философскими представлениями о конечности Вселенной.

Приведем характерное высказывание В.А. Успенского: “*Поистине революционный характер носило осознание древнегреческими математиками бесконечности натурального ряда, точнее создание такого понятия натурального числа, при котором натуральных чисел оказалось бесконечно много. Возникнув как инструмент исследования мира, понятие натурального числа само стало предметом исследований, которые привели к выявлению скрытых свойств этого понятия.*”



Удивительным достижением античной математики было установление бесконечности множества простых чисел. Факт поразительный как по постановке вопроса о бесконечности, хотя и без использования самого слова “бесконечность”, так и по безукоризненной точности формулировки ответа (двадцатое предложение IX книги “Начал” Евклида, “простых чисел существует больше всякого предложенного количества простых чисел”) и по неожиданной простоте доказательства.”

Смелая идея бесконечности открывала широкие возможности в математике, но и приводила к парадоксам. Смысл понятия бесконечности не до конца раскрыт и до сегодняшнего дня.

Теория множеств Г. Кантора продемонстрировала возможность строгого изучения бесконечности, распространила на бесконечные множества понятие количества элементов, обнаружила, что и бесконечные множества могут состоять из разного количества элементов.

Не менее трудно оказалось сделать шаг от положительных чисел к отрицательным. Положительные дроби подробно обсуждаются уже в папирусе Ринда (1500 г. до н.э.). Обозначения для дробей  $a/b$  и современные способы действий с ними восходят к XV–XVI векам. В то же время отрицательные числа были приняты в математике лишь после появления в 1545 году “*Arts Magna*” Джироламо Кардано (1501–1576). И уже в эпоху Возрождения были введены в употребление комплексные числа, которые окончательно утвердились в математике в XIX веке: ирландский математик Уильям Роуэн Гамильтон предложил использовать упорядоченную пару  $\langle a, b \rangle$  для обозначения комплексного числа  $a + bi$ , тем самым лишив мнимую единицу  $i$  “мистического статуса”, а норвежец Гаспар Вессель ввел геометрическое представление комплексных чисел точками плоскости. Великим творением У.Р. Гамильтона являются кватернионы.

С падением древнегреческой цивилизации математические исследования переместились в арабоязычные страны.

Арабские ученые восприняли геометрическое наследие древнегреческих математиков, их критерии строгости. Но они восприняли и идущую от вавилонских писцов традицию составления текстов, содержащих общие методы решения арифметических задач. Знакомы они были и с открытиями индийских математиков, создавших десятичную систему счисления, свободно использовавших отрицательные числа (в отличие от древнегреческих математиков).

Была подготовлена почва для создания алгебры. Зарождение алгебры как науки об уравнениях относят к IX веку. Через несколько столетий исследования по алгебре начались в Италии, а затем и в Западной Европе.

Велика роль уроженца Хивы Мухаммеда ибн Муссы аль-хорезми. Его сочинение “Хисаб ал-джабр вал-мукабала” сыграло особую роль в появлении широко используемых сегодня понятий “алгебра” и “алгоритм”.

Теория квадратных уравнений была известна еще в Древнем Вавилоне. В Италии в XVI веке были получены формулы для решения уравнений 3-ей и 4-ой

изучение комплексных чисел. С этого периода начинается использование буквенной символики, создание современной алгебраической символики (Ф. Виет (1540–1603)). Дальнейшее продвижение в этой области связано с именами Ж.Л. Лагранжа (1736–1813), А. Руффини (1765–1822), Нильса Хенрика Абеля (1802–1829) и Эвариста Галуа (1811–1832).

300 лет тому назад математическое мышление основывалось на геометрии, унаследованной от древних греков и лишь незначительно продвинувшейся за два тысячелетия. В XVII веке началось стремительное и радикальное преобразование математики. Строгий аксиоматический дедуктивный стиль геометрии уступил место интуитивному индуктивному подходу, а чисто геометрические понятия — представлениям о числе и алгебраической операции. Создаются аналитическая геометрия (Р. Декарт (1596–1650), П. Ферма (1601–1665)) и математический анализ (дифференциальное и интегральное исчисления — И. Ньютон (1643–1727), Г.В. фон Лейбниц (1646–1716)). Основные понятия математического анализа — функция и предел. Понятие предела вводит интуитивное представление о непрерывности в жесткие математические рамки.

Можно сказать, что в XVII веке возникла “классическая математика”.

Ко времени Великой французской революции математика достигла расцвета. Значительно возросло число активно занимающихся научными исследованиями. Появилась учебная литература, позволившая знакомиться с новыми достижениями математики. Университеты стали систематически готовить специалистов в области естественных наук и математики.

Возникла необходимость освобождения алгебры от несвойственной ей геометрической терминологии.

Р. Декарт (1596–1650) предложил зафиксировать отрезок  $e$ , назвав его единичным. Тогда произведение чисел  $a$  и  $b$  можно рассматривать не как площадь прямоугольника со сторонами  $a$  и  $b$ , а как длину такого отрезка  $c$ , что  $a : e = c : b$  (теория пропорций была разработана еще древнегреческими математиками). Квадратный корень из  $a$  — среднее геометрическое отрезков  $a$  и  $e$ .

После работ Р. Декарта появилась возможность свободно оперировать с произвольными алгебраическими выражениями, не заботясь об их геометрическом смысле. Со времени Р. Декарта начался длившийся более 200 лет процесс “арифметизации” математики, ее перевода с геометрического на арифметический язык. Итоги этого периода ярко характеризует высказывание Анри Пуанкаре (1854–1912): “*В математике остались лишь натуральные числа и множества натуральных чисел*”.

В 70-х годах XIX века в работах Г. Кантора (1845–1918), К. Вейерштрасса (1815–1897), Р. Дедекинда (1831–1916) и Ш. Мэре (1835–1911, французский математик, построил одновременно с К. Вейерштрассом арифметическую теорию действительного числа) было получено свободное от геометрии определение действительного числа — действительные числа строились исходя из чисел натуральных, они определялись как бесконечные множества рациональных чисел.

Последователи И. Ньютона и Г.В. фон Лейбница чрезвычайно свободно об-

ращались с расплывчатыми понятиями *бесконечно малой* и *бесконечно большой* величин, складывали бесконечные суммы слагаемых по правилам, верным для конечных сумм.

Основные понятия созданного И. Ньютоном и Г.В. Лейбницем исчисления казались туманными математикам, воспитанным на античной строгости. Однако успехи нового исчисления в решении старых, казавшихся неприступными, задач заставляли отбрасывать сомнения. Как девиз того переломного периода звучит призыв Ж. Д'Аламбера (1717–1783) *“Идите вперед, и вера к вам придет”*. Дифференциальное и интегральное исчисления позволили решить самые разнообразные задачи: от расчета траектории артиллерийского снаряда до предсказаний движений планет и комет.

Но основа тогдашнего анализа — понятие *бесконечно малой величины* казалось стоящим на грани бытия и небытия, чем-то вроде нуля, но не совсем нуля.

В конце XVIII века появились первые признаки неблагополучия — некорректное использование бесконечно больших и бесконечно малых величин стало приводить к противоречиям.

В начале XIX века понятия *актуально бесконечно большой* и *бесконечно малой* величин были заменены идеей предела и понятиями *потенциально бесконечно большой* и *бесконечно малой* величин. Велик вклад в это дело Нильса Хенрика Абеля (1802–1829, норвежский математик, один из создателей современных критериев строгости рассуждений в математическом анализе; доказал теорему о неразрешимости в радикалах для уравнений 5-ой степени. Как признание выдающихся математических заслуг Н.Х. Абеля можно рассматривать учреждение Норвежской Академией наук и литературы “Премии Абеля”, которая сегодня является высшей математической наградой), Огюстена Коши (1789–1857, французский математик, поставил математический анализ на фундамент теории пределов), Карла Фридриха Гаусса (1777–1855, крупнейший немецкий математик XIX века).

Недопущение в математику для изучения бесконечных множеств почти 2 тысячи лет держалось на авторитете Аристотеля — в математике господствовала потенциальная бесконечность Аристотеля.

В 1831 году К.Ф. Гаусс заявлял: *“... Я протестую против употребления бесконечной величины как чего-то законченного, что в математике никогда не допустимо. Бесконечность не нужно понимать буквально, когда речь идет собственно о пределе, к которому сколь угодно близко приближаются определенные отношения, когда другие принимаются неограниченно возрастающими.”*

Использование актуальной бесконечности в математике начинается в XVIII веке (бесконечные ряды рассматривались как суммы бесконечного числа слагаемых). Сам К.Ф. Гаусс в XIX веке уже фактически использует актуальную бесконечность в теоретико-числовых исследованиях.

Еще отчетливее это видно в работах немецких математиков Лежена Дирихле (1805–1859), Рихарда Дедекинда (1831–1916), Карла Вейерштрасса (1815–1897),

Георга Кантора (1845–1918) и итальянца Джузеппе Пеано (1858–1932).

До середины XIX века не велось систематических исследований свойств бесконечных множеств. Только в 1851 году была посмертно опубликована книга чешского математика и философа Бернарда Больцано (1781–1848) “Парадоксы бесконечности”. В ней была сделана одна из первых попыток исследования свойств *актуальной бесконечности*.

Георг Кантор, занимаясь теорией тригонометрических рядов, пришел к необходимости изучения множеств на прямой. В частности, у него возник вопрос *о возможности занумеровать элементы произвольного множества на прямой*.

С 1871 по 1874 год Г. Кантор искал доказательство неравномошности квадрата и отрезка. Но ему удалось доказать обратное. В письме Р. Дедекинду он пишет “*Я вижу это, но не верю*”.

Ярким успехом созданной Г. Кантором теории множеств стало полученное в 1873 году Г. Кантором доказательство *несчетности множества трансцендентных чисел*.

Первые примеры трансцендентных чисел были построены в 1844 году французским математиком Жозефом Лиувиллем. Сам термин “*трансцендентное число*” введен Г. Лейбницем, а предположение о их существовании высказано Л. Эйлером (1707–1783).

Величайшим математическим достижением было доказательство в 1882 году Карлом Линдеманом (1852–1939, немецкий математик, научный руководитель Д. Гильберта (1862–1943)) трансцендентности числа  $\pi$  и решение знаменитой проблемы *квадратуры круга*.

История развития математики свидетельствует, что математическая модель часто задается в виде особого языка, предназначенного для описания исследуемого явления. Именно в виде языка в XVII веке возникли дифференциальное и интегральное исчисления. Теория множеств дала универсальную систему понятий, которая охватила все существовавшие к тому времени математические теории. Значение математической строгости не следует преувеличивать и доводить до абсурда: здравый смысл в математике не менее уместен, чем во всякой другой области человеческой деятельности. Во все времена крупные математические идеи опережали господствовавшие стандарты строгости. Великое открытие XVII в. — создание основ анализа бесконечно малых (основ дифференциального и интегрального исчислений) базировалось на туманном понятии “*бесконечно малой*”. Разработанный И. Ньютоном и Г.В. Лейбницем язык не имел точной семантики, которая в удовлетворяющей нас сейчас форме была найдена лишь через 150 лет, но позволял описывать и исследовать важнейшие явления действительности. Такими фундаментальными математическими понятиями, как предел, вероятность, алгоритм и т.д. успешно пользовались, не дожидаясь их уточнения.

Аналогичным образом обстояло дело с основным понятием математики — понятием *доказательства*. Трактат Н. Бурбаки “Начала математики” открывается словами “*Со времен древних греков говорить “математика” — значит, говорить “доказательство”*”.



Так как еще со времен Р. Декарта методами аналитической геометрии математики умели изучение геометрических объектов сводить к изучению действительных чисел, то появилась возможность *“арифметизировать”* и геометрию. Возникло новое *единство математики на арифметическом фундаменте*.

В работах Г. Фреге (Готлоб Фреге (1848–1925) — немецкий математик и логик) предложен способ построения арифметики натуральных чисел на базе понятия множества.

Теория бесконечных множеств, основы которой заложил в XIX веке Г. Кантор, стала на многие годы единым фундаментом арифметики и геометрии, дискретного и непрерывного. Это отражено в ярком высказывании великого немецкого математика Давида Гильберта (1862–1943): *“благодаря гигантской совместной работе Г. Фреге, Р. Дедекинда и Г. Кантора бесконечное было возведено на трон и наслаждалось временем своего полного триумфа. Бесконечное в своем дерзком полете достигло головокружительной высоты успеха”*.

Однако следует заметить, что не все математики безоговорочно принимали новую точку зрения на математику. Вначале открытия Г. Кантора натолкнулись на недоверие и даже антагонизм многих математиков и безразличие со стороны большинства философов. Оппозицию новым взглядам возглавил немецкий математик Леопольд Кронекер (1823–1891), по взглядам которого предмет математики могло быть лишь то, что могло быть получено за конечное число шагов из натуральных чисел. Сама идея рассматривать бесконечность как нечто завершенное (актуальная бесконечность) противоречила господствовавшим взглядам. Отношение ряда математиков к построенным методами теории множеств *“экзотическим примерам”* наглядно выражают слова Ш. Эрмита (1822–1901): *“Я с ужасом отворачиваюсь от этой достойной сожаления язвы непрерывных функций, не имеющих производной ни в одной точке”*.

Теория множеств в конце XIX — начале XX века быстро завоевывала все новые и новые позиции.

На Первом Международном конгрессе математиков, проходившем в 1897 году в швейцарском городе Цюрихе, в докладах видных специалистов по математическому анализу Адольфа Гурвица (1859–1919) и Жака Адамара (1865–1963) приводились многочисленные примеры применения теории множеств.

На Втором Международном конгрессе математиков Давид Гильберт включил под номером 1 в свой знаменитый список из 23 проблем континуум-гипотезу Г. Кантора. На том же конгрессе Анри Пуанкаре (1854–1912) сказал, что *в теории множеств математика обрела совершенно прочный и надежный фундамент, и теперь в математике остаются только натуральные числа и конечные или бесконечные системы таких чисел*. По его мнению, математика стала полностью *арифметизированной* и в ней, наконец, достигнута абсолютная строгость.

Однако, как гласит английская пословица, *“каждая семья имеет свой скелет в шкафу”* — вскоре разразился третий кризис оснований математики.

Благодаря работам Евдокса и Евклида был преодолен первый кризис оснований математики, начало которому положило открытие в школе Пифагора



несоизмеримости диагонали квадрата с его стороной.

Через два тысячелетия К. Вейерштрассу, Г. Кантору, О. Коши К.Ф. Гауссу, Р. Дедекинду, Ш. Мэре, Н.Х. Абелю и др. удалось устранить второй кризис оснований, вызванный бурным развитием дифференциального и интегрального исчисления, недостаточно критическим подходом к операциям над бесконечными рядами и произведениями, лейбницеvским понятием бесконечно малой величины.

А уже через двадцать лет вновь возникли проблемы.

По словам Д. Гильберта, *“произошло нечто, аналогичное тому, что случилось при развитии исчисления бесконечно малых. На радостях по поводу новых богатых результатов стали явным образом недостаточно критически относиться к законности умозаключений; поэтому уже при простом образовании понятий и применении умозаключений, постепенно ставших обычными, выявились противоречия, сначала единичные, а потом все более серьезные... На учение Кантора с различных сторон были произведены бурные нападки. Контрдвижение было столь стремительно, что общепотребительнейшие и плодотворнейшие понятия математики, простейшие и важнейшие ее умозаключения оказались под угрозой и применение их запрещалось”*.

В 1895 году Г. Кантором открыт парадокс, связанный с мощностью множества всех множеств. В 1903 году открыт парадокс Бертрана Рассела (1872–1970): допущение о существовании “безобидного” на первый взгляд множества  $A = \{x \mid x \notin x\}$  ведет к противоречию.

Казалось, все лежало в развалинах, о чем красноречиво свидетельствует высказывание А. Пуанкаре: *“Как могла интуиция до такой степени обмануть нас!”*

В 1883 году Г. Кантор сформулировал вопрос: *можно ли вполне упорядочить множество действительных чисел*, положительный ответ на который получил в 1904 году немецкий математик Эрнест Цермело (1871–1953), доказав, что *любое множество можно вполне упорядочить*. Однако в доказательстве им была использована уже упоминавшаяся выше аксиома выбора, по поводу которой в первой половине XX века было достаточно много весьма жарких споров. Традиционно считается, что именно Цермело ввел в рассмотрение аксиому выбора. В то же время по мнению ряда авторов впервые явная ссылка на аксиому выбора приведена в работе Дж. Пеано по дифференциальным уравнениям, а еще раньше ее в неявном виде уже использовал Г. Кантор.

Приведем яркое высказывание Бертрана Рассела об аксиоме выбора: *“Сначала она кажется очевидной; но чем больше вдумываешься в нее, тем более странными кажутся выводы из этой аксиомы: под конец же перестаешь понимать, что же она означает”*.

Без использования аксиомы выбора мы не можем доказать, что любое бесконечное множество содержит счетное подмножество и равномощно некоторому своему собственному подмножеству.

Без использования аксиомы выбора можно доказать, что счетное множество равномощно своему собственному подмножеству. Пусть  $X$  — счетное множество

и  $f$  — биекция множества  $\mathbb{N}$  натуральных чисел на множество  $X$ . Полагаем  $g(x) = f(f^{-1}(x) + 1)$ , тогда  $g$  — биекция множества  $X$  на свое собственное подмножество. Аналогичное утверждение можно доказать для любого бесконечного вполне упорядоченного множества.

Если известно, что множество  $U$  равномощно своему собственному подмножеству  $V$  и  $f$  — биекция  $U$  на  $V$ , то пусть  $a \in U \setminus V$ , тогда полагаем  $g(1) = a$ ,  $g(n+1) = f(g(n))$ . Пусть  $T = g(\mathbb{N})$ . Тогда  $T$  — счетное подмножество множества  $U$ .

Предположение, что любое несчетное множество точек прямой равномощно множеству всех точек прямой называется континуум-гипотезой. Эта гипотеза высказана Г. Кантором.

До Э. Цермело в 1902 году итальянский математик Б. Леви отмечал необходимость аксиомы типа аксиомы выбора. Однако в явном виде аксиома выбора была сформулирована в 1904 году Э. Цермело и использована в доказательстве возможности вполне упорядочить любое множество.

Сомнения по поводу аксиомы выбора приводят к вопросу: “Можно ли выбор осуществлять бесконечное число раз? Не потребуется ли для этого бесконечное время?”

Трудно переоценить значение теории множеств для таких математических дисциплин, как топология. Как самостоятельная математическая дисциплина топология оформилась в начале XX века. Однако некоторые топологические вопросы рассматривал еще Г. Лейбниц, который называл топологию *Analysis Situs*, а затем Л. Эйлер.

Л. Эйлеру приписывают формулу Р. Декарта для выпуклых многогранников  $F + V = E + 2$ . С именем Л. Эйлера связана и проблема семи мостов в Кенигсберге на реке Преголя: можно ли пройти все их последовательно, не вступая ни на один из них дважды.

Сегодня теория множеств лежит в основании большинства разделов классической математики. Группа французских математиков, известная под псевдонимом Николя Бурбаки, на протяжении нескольких десятилетий осуществляет попытку построить все здание математики на теоретико-множественном фундаменте. Эта попытка оказала большое влияние на развитие математики в XX веке. Многотомный трактат Николя Бурбаки “Элементы математики” начинается с книги “Теория множеств”.

Во второй половине XX века широкое распространение в математике получила точка зрения, выраженная в высказывании Николя Бурбаки — *существует все, что непротиворечиво*.

Беспокойство по поводу оснований математики чаще всего возникает в критические моменты, когда кажется, что основополагающие идеи становятся шаткими, и математики вынуждены проверять их.

Проверка идеи бесконечно малых была проведена спустя много лет после разработки дифференциального и интегрального исчислений И. Ньютоном и Г.В. фон Лейбницем.

Характерная задача для проблем, возникающих при перестройке оснований

математики: как, сохранив полезную надстройку, отделаться от бесконечно малых, отдав предпочтение более ясным идеям? В XIX веке О. Коши и его последователи решили эту проблему на основе понятия предела. Бесконечно малые — не единственное математическое понятие, которое нужно было либо узаконить, либо отвергнуть. Мнимые числа дают другой пример.

Как сказал У.В. Куайн (1908–2000) *“Если кто-то проявляет беспокойство по поводу оснований математики, то не значит ли это, что стандарты научной строгости стали суровыми?”*

Следует заметить без каких-либо комментариев, что огромное влияние на направление математических исследований в конце XIX в., которое продолжалось и в XX в., оказал Георг Фридрих Бернгард Риман (1826–1866).

Значительное влияние на выработку различных точек зрения на проблемы существования в математике оказали работы специалистов по математической логике и, прежде всего, одного из величайших логиков не только XX века, но и всего последнего двухтысячелетнего периода развития математики Курта Геделя (1906–1978), английского математика и логика Альфреда Уайтхеда (1861–1947), одного из крупнейших специалистов в области математической логики и оснований математики американского математика Вилларда Куайна (1908–2000), американского математика польского происхождения Альфреда Тарского (1902–1983), американского математика Пауля Дж. Коэна и др.

На регулярно возникающий у студентов вопрос “Зачем все это нужно?” трудно дать достаточно убедительный (для обеих сторон) ответ. Приведем лишь один, на наш взгляд, достаточно показательный исторический пример.

В 1910 году математик Освальд Веблен и физик Джеймс Джинс обсуждали реформу учебного плана по математике в Принстонском университете. “Можно обойтись без теории групп, — сказал Джинс, — этот раздел никогда не принесет какой-либо пользы физике”. Однако теорию групп продолжали преподавать. Очень скоро именно теория групп стала центральным предметом для тех, кто стремится раскрыть тайны элементарных частиц. Причем именно принстонские профессора Г. Вейль и Е. Вигнер стали пионерами теоретико-группового направления в физике двадцатых годов.

Не следует столь безапелляционно высказываться по вопросам, стоящим вне твоей узкой компетенции. Как свидетельствует история, будущее науки, как впрочем и многих других областей человеческой деятельности, предсказать практически невозможно.

Трудно удержаться от комментариев по вопросу преподавания математики, особенно в школе. Начиная с начала XX столетия ужасающее впечатление на многих математиков производила пропасть, существующая между школьной и современной математикой.

Однако вопрос слишком сложен, чтобы его можно было обсуждать на страницах учебного пособия. Сложность проблемы хорошо отражает вопрос Х. Фройденшталя (H. Freudenthal) “Обучение современной математике или современное обучение математике?” Как пишут Г. Радемахер и О. Теплиц в своей известной книге “Числа и фигуры”, “Настоящая математика заключается не в

нагромождении искусственных вычислительных приемов, а в умении получать нетривиальные результаты путем размышления при минимуме применяемого аппарата”. Но это тема для отдельного разговора.

## ГЛАВА II.

# ЛОГИКА И ИСЧИСЛЕНИЕ ВЫСКАЗЫВАНИЙ

### 1. Алфавиты. Слова

**Определение 1.1.** *Алфавитом называется любое непустое множество  $\Sigma$  символов. Элементы множества  $\Sigma$  называются символами или буквами данного алфавита.*

Никаких ограничений на природу элементов множества  $\Sigma$  (символов алфавита) мы не накладываем, единственное предположение относительно  $\Sigma$  состоит в том, что мы должны уметь распознавать каждый символ из  $\Sigma$  как тот же самый при каждом из его вхождений и отличать его от всех других символов из  $\Sigma$ , т.е. предполагается, что различия неодинаковых символов значительно превосходят мелкие различия одинаковых символов. Символы из  $\Sigma$  рассматриваются как простые знаки, а не как символы, которые что-либо означают. Символы алфавита  $\Sigma$  считаются элементарными знаками, далее неделимыми. Например, если  $W$  и  $V$  входят в  $\Sigma$ , то мы считаем, что  $W$  — это элементарный объект, далее неделимый, в частности, не считаем, что  $W$  — это два раза повторенное  $V$ .

**Определение 1.2.** *Словом или выражением в алфавите  $\Sigma$  называется произвольная конечная (возможно пустая) последовательность  $w_1 w_2 \dots w_n$  символов из  $\Sigma$ , т.е.  $n \geq 0$  и при любом  $i$  ( $1 \leq i \leq n$ )  $w_i \in \Sigma$ . Число  $n$  называется длиной слова  $w_1 w_2 \dots w_n$ .*

Длину произвольного слова  $X$  будем обозначать через  $|X|$ . Пустое слово — это слово длины 0, будем его обозначать через  $\Lambda$  или через 1, если это не приведет к путанице.

Пусть  $X$  — это слово  $w_1 w_2 \dots w_n$  ( $w_i \in \Sigma$ ,  $i = 1, \dots, n$ ), а  $Y$  — это слово  $v_1 v_2 \dots v_m$  ( $v_i \in \Sigma$ ,  $i = 1, \dots, m$ ).

**Определение 1.3.** *Слова  $X$  и  $Y$  называются графически равными, если  $n = m$  и при любом  $i$  ( $i = 1, \dots, n$ )  $w_i$  и  $v_i$  один и тот же символ из  $\Sigma$ .*



Утверждение “слова  $X$  и  $Y$  равны графически” будем записывать в виде

$$X = Y.$$

**Определение 1.4.** Произведением (соединением, сочленением, конкатенацией) слов  $X$  и  $Y$  называется слово  $XY$ , т.е. если  $X$  — это слово  $w_1w_2 \dots w_n$ , а  $Y$  — это слово  $v_1v_2 \dots v_m$ , то  $XY$  — это слово

$$w_1w_2 \dots w_nv_1v_2 \dots v_m.$$

Очевидно, что  $|XY| = |X| + |Y|$  и  $X\Lambda = \Lambda X = X$ .

Отметим следующее очевидное свойство: если  $X = Y$ , а  $Z$  — любое слово, то

$$XZ = YZ \quad \text{и} \quad ZX = ZY$$

и обратно, если

$$XZ = YZ \quad \text{или} \quad ZX = ZY,$$

то  $X = Y$ .

**Определение 1.5.** Слово  $X$  называется подсловом слова  $Y$ , если найдутся такие слова  $U$  и  $V$ , что выполняется равенство  $Y = UXV$ . При этом, если слово  $U$  пусто, т.е. выполняется равенство  $Y = XV$ , то слово  $X$  называется **началом** слова  $Y$ . Если же пусто слово  $V$ , т.е. выполняется равенство  $Y = UX$ , то слово  $X$  называется **концом** слова  $Y$ .

**Лемма 1.1.** Если  $X, Y, Z, V$  — слова в алфавите  $\Sigma$  и  $XY = ZV$ , то для некоторого слова  $P$  либо  $X = ZP$  и  $V = PY$ , либо  $Z = XP$  и  $Y = PV$ .

*Доказательство.* Если  $|Z| \leq |X|$ , то, очевидно, найдется такое слово  $P$  (возможно пустое), что  $X = ZP$ , но тогда  $ZPY = ZV$  и, значит,  $V = PY$ . В случае, когда  $|X| \leq |Z|$ , совершенно аналогично показываем, что для некоторого слова  $P$

$$Z = XP \quad Y = PV.$$

□

**Определение 1.6.** Пусть  $*$   $\notin \Sigma$ . Вхождением слова  $Y$  в слово  $X$  называется слово  $V$  вида  $X_1 * Y * X_2$  при условии, что  $X = X_1 Y X_2$ .

**Определение 1.7.** Результатом замены данного вхождения  $V = X_1 * Y * X_2$  слова  $Y$  в слово  $X$  на слово  $Z$  называется слово  $X_1 Z X_2$ .

Ясно, что одно и то же слово  $Y$  может иметь более одного вхождения в слово  $X$ , поэтому следует говорить о замене *данного* вхождения  $V$  слова  $Y$  в слово  $X$  на слово  $Z$ , а не просто о замене слова  $Y$  в слове  $X$  на слово  $Z$ . В частности, если  $Y$  — пустое слово, то вхождение  $V$  слова  $Y$  в слово  $X$  имеет вид  $X_1 * X_2$ ,

и тогда результат замены вхождения  $V$  слова  $Y$  в слово  $X$  на слово  $Z$  — это слово  $X_1 Z X_2$ .

Если слово  $Y$  состоит из одного символа, т.е.  $Y$  — это некоторое  $\alpha$  ( $\alpha \in \Sigma$ ), то вхождение  $V$  слова  $Y$  в слово  $X$  называется *вхождением символа (буквы)  $\alpha$  в слово  $X$* .

Если  $\alpha$  — символ алфавита  $\Sigma$ , а  $X$  и  $Z$  — слова в алфавите  $\Sigma$ , то *результат одновременной замены каждого вхождения символа  $\alpha$  в слово  $X$  на слово  $Z$*  обозначается через

$$X_\alpha [Z].$$

Аналогично, если  $\alpha_1, \dots, \alpha_n$  — попарно различные символы из  $\Sigma$ , а  $X, Z_1, \dots, Z_n$  — слова в алфавите  $\Sigma$ , то *результат одновременной замены всех вхождений  $\alpha_1, \dots, \alpha_n$  соответственно на слова  $Z_1, \dots, Z_n$*  называется *результатом подстановки  $Z_1, \dots, Z_n$  вместо  $\alpha_1, \dots, \alpha_n$*  и обозначается через  $X_{\alpha_1, \dots, \alpha_n} [Z_1, \dots, Z_n]$ .

## 2. Логика Высказываний

В этом параграфе будет рассмотрен один из простейших языков математической логики — **язык Логика Высказываний**.

Произвольный логический язык  $L$  считается заданным, если выполнены следующие условия:

- (1) задан алфавит  $\Sigma$  языка, т.е. некоторое множество символов — символов языка  $L$ . Слова в алфавите  $\Sigma$ , т.е. конечные последовательности символов из  $\Sigma$ , называются *выражениями языка  $L$* ;
- (2) определено подмножество  $F$  множества всех выражений языка  $L$ ; элементы этого множества  $F$  называются *формулами*.

Если имеется эффективная процедура, позволяющая по произвольному выражению языка  $L$  определить, является ли оно формулой, то говорят, что  $L$  — язык с эффективным понятием формулы.

**Алфавит  $\Sigma_{\text{ЛВ}}$  языка  $L_{\text{ЛВ}}$  Логика Высказываний** является объединением трех множеств символов:  $\Sigma_1, \Sigma_2, \Sigma_3$ .

(i) Множество  $\Sigma_1 = \{A_1, A_2, \dots\}$  — счетное множество *пропозициональных переменных*.

Каждый элемент  $A_i$  множества  $\Sigma_1$  называется *пропозициональной переменной* или *переменным высказыванием*. Смысл этого названия будет ясен из дальнейшего употребления элементов множества  $\Sigma_1$ .

(ii) Множество  $\Sigma_2 = \{\neg, \vee, \&, \rightarrow\}$  состоит из четырех символов  $\neg, \vee, \&$  и  $\rightarrow$ .

Символ  $\neg$  называется *отрицанием*, символ  $\vee$  — *дизъюнкцией*, символ  $\&$  — *конъюнкцией*, а символ  $\rightarrow$  — *импликацией*.

Эти четыре символа называются *пропозициональными или логическими связками*, причем  $\neg$  — одноместной связкой, а  $\vee$ ,  $\&$  и  $\rightarrow$  — двуместными связками.

(iii) Множество  $\Sigma_3$  состоит из двух технических символов: ( — левая скобка и ) — правая скобка.

Итак, алфавит  $\Sigma_{ЛВ}$  языка  $L_{ЛВ}$  **Логики Высказываний** — это

$$\Sigma_1 \cup \Sigma_2 \cup \Sigma_3.$$

**Формулы языка  $L_{ЛВ}$ .** Понятие *формулы* языка  $L_{ЛВ}$  определяется следующими четырьмя пунктами:

- (i) каждая пропозициональная переменная  $A_i$  — *формула* языка  $L_{ЛВ}$ , называемая *атомной* или *элементарной формулой*;
- (ii) если  $A$  и  $B$  — формулы языка  $L_{ЛВ}$ , то и следующие выражения являются формулами языка  $L_{ЛВ}$ :

$$(\neg A), (A \vee B), (A \& B), (A \rightarrow B).$$

- (iii) выражение в алфавите языка  $L_{ЛВ}$  является формулой этого языка тогда и только тогда, когда это следует из пунктов (i) и (ii).

Формула  $(\neg A)$  называется *отрицанием* формулы  $A$  и читается “не  $A$ ” или “отрицание  $A$ ”, формула  $(A \vee B)$  называется “*дизъюнкцией  $A, B$* ” и читается “*дизъюнкция  $A, B$* ” или “ *$A$  или  $B$* ”, формула  $(A \& B)$  называется “*конъюнкцией  $A, B$* ” и читается “*конъюнкция  $A, B$* ” или “ *$A$  и  $B$* ”, формула  $(A \rightarrow B)$  называется “*импликацией  $A, B$* ” и читается “ *$A$  влечет  $B$* ” или “*из  $A$  следует  $B$* ”.

**Множество всех формул языка  $L_{ЛВ}$**  будем обозначать через  $F_{ЛВ}$ .

Приведенное определение понятия формулы дает следующий способ доказательства теорем о формулах языка  $L_{ЛВ}$  — **доказательство индукцией по формулам**.

Суть его заключается в следующем: чтобы доказать, что каждая формула языка  $L_{ЛВ}$  обладает свойством  $\mathcal{D}$ , достаточно показать, что

- (i) каждая элементарная формула языка  $L_{ЛВ}$  обладает свойством  $\mathcal{D}$ ;
- (ii) если формулы  $A$  и  $B$  обладают свойством  $\mathcal{D}$ , то и формулы

$$(\neg A), (A \vee B), (A \& B), (A \rightarrow B)$$

обладают свойством  $\mathcal{D}$ .

Определим теперь одно из основных понятий математической логики — понятие **интерпретации**.

**Определение 2.1.** Интерпретацией языка  $L_{ЛВ}$  назовем любое отображение  $\varphi$  множества пропозициональных переменных  $\Sigma_1 = \{A_1, A_2, \dots\}$  этого языка  $L_{ЛВ}$  во множество истинностных значений  $\{И, Л\}$ .

Будем говорить, что интерпретация  $\varphi$  задает истинностные значения для пропозициональных переменных языка  $L_{ЛВ}$ .

Пусть  $\varphi$  — произвольная интерпретация языка  $L_{ЛВ}$ . Распространим  $\varphi$  на множество  $F_{ЛВ}$  всех формул языка  $L_{ЛВ}$  **Логики Высказываний**, т.е. каждой формуле  $\mathcal{A}$  из множества  $F$  сопоставим истинностное значение  $\varphi(\mathcal{A}) \in \{И, Л\}$ .

Каждой  $n$ -местной логической (пропозициональной) связке  $\alpha$  ( $n = 1, 2$ ) сопоставим некоторую  $n$ -местную функцию  $H_\alpha$ , определенную на множестве истинностных значений  $\{И, Л\}$  и принимающую значения в том же множестве.

Традиционно функции  $H_\alpha$  задаются с помощью таблиц, которые называются **истинностными таблицами**.

$A_1$	$H_{\neg}(A_1)$
И	Л
Л	И

$A_1$	$A_2$	$H_{\vee}(A_1, A_2)$
И	И	И
И	Л	И
Л	И	И
Л	Л	Л

$A_1$	$A_2$	$H_{\&}(A_1, A_2)$
И	И	И
И	Л	Л
Л	И	Л
Л	Л	Л

$A_1$	$A_2$	$H_{\rightarrow}(A_1, A_2)$
И	И	И
И	Л	Л
Л	И	И
Л	Л	И

Определим значение  $\varphi$  для произвольной формулы из множества  $F_{ЛВ}$  языка  $L_{ЛВ}$  индукцией по построению формул.

Заметим, что  $\Sigma_1 \subset F_{ЛВ}$ .

(i) *Атомная или элементарная формула*  $\Phi$  языка  $L_{ЛВ}$  — это просто любая пропозициональная переменная  $A_i$ , поэтому для любой элементарной формулы  $\Phi$  истинностное значение  $\varphi(\Phi)$  уже определено.

(ii) Если формула  $\Phi$  языка  $L_{ЛВ}$  имеет один из следующих видов:

$$(\neg \mathcal{A}), (\mathcal{A} \vee \mathcal{B}), (\mathcal{A} \& \mathcal{B}), (\mathcal{A} \rightarrow \mathcal{B}),$$

где  $\mathcal{A}$  и  $\mathcal{B}$  — формулы языка  $L_{ЛВ}$ , то истинностное значение  $\varphi(\Phi)$  определяем следующими равенствами

$$\begin{aligned} \varphi(\neg \mathcal{A}) &= H_{\neg}(\varphi(\mathcal{A})), \\ \varphi(\mathcal{A} \vee \mathcal{B}) &= H_{\vee}(\varphi(\mathcal{A}), \varphi(\mathcal{B})), \\ \varphi(\mathcal{A} \& \mathcal{B}) &= H_{\&}(\varphi(\mathcal{A}), \varphi(\mathcal{B})), \\ \varphi(\mathcal{A} \rightarrow \mathcal{B}) &= H_{\rightarrow}(\varphi(\mathcal{A}), \varphi(\mathcal{B})). \end{aligned}$$

Итак, любую интерпретацию  $\varphi$  языка  $L_{ЛВ}$ , т.е. любое отображение

$$\varphi : \Sigma_1 \rightarrow \{И, Л\},$$

множества пропозициональных переменных языка  $L_{ЛВ}$  во множество истинностных значений, можно естественным образом продолжить до отображения

$$\varphi : F_{ЛВ} \rightarrow \{И, Л\}$$

множества  $F_{ЛВ}$  всех формул языка  $L_{ЛВ}$  во множество  $\{И, Л\}$  истинностных значений.

**Определение 2.2.** Для произвольной интерпретации  $\varphi$  и любой формулы  $A$  языка  $L_{ЛВ}$  истинностное значение  $\varphi(A)$  будем называть **истинностным значением** формулы  $A$  в интерпретации  $\varphi$ . Если при этом  $\varphi(A) = И$ , то будем говорить, что формула  $A$  **истинна** в интерпретации  $\varphi$ , а если  $\varphi(A) = Л$ , то будем говорить, что формула  $A$  **ложна** в интерпретации  $\varphi$ .

**Определение 2.3.** Формула  $A$  языка  $L_{ЛВ}$  называется **выполнимой**, если существует интерпретация, в которой эта формула истинна.

**Определение 2.4.** Множество формул  $\Gamma$  языка  $L_{ЛВ}$  называется **совместным**, если существует интерпретация, в которой все формулы из этого множества истинны.

**Замечание.** Для произвольного множества формул  $\Gamma$  языка  $L_{ЛВ}$  и для любой интерпретации  $\varphi$  запись

$$\varphi(\Gamma) = И$$

будет служить сокращением для утверждения “все формулы множества  $\Gamma$  истинны в интерпретации  $\varphi$ .”

**Определение 2.5.** Формула  $A$  языка  $L_{ЛВ}$  называется **тождественно истинной**, если она истинна в любой интерпретации этого языка.

**Замечание.** Запись  $\models A$  будет служить сокращением для утверждения “формула  $A$  является тождественно истинной.”

**Определение 2.6.** Формулы  $A$  и  $B$  языка  $L_{ЛВ}$  называются **равносильными** или **эквивалентными**, если для любой интерпретации  $\varphi$  этого языка выполняется равенство

$$\varphi(A) = \varphi(B).$$



**Определение 2.7.** Формула  $A$  языка  $L_{ЛВ}$  называется **логическим следствием** множества формул  $\Gamma$  этого языка  $L_{ЛВ}$ , если для любой интерпретации  $\varphi$ , в которой все формулы из этого множества  $\Gamma$  истинны, истинна и формула  $A$ .

**Замечание.** Запись  $\Gamma \models A$  будет служить сокращением для утверждения “формула  $A$  является логическим следствием множества формул  $\Gamma$ .”

**Определение 2.8.** Множество формул  $\Gamma$  языка  $L_{ЛВ}$  назовем **локально совместным**, если любое его конечное подмножество совместно.

**Определение 2.9.** Формула  $A$  языка  $L_{ЛВ}$  называется **локальным логическим следствием** множества формул  $\Gamma$  этого языка  $L_{ЛВ}$ , если она является логическим следствием некоторого конечного подмножества  $\Gamma_0$  множества  $\Gamma$ .

**Замечание.** Запись  $\Gamma \models_{fin} A$  будет служить сокращением для утверждения “формула  $A$  является локальным логическим следствием множества формул  $\Gamma$ .”

**Определение 2.10.** Множество формул  $\Gamma$  языка  $L_{ЛВ}$  назовем **локально полным**, если оно локально совместно и для любой формулы  $A$  языка  $L_{ЛВ}$  либо  $\Gamma \models_{fin} A$ , либо  $\Gamma \models_{fin} (\neg A)$ .

**Замечание.** Если  $\Gamma$  — локально совместное множество формул, то не существует такой формулы  $A$ , что  $\Gamma \models_{fin} A$  и  $\Gamma \models_{fin} (\neg A)$ . В самом деле, предположим, что существует такая формула  $A$ , что  $\Gamma \models_{fin} A$  и  $\Gamma \models_{fin} (\neg A)$ . В соответствии с определением найдутся такие конечные подмножества  $\Gamma_1$  и  $\Gamma_2$  множества  $\Gamma$ , что  $\Gamma_1 \models A$  и  $\Gamma_2 \models (\neg A)$ . Тогда  $\Gamma_1 \cup \Gamma_2 \models (A \& (\neg A))$ . Значит, множество  $\Gamma_1 \cup \Gamma_2$  не является совместным, что противоречит предположению о локальной совместности множества  $\Gamma$ .

**Теорема о локальном пополнении.** Для любого локально совместного множества формул  $\Gamma$  языка  $L_{ЛВ}$  **Логики Высказываний** существует такое локально полное множество формул  $\Gamma^*$  языка  $L_{ЛВ}$ , что

$$\Gamma \subseteq \Gamma^*.$$

**Д о к а з а т е л ь с т в о.** Так как алфавит языка  $L_{ЛВ}$  **Логики Высказываний** счетен, то счетным является и множество  $F_{ЛВ}$  всех формул **Логики Высказываний**.

Пусть  $F_{ЛВ} = (\Phi_n)_{n \in \mathbb{N}}$ .

Определим последовательность  $(\Gamma_n)_{n \in \mathbb{N}}$  множеств формул.

Полагаем

$$\Gamma_1 \Rightarrow \Gamma.$$

Если множество  $\Gamma_n$  уже определено, то полагаем

$$\Gamma_{n+1} \Rightarrow \begin{cases} \Gamma_n \cup \{\Phi_n\}, & \text{если } \Gamma_n \models_{fin} \Phi_n \\ \Gamma_n \cup \{\neg\Phi_n\}, & \text{если } \Gamma_n \not\models_{fin} \Phi_n \end{cases}.$$

Индукцией по  $n$  докажем, что каждое из множеств формул  $\Gamma_n$  является локально совместным.

Так как  $\Gamma_1 \Rightarrow \Gamma$ , то множество формул  $\Gamma_1$  является локально совместным по условию теоремы.

Предположим, что уже доказана локальная совместность множества формул  $\Gamma_n$ . Докажем локальную совместность множества формул  $\Gamma_{n+1}$ .

Если  $\Gamma_n \models_{fin} \Phi_n$ , то  $\Gamma_{n+1} = \Gamma_n \cup \{\Phi_n\}$ .

Ясно, что достаточно доказать совместность любого конечного множества вида  $\Gamma' \cup \{\Phi_n\}$ , где  $\Gamma'$  — конечное подмножество множества  $\Gamma_n$ . Пусть  $\Gamma''$  — такое конечное подмножество множества  $\Gamma_n$ , что  $\Gamma'' \models \Phi_n$ . Для конечного подмножества  $\Gamma' \cup \Gamma''$  локально совместного множества формул  $\Gamma_n$  существует интерпретация  $\varphi$  такая, что  $\varphi(\Gamma' \cup \Gamma'') = \text{И}$ . Тогда  $\varphi(\Phi_n) = \text{И}$  и  $\varphi(\Gamma' \cup \{\Phi_n\}) = \text{И}$ . Значит, множество  $\Gamma' \cup \{\Phi_n\}$  совместно, поэтому в рассматриваемом случае множество  $\Gamma_{n+1}$  локально совместно.

Если  $\Gamma_n \not\models_{fin} \Phi_n$ , то  $\Gamma_{n+1} = \Gamma_n \cup \{\neg\Phi_n\}$ .

Если множество формул  $\Gamma_{n+1}$  не является локально совместным, то найдется такое конечное подмножество  $\Gamma'$  множества  $\Gamma_n$ , что множество  $\Gamma' \cup \{\neg\Phi_n\}$  несовместно, значит,  $\Gamma' \models \Phi_n$ , поэтому  $\Gamma_n \models_{fin} \Phi_n$ . Но последнее противоречит предположению  $\Gamma_n \not\models_{fin} \Phi_n$  и сделанному выше замечанию. Значит, и в этом случае множество формул  $\Gamma_{n+1}$  является локально совместным.

Тем самым доказано, что при любом  $n$  множество формул  $\Gamma_n$  является локально совместным.

Полагаем

$$\Gamma^* \Rightarrow \bigcup_{n=1}^{\infty} \Gamma_n.$$

Покажем, что  $\Gamma^*$  — локально полное множество формул и

$$\Gamma \subseteq \Gamma^*.$$

Последнее очевидно, так как

$$\Gamma = \Gamma_1 \subseteq \Gamma^*.$$

Если бы множество формул  $\Gamma^*$  не было локально совместным, то нашлось бы **конечное** несовместное множество формул  $T \subseteq \Gamma^*$ .

Так как

$$\Gamma_1 \subseteq \Gamma_2 \subseteq \dots \subseteq \Gamma_n \subseteq \Gamma_{n+1} \subseteq \dots,$$

то найдется такое число  $n$ , что  $T \subseteq \Gamma_n$ . Но это противоречит уже установленной локальной совместности множества формул  $\Gamma_n$ .

Значит,  $\Gamma^*$  — локально совместное множество формул.

Пусть  $A$  — произвольная формула. Тогда найдется такое число  $n$ , что  $A \in \Phi_n$ .

Если  $\Gamma_n \models_{fin} \Phi_n$ , то  $\Gamma^* \models_{fin} \Phi_n$ , а значит,  $\Gamma^* \models_{fin} A$ .

Если же  $\Gamma_n \not\models_{fin} \Phi_n$ , то  $\neg \Phi_n \in \Gamma_{n+1}$ , поэтому  $\Gamma_{n+1} \models_{fin} \neg \Phi_n$ , значит,  $\Gamma^* \models_{fin} \neg \Phi_n$ , т.е.  $\Gamma^* \models_{fin} \neg A$ .

Итак доказано, что  $\Gamma^*$  — локально полное множество формул языка  $L_{ЛВ}$  такое, что  $\Gamma \subseteq \Gamma^*$ .  $\square$

**Теорема компактности.** Множество формул  $\Gamma$  языка  $L_{ЛВ}$  является совместным тогда и только тогда, когда оно является локально совместным, т.е. совместно любое его конечное подмножество.

*Доказательство.* Если множество формул  $\Gamma$  языка  $L_{ЛВ}$  является совместным, то, очевидно, является совместным и любое его подмножество. В частности, является совместным и любое конечное подмножество множества формул  $\Gamma$ . Значит,  $\Gamma$  локально совместно.

Обратно, предположим, что множество  $\Gamma$  локально совместно, т.е. любое его конечное подмножество является совместным. Докажем, что тогда совместно и все множество  $\Gamma$ . Мы дадим два доказательства этого важного факта, чтобы в этой достаточно простой ситуации продемонстрировать общие методы, работающие в более сложных логических исчислениях, чем Исчисление Высказываний.

**Первое доказательство.**

По теореме о локальном пополнении существует локально полное множество формул  $\Gamma^*$  такое, что  $\Gamma \subseteq \Gamma^*$ .

Покажем, что множество формул  $\Gamma^*$  является совместным. Отсюда, конечно, сразу будет следовать совместность и множества формул  $\Gamma$ .

Построим интерпретацию  $\varphi$  такую, что  $\varphi(\Gamma^*) = И$ .

Полагаем для произвольной пропозициональной переменной  $A_n$

$$\varphi(A_n) = \begin{cases} И, & \text{если } \Gamma^* \models_{fin} A_n, \\ Л, & \text{если } \Gamma^* \models_{fin} \neg A_n. \end{cases}$$

Напомним, что  $\Gamma^*$  — локально полное множество формул, поэтому для любой формулы  $A$

$$\Gamma^* \models_{fin} A \quad \text{или} \quad \Gamma^* \models_{fin} \neg A,$$

но не то и другое одновременно, в частности, это верно и для произвольной пропозициональной переменной  $A_n$ . Поэтому интерпретация  $\varphi$  определена корректно.

Обычным образом продолжаем отображение  $\varphi$ , заданное на множестве  $\Sigma_1$  пропозициональных переменных, до отображения, заданного на множестве  $F_{ЛВ}$  всех формул языка  $L_{ЛВ}$  Логике Высказываний.

Индукцией по построению формул докажем, что для произвольной формулы  $\mathcal{A}$  имеет место эквивалентность:

$$\Gamma^* \models_{fin} \mathcal{A} \iff \varphi(\mathcal{A}) = \text{И.}$$

(i) Для элементарных формул  $\mathcal{A}$  указанная эквивалентность имеет место по определению интерпретации  $\varphi$ .

(ii) Предположим, что указанная эквивалентность имеет место для формул  $\mathcal{A}$  и  $\mathcal{B}$  и докажем, что тогда она выполняется и для формул

$$\begin{aligned} (\neg \mathcal{A}), \quad (\mathcal{A} \& \mathcal{B}), \\ (\mathcal{A} \vee \mathcal{B}), \quad (\mathcal{A} \rightarrow \mathcal{B}). \end{aligned}$$

Так как

$$\Gamma^* \models_{fin} \neg \mathcal{A} \iff \Gamma^* \not\models_{fin} \mathcal{A}$$

и

$$\varphi(\mathcal{A}) = \text{Л} \iff \varphi(\neg \mathcal{A}) = \text{И},$$

то

$$\Gamma^* \models_{fin} \neg \mathcal{A} \iff \varphi(\neg \mathcal{A}) = \text{И}.$$

Нетрудно показать, что

$$\Gamma^* \models_{fin} (\mathcal{A} \& \mathcal{B}) \iff \Gamma^* \models_{fin} \mathcal{A} \text{ и } \Gamma^* \models_{fin} \mathcal{B}.$$

Кроме того, по определению интерпретации  $\varphi$

$$\varphi(\mathcal{A}) = \text{И} \text{ и } \varphi(\mathcal{B}) = \text{И} \iff \varphi(\mathcal{A} \& \mathcal{B}) = \text{И}.$$

Значит,

$$\Gamma^* \models_{fin} (\mathcal{A} \& \mathcal{B}) \iff \varphi(\mathcal{A} \& \mathcal{B}) = \text{И}.$$

Покажем, что для локально полного множества формул  $\Gamma^*$  и произвольных формул  $\mathcal{A}$  и  $\mathcal{B}$  имеет место эквивалентность

$$\Gamma^* \models_{fin} (\mathcal{A} \vee \mathcal{B}) \iff \Gamma^* \models_{fin} \mathcal{A} \text{ или } \Gamma^* \models_{fin} \mathcal{B}$$

В самом деле, если

$$\Gamma^* \models_{fin} \mathcal{A} \text{ или } \Gamma^* \models_{fin} \mathcal{B},$$

то, конечно,

$$\Gamma^* \models_{fin} (\mathcal{A} \vee \mathcal{B}).$$

Обратно, предположим, что

$$\Gamma^* \models_{fin} (\mathcal{A} \vee \mathcal{B}).$$

Покажем, что тогда

$$\Gamma^* \models_{fin} \mathcal{A} \text{ или } \Gamma^* \models_{fin} \mathcal{B}.$$

Предположим противное, т.е. что

$$\Gamma^* \not\models_{fin} \mathcal{A} \text{ и } \Gamma^* \not\models_{fin} \mathcal{B}.$$

Так как  $\Gamma^*$  — локально полное множество формул, то тогда

$$\Gamma^* \models_{fin} (\neg \mathcal{A}) \text{ и } \Gamma^* \models_{fin} (\neg \mathcal{B}),$$

а значит,

$$\Gamma^* \models_{fin} (\neg \mathcal{A}) \wedge (\neg \mathcal{B}),$$

поэтому

$$\Gamma^* \models_{fin} \neg(\mathcal{A} \vee \mathcal{B}).$$

Так как выше мы предположили, что

$$\Gamma^* \models_{fin} (\mathcal{A} \vee \mathcal{B}),$$

то получаем противоречие с предположением о локальной совместности множества формул  $\Gamma^*$ .

В итоге получаем

$$\Gamma^* \models_{fin} (\mathcal{A} \vee \mathcal{B}) \iff \Gamma^* \models_{fin} \mathcal{A} \text{ или } \Gamma^* \models_{fin} \mathcal{B}$$

и

$$\varphi(\mathcal{A}) = \text{И} \text{ или } \varphi(\mathcal{B}) = \text{И} \iff \varphi(\mathcal{A} \vee \mathcal{B}) = \text{И},$$

поэтому

$$\Gamma^* \models_{fin} (\mathcal{A} \vee \mathcal{B}) \iff \varphi(\mathcal{A} \vee \mathcal{B}) = \text{И}.$$

Доказательство эквивалентности

$$\Gamma^* \models_{fin} (\mathcal{A} \rightarrow \mathcal{B}) \iff \varphi(\mathcal{A} \rightarrow \mathcal{B}) = \text{И}$$

проводится по той же схеме с использованием локальной полноты и локальной совместности множества формул  $\Gamma^*$ .

В итоге доказано, что для произвольной формулы  $\mathcal{A}$  имеет место эквивалентность:

$$\Gamma^* \models_{fin} \mathcal{A} \iff \varphi(\mathcal{A}) = \text{И}.$$

Если  $\mathcal{A}$  — произвольная формула из множества  $\Gamma^*$ , то, очевидно,  $\Gamma^* \models_{fin} \mathcal{A}$ , поэтому  $\varphi(\mathcal{A}) = \text{И}$ .

Значит,  $\varphi(\Gamma^*) = \text{И}$ , поэтому множество формул  $\Gamma^*$  является совместным.  $\square$

**Второе доказательство** использует понятие ультрафильтра на булевой алгебре. Для читателя, не знакомого с этим понятием, рекомендуется обратиться к материалу из **Дополнения**.



Так как алфавит языка  $L_{\text{ЛВ}}$  является **счетным** множеством, то счетным является и множество  $F_{\text{ЛВ}}$  всех формул языка  $L_{\text{ЛВ}}$ , поэтому счетно и любое множество формул  $\Gamma$ .

Счетным будет множество всех **конечных** подмножеств множества формул  $\Gamma$ .

Пусть  $(\Gamma_i)_{i \in \mathbb{N}}$  — семейство всех **конечных** подмножеств множества формул  $\Gamma$ .

Так как каждое множество формул  $(\Gamma_i)_{i \in \mathbb{N}}$  по предположению является совместным, то найдется такая интерпретация  $\varphi_i$ , что  $\varphi_i(\Gamma_i) = \text{И}$ .

Зададим следующим образом счетное семейство подмножеств множества  $\mathbb{N}$  натуральных чисел

$$I_k \Leftarrow \{i \mid i \in \mathbb{N}, \varphi_i(\Gamma_k) = \text{И}\}.$$

Покажем, что пересечение любого конечного числа множеств  $I_k$  непусто.

Пусть  $I_{k_1}, \dots, I_{k_n}$  — произвольные множества.

Полагаем

$$\Gamma_s \Leftarrow \bigcup_{t=1}^n \Gamma_{k_t}.$$

Так как множество  $\Gamma_s$  является конечным, то найдется интерпретация  $\varphi_s$  такая, что  $\varphi_s(\Gamma_s) = \text{И}$ .

Но тогда при любом  $t$  ( $t = 1, \dots, n$ )  $\varphi_s(\Gamma_{k_t}) = \text{И}$ , поэтому

$$s \in \bigcap_{t=1}^n I_{k_t},$$

значит,

$$\bigcap_{t=1}^n I_{k_t} \neq \emptyset.$$

Пусть  $D$  — **ультрафильтр**, порожденный семейством множеств  $(I_k)_{k \in \mathbb{N}}$ .

Определим интерпретацию  $\varphi$ , полагая для произвольной пропозициональной переменной  $A_j$

$$\varphi(A_j) \Leftarrow \text{И} \iff \{i \mid \varphi_i(A_j) = \text{И}\} \in D.$$

Покажем, что для произвольной формулы  $\mathcal{A}$  имеет место эквивалентность

$$\varphi(\mathcal{A}) = \text{И} \iff \{i \mid \varphi_i(\mathcal{A}) = \text{И}\} \in D.$$

Доказательство проведем **индукцией по построению формул**.

(i) Для элементарных формул (пропозициональных переменных) указанная эквивалентность имеет место по определению интерпретации  $\varphi$ .

(ii) Предположим, что для формул  $\mathcal{A}$  и  $\mathcal{B}$  эта эквивалентность выполняется. Покажем, что она выполняется и для формул

$$(\neg \mathcal{A}), (\mathcal{A} \vee \mathcal{B}), (\mathcal{A} \& \mathcal{B}), (\mathcal{A} \rightarrow \mathcal{B}).$$

При этом существенно будет использоваться тот факт, что  $D$  — ультра-фильтр, а значит, для любых подмножеств  $A$  и  $B$  множества натуральных чисел  $\mathbb{N}$  выполняются эквивалентности

- 1)  $A \in D \iff (\mathbb{N} \setminus A) \notin D$ ,
- 2)  $(A \cup B) \in D \iff A \in D$  или  $B \in D$ ,
- 3)  $(A \cap B) \in D \iff A \in D$  и  $B \in D$ .

Заметим, что последнее верно и для любого фильтра. Отметим, что

$$\varphi(\neg \mathcal{A}) = \text{И} \iff \varphi(\mathcal{A}) = \text{Л}.$$

Предположим, что

$$\varphi(\mathcal{A}) = \text{И} \iff \{i \mid \varphi_i(\mathcal{A}) = \text{И}\} \in D.$$

Значит,

$$\varphi(\mathcal{A}) = \text{Л} \iff \{i \mid \varphi_i(\mathcal{A}) = \text{И}\} \notin D.$$

Так как  $D$  — ультрафильтр, то

$$\{i \mid \varphi_i(\mathcal{A}) = \text{И}\} \notin D \iff \mathbb{N} \setminus \{i \mid \varphi_i(\mathcal{A}) = \text{И}\} \in D.$$

Но

$$\mathbb{N} \setminus \{i \mid \varphi_i(\mathcal{A}) = \text{И}\} = \{i \mid \varphi_i(\mathcal{A}) = \text{Л}\} = \{i \mid \varphi_i(\neg \mathcal{A}) = \text{И}\}.$$

Окончательно получаем

$$\varphi(\neg \mathcal{A}) = \text{И} \iff \{i \mid \varphi_i(\neg \mathcal{A}) = \text{И}\} \in D.$$

Предположим, что

$$\varphi(\mathcal{A}) = \text{И} \iff \{i \mid \varphi_i(\mathcal{A}) = \text{И}\} \in D$$

и

$$\varphi(\mathcal{B}) = \text{И} \iff \{i \mid \varphi_i(\mathcal{B}) = \text{И}\} \in D.$$

Покажем, что тогда

$$\begin{aligned} \varphi(\mathcal{A} \vee \mathcal{B}) = \text{И} &\iff \{i \mid \varphi_i(\mathcal{A} \vee \mathcal{B}) = \text{И}\} \in D, \\ \varphi(\mathcal{A} \& \mathcal{B}) = \text{И} &\iff \{i \mid \varphi_i(\mathcal{A} \& \mathcal{B}) = \text{И}\} \in D, \\ \varphi(\mathcal{A} \rightarrow \mathcal{B}) = \text{И} &\iff \{i \mid \varphi_i(\mathcal{A} \rightarrow \mathcal{B}) = \text{И}\} \in D. \end{aligned}$$

Напомним, что

$$\varphi(\mathcal{A} \vee \mathcal{B}) = \text{И} \iff \varphi(\mathcal{A}) = \text{И} \text{ или } \varphi(\mathcal{B}) = \text{И}.$$

По предположению

$$\varphi(\mathcal{A}) = \text{И} \iff \{i \mid \varphi_i(\mathcal{A}) = \text{И}\} \in D$$

и

$$\varphi(\mathcal{B}) = \text{И} \iff \{i \mid \varphi_i(\mathcal{B}) = \text{И}\} \in D.$$

Так как  $D$  — ультрафильтр, то

$$\begin{aligned} \{i \mid \varphi_i(\mathcal{A}) = \text{И}\} \in D \text{ или } \{i \mid \varphi_i(\mathcal{B}) = \text{И}\} \in D &\iff \\ \{i \mid \varphi_i(\mathcal{A}) = \text{И}\} \cup \{i \mid \varphi_i(\mathcal{B}) = \text{И}\} &\in D. \end{aligned}$$

Окончательно получаем

$$\begin{aligned} \varphi(\mathcal{A} \vee \mathcal{B}) = \text{И} &\iff \varphi(\mathcal{A}) = \text{И} \text{ или } \varphi(\mathcal{B}) = \text{И} \iff \\ \{i \mid \varphi_i(\mathcal{A}) = \text{И}\} \in D \text{ или } \{i \mid \varphi_i(\mathcal{B}) = \text{И}\} \in D &\iff \\ \{i \mid \varphi_i(\mathcal{A}) = \text{И}\} \cup \{i \mid \varphi_i(\mathcal{B}) = \text{И}\} &\in D. \end{aligned}$$

Остается заметить, что

$$\{i \mid \varphi_i(\mathcal{A}) = \text{И}\} \cup \{i \mid \varphi_i(\mathcal{B}) = \text{И}\} = \{i \mid \varphi_i(\mathcal{A} \vee \mathcal{B}) = \text{И}\}.$$

Полученная цепочка эквивалентностей дает эквивалентность

$$\varphi(\mathcal{A} \vee \mathcal{B}) = \text{И} \iff \{i \mid \varphi_i(\mathcal{A} \vee \mathcal{B}) = \text{И}\} \in D.$$

Эквивалентность

$$\varphi(\mathcal{A} \& \mathcal{B}) = \text{И} \iff \{i \mid \varphi_i(\mathcal{A} \& \mathcal{B}) = \text{И}\} \in D$$

получается по той же схеме.

Напомним, что

$$\varphi(\mathcal{A} \& \mathcal{B}) = \text{И} \iff \varphi(\mathcal{A}) = \text{И} \text{ и } \varphi(\mathcal{B}) = \text{И}.$$

По предположению

$$\varphi(\mathcal{A}) = \text{И} \iff \{i \mid \varphi_i(\mathcal{A}) = \text{И}\} \in D$$

и

$$\varphi(\mathcal{B}) = \text{И} \iff \{i \mid \varphi_i(\mathcal{B}) = \text{И}\} \in D.$$

Для любого фильтра  $D$  выполняется эквивалентность

$$\begin{aligned} \{i \mid \varphi_i(\mathcal{A}) = \text{И}\} \in D \text{ и } \{i \mid \varphi_i(\mathcal{B}) = \text{И}\} \in D &\iff \\ \{i \mid \varphi_i(\mathcal{A}) = \text{И}\} \cap \{i \mid \varphi_i(\mathcal{B}) = \text{И}\} &\in D. \end{aligned}$$

Окончательно получаем

$$\begin{aligned} \varphi(\mathcal{A} \& \mathcal{B}) = \text{И} &\iff \varphi(\mathcal{A}) = \text{И} \text{ и } \varphi(\mathcal{B}) = \text{И} \iff \\ \{i \mid \varphi_i(\mathcal{A}) = \text{И}\} \in D \text{ и } \{i \mid \varphi_i(\mathcal{B}) = \text{И}\} \in D &\iff \\ \{i \mid \varphi_i(\mathcal{A}) = \text{И}\} \cap \{i \mid \varphi_i(\mathcal{B}) = \text{И}\} &\in D. \end{aligned}$$

Остается заметить, что

$$\{i \mid \varphi_i(\mathcal{A}) = \text{И}\} \cap \{i \mid \varphi_i(\mathcal{B}) = \text{И}\} = \{i \mid \varphi_i(\mathcal{A} \& \mathcal{B}) = \text{И}\}.$$

Полученная цепочка эквивалентностей дает эквивалентность

$$\varphi(\mathcal{A} \& \mathcal{B}) = \text{И} \iff \{i \mid \varphi_i(\mathcal{A} \& \mathcal{B}) = \text{И}\} \in D.$$

Эквивалентность

$$\varphi(\mathcal{A} \rightarrow \mathcal{B}) = \text{И} \iff \{i \mid \varphi_i(\mathcal{A} \rightarrow \mathcal{B}) = \text{И}\} \in D$$

может быть получена аналогичным образом. Это предоставляется сделать читателю в качестве простого упражнения.

Покажем, что в интерпретации  $\varphi$  истинна любая формула из множества формул  $\Gamma$ .

В самом деле, пусть  $\mathcal{A}$  — произвольная формула из множества формул  $\Gamma$ . Рассмотрим конечное множество  $\Gamma_k \Leftarrow \{\mathcal{A}\}$ .

Напомним, что

$$I_k = \{i \mid i \in \mathbb{N}, \varphi_i(\mathcal{A}) = \text{И}\}.$$

Так как  $I_k \in D$ , то  $\{i \mid i \in \mathbb{N}, \varphi_i(\mathcal{A}) = \text{И}\} \in D$ .

Поэтому в силу доказанной эквивалентности

$$\varphi(\mathcal{A}) = \text{И} \iff \{i \mid \varphi_i(\mathcal{A}) = \text{И}\} \in D$$

получаем, что  $\varphi(\mathcal{A}) = \text{И}$ .

Значит, множество формул  $\Gamma$  является **совместным**.

Это завершает второе доказательство **Теоремы компактности**.  $\square$

**Следствие.** Для любой формулы  $\mathcal{A}$  языка  $L_{\text{ЛВ}}$  и для любого множества формул  $\Gamma$  этого языка имеет место следующая эквивалентность:

формула  $\mathcal{A}$  является логическим следствием множества формул  $\Gamma$  тогда и только тогда, когда она является логическим следствием некоторого конечного подмножества  $\Gamma_0$  множества формул  $\Gamma$ , т.е.

$$\Gamma \models \mathcal{A} \iff \Gamma \models_{\text{fin}} \mathcal{A}.$$

**Д о к а з а т е л ь с т в о.** Если формула  $\mathcal{A}$  является логическим следствием некоторого конечного подмножества  $\Gamma_0$  множества формул  $\Gamma$ , то, очевидно, формула  $\mathcal{A}$  является логическим следствием и множества формул  $\Gamma$ .

Предположим теперь, что формула  $\mathcal{A}$  является логическим следствием множества формул  $\Gamma$ .

Тогда множество формул  $\Gamma \cup \{\neg \mathcal{A}\}$  не является совместным, значит, по **Теореме компактности** найдется такое конечное подмножество  $\Gamma_0$  множества формул  $\Gamma$ , что множество формул  $\Gamma_0 \cup \{\neg \mathcal{A}\}$  не является совместным. Значит, для любой интерпретации  $\varphi$  из того, что  $\varphi(\Gamma_0) = \text{И}$  следует, что  $\varphi(\neg \mathcal{A}) = \text{Л}$ ,

т.е. что  $\varphi(\mathcal{A}) = \text{И}$ , поэтому формула  $\mathcal{A}$  является логическим следствием конечного подмножества  $\Gamma_0$  множества формул  $\Gamma$ .  $\square$

Сделаем некоторые пояснения по поводу использования термина “компактность.”

Напомним некоторые топологические понятия и определения.

**Определение 2.11.** Топологическое пространство называется **компактным**, если любое его покрытие открытыми множествами содержит **конечное подпокрытие**.

Это определение компактности равносильно следующему определению, основанному на использовании вместо открытых множеств замкнутых множеств.

**Определение 2.12.** Семейство  $\mathcal{R}$  подмножеств множества  $X$  называется **центрированным**, если непусто пересечение любого конечного числа множеств из семейства  $\mathcal{R}$ .

**Определение 2.13.** Топологическое пространство называется **компактным**, если любое центрированное семейство его замкнутых подмножеств имеет непустое пересечение.

Обозначим через  $U$  множество всех интерпретаций языка  $L_{ЛВ}$ .

Наделим множество  $U$  структурой топологического пространства. Как известно, для этого достаточно определить понятие **замкнутого** множества. Тогда открытые подмножества определяются как дополнения замкнутых подмножеств.

Напомним, что для произвольной интерпретации языка  $L_{ЛВ}$  и произвольного множества  $\Gamma$  формул этого языка запись  $\varphi(\Gamma) = \text{И}$  означает, что для любой формулы  $\Phi$  из множества  $\Gamma$  выполняется равенство  $\varphi(\Phi) = \text{И}$ .

**Определение 2.14.** Подмножество  $X$  множества  $U$  назовем **замкнутым**, если найдется такое подмножество  $\Gamma$  множества формул  $F_{ЛВ}$  языка  $L_{ЛВ}$ , что

$$X = \{\varphi \mid \varphi(\Gamma) = \text{И}\}.$$

Проверим, что при таком определении понятия замкнутого множества выполняются аксиомы топологического пространства:

- 1) пустое множество и все пространство являются замкнутыми множествами;
- 2) пересечение любого семейства замкнутых множеств замкнуто;
- 3) объединение двух замкнутых множеств замкнуто.



Легко понять, что выполняются равенства

1.

$$\emptyset = \{\varphi \mid \varphi(\{(A_1 \& \neg A_1)\}) = \text{И}\},$$

$$U = \{\varphi \mid \varphi(\{(A_1 \vee \neg A_1)\}) = \text{И}\}.$$

2. Если  $(X_i)_{i \in I}$  — произвольное семейство замкнутых множеств и

$$X_i = \{\varphi \mid \varphi(\Gamma_i) = \text{И}\},$$

то

$$\bigcap_{i \in I} X_i = \{\varphi \mid \varphi(\bigcup_{i \in I} \Gamma_i) = \text{И}\}.$$

3. Пусть  $X_i$  ( $i = 1, 2$ ) — два произвольных замкнутых множества и

$$X_i = \{\varphi \mid \varphi(\Gamma_i) = \text{И}\}.$$

Обозначим через  $\Gamma_1 \vee \Gamma_2$  следующее множество формул языка  $L_{\text{ЛВ}}$

$$\{\Phi_1 \vee \Phi_2 \mid \Phi_1 \in \Gamma_1, \Phi_2 \in \Gamma_2\}.$$

Нетрудно понять, что выполняется равенство

$$X_1 \cup X_2 = \{\varphi \mid \varphi(\Gamma_1 \vee \Gamma_2) = \text{И}\}.$$

Поэтому множество  $U$  вместе с определенной выше системой замкнутых подмножеств является топологическим пространством.

Покажем, что доказанная выше **Теорема компактности** для языка  $L_{\text{ЛВ}}$  устанавливает *компактность* этого топологического пространства.

В самом деле, пусть  $\mathcal{R} = (X_i)_{i \in I}$  — произвольное *центрированное* семейство замкнутых подмножеств пространства  $U$ .

Тогда при любом  $i$  для подходящего множества  $\Gamma_i$  формул языка  $L_{\text{ЛВ}}$  выполняется равенство

$$X_i = \{\varphi \mid \varphi(\Gamma_i) = \text{И}\}.$$

Для установления компактности пространства  $U$  необходимо показать, что

$$\bigcap_{i \in I} X_i \neq \emptyset,$$

т.е. что

$$\{\varphi \mid \varphi(\bigcup_{i \in I} \Gamma_i) = \text{И}\} \neq \emptyset.$$

Другими словами, требуется установить совместность множества формул

$$\bigcup_{i \in I} \Gamma_i.$$

Пусть  $\Gamma$  — произвольное *конечное* подмножество этого множества. Тогда найдется такое *конечное* подмножество  $I_0$  множества  $I$ , что

$$\Gamma \subset \bigcup_{i \in I_0} \Gamma_i.$$

Так как  $(X_i)_{i \in I}$  — *центрированное* семейство множеств, то

$$\bigcap_{i \in I_0} X_i \neq \emptyset.$$

Но

$$\bigcap_{i \in I_0} X_i = \{ \varphi \mid \varphi(\bigcup_{i \in I_0} \Gamma_i) = \mathbb{I} \}.$$

Поэтому

$$\{ \varphi \mid \varphi(\bigcup_{i \in I_0} \Gamma_i) = \mathbb{I} \} \neq \emptyset,$$

т.е. множество формул

$$\bigcup_{i \in I_0} \Gamma_i$$

совместно.

Поэтому совместно и множество формул  $\Gamma$ .

Так как мы установили совместность любого конечного подмножества  $\Gamma$  множества формул

$$\bigcup_{i \in I} \Gamma_i,$$

то по **Теореме компактности** совместно и само это множество формул

$$\bigcup_{i \in I} \Gamma_i.$$

Значит,

$$\{ \varphi \mid \varphi(\bigcup_{i \in I} \Gamma_i) = \mathbb{I} \} \neq \emptyset,$$

поэтому

$$\bigcap_{i \in I} X_i \neq \emptyset.$$

Традиционно в определение компактного пространства включается **аксиома отделимости** Хаусдорфа:

для любых двух точек топологического пространства найдутся содержащие их непересекающиеся открытые множества.

Покажем, что для пространства интерпретаций выполняется аксиома отделимости.

Пусть  $\varphi_1, \varphi_2$  — две различные интерпретации, тогда найдется число  $i$  такое, что

$$\varphi_1(A_i) \neq \varphi_2(A_i).$$

Предположим, что

$$\varphi_1(A_i) = \text{И}, \quad \varphi_2(A_i) = \text{Л}.$$

Рассмотрим замкнутые множества

$$F_1 = \{\varphi \mid \varphi(\neg A_i) = \text{И}\}, \quad F_2 = \{\varphi \mid \varphi(A_i) = \text{И}\}.$$

Полагаем

$$U_1 = U \setminus F_1, \quad U_2 = U \setminus F_2.$$

Тогда  $U_1, U_2$  — открытые множества и

$$\varphi_1 \in U_1, \quad \varphi_2 \in U_2, \quad U_1 \cap U_2 = \emptyset.$$

Тем самым установлена компактность пространства  $U$  интерпретаций языка  $L_{\text{ЛВ}}$ .

Заметим, что для любой формулы  $\mathcal{A}$  выполняется равенство

$$\{\varphi \mid \varphi(\mathcal{A}) = \text{И}\} = U \setminus \{\varphi \mid \varphi(\neg \mathcal{A}) = \text{И}\},$$

поэтому множество

$$\{\varphi \mid \varphi(\mathcal{A}) = \text{И}\}$$

является одновременно замкнутым и открытым.

Из последнего, очевидно, следует, что пространство интерпретаций  $U$  не является связным.

### 3. Исчисление Высказываний

Алфавит Исчисления Высказываний  $\Sigma_{\text{ИВ}}$  совпадает с Алфавитом Логике Высказываний  $\Sigma_{\text{ЛВ}}$ .

Понятие формулы Исчисления Высказываний определяется дословно так же, как и понятие формулы Логике Высказываний, т.е. язык  $L_{\text{ИВ}}$  Исчисления Высказываний совпадает с языком  $L_{\text{ЛВ}}$  Логике Высказываний.

Теперь мы приступаем к определению двух важнейших понятий Исчисления Высказываний — понятия ВЫВОДА и понятия ВЫВОДИМОЙ ФОРМУЛЫ.

### Аксиомы Исчисления Высказываний

Для произвольных формул  $A, B, C$  Исчисления Высказываний формула любого указанного ниже вида является Логической Аксиомой Исчисления Высказываний.

$I_{\rightarrow}$ .

- I.1.  $(A \rightarrow (B \rightarrow A)).$
- I.2.  $((A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))).$

$II_{\&}$ .

- II.1.  $((A \& B) \rightarrow A).$
- II.2.  $((A \& B) \rightarrow B).$
- II.3.  $(A \rightarrow (B \rightarrow (A \& B))).$
- II.4.  $((A \rightarrow B) \rightarrow ((A \rightarrow C) \rightarrow (A \rightarrow (B \& C)))).$

$III_{\vee}$ .

- III.1.  $(A \rightarrow (A \vee B)).$
- III.2.  $(B \rightarrow (A \vee B)).$
- III.3.  $((A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow ((A \vee B) \rightarrow C))).$

$IV_{\neg}$ .

- IV.1.  $((A \rightarrow (\neg B)) \rightarrow (B \rightarrow (\neg A))).$
- IV.2.  $((\neg(\neg A)) \rightarrow A).$

### Правила Вывода Исчисления Высказываний

В Исчислении Высказываний используется лишь одно Правило Вывода — Правило Отделения (*Modus Ponens*).

Кратко это правило будем обозначать через МР:

$$\frac{A, (A \rightarrow B)}{B}.$$

Эта запись означает, что по правилу МР из формул  $A$  и  $(A \rightarrow B)$  получается формула  $B$ . При этом формулы  $A$  и  $(A \rightarrow B)$  называются посылками правила МР, а формула  $B$  — его заключением.

### Вывод и вывод из множества формул

**Определение 3.1.** Выводом в Исчислении Высказываний называется любая конечная последовательность

$$B_1, \dots, B_n$$

формул Исчисления Высказываний, удовлетворяющая следующему условию:

для любого  $i$  ( $i = 1, \dots, n$ )

либо

- 1) формула  $B_i$  является Логической Аксиомой Исчисления Высказываний, либо
- 2) найдутся числа  $j$  и  $k$  меньшие, чем  $i$ , такие, что формула  $B_i$  получается из формул  $B_j$  и  $B_k$  по правилу МР.

**Определение 3.2.** Формула  $B$  называется выводимой в Исчислении Высказываний, если существует Вывод в Исчислении Высказываний

$$B_1, \dots, B_n,$$

оканчивающийся формулой  $B$ .

Выражение  $\vdash_{\text{ИВ}} A$  служит сокращенной записью утверждения “формула  $A$  выводима в Исчислении Высказываний”. В дальнейшем для сокращения индекса ИВ будем опускать, т.е. вместо  $\vdash_{\text{ИВ}} A$  будем писать просто  $\vdash A$ .

**Теорема 3.1.** Для любой формулы  $A$  формула  $(A \rightarrow A)$  выводима в Исчислении Высказываний.

*Доказательство.* Чтобы доказать, что формула  $(A \rightarrow A)$  выводима в Исчислении Высказываний, необходимо построить вывод, оканчивающийся этой формулой. В качестве такого вывода предлагается следующая последовательность формул:

- 1)  $((A \rightarrow ((A \rightarrow A) \rightarrow A)) \rightarrow ((A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A)))$  — логическая аксиома I.2,
- 2)  $(A \rightarrow ((A \rightarrow A) \rightarrow A))$  — логическая аксиома I.1,
- 3)  $((A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A))$  — получается из 2) и 1) по правилу МР,
- 4)  $(A \rightarrow (A \rightarrow A))$  — логическая аксиома I.1,
- 5)  $(A \rightarrow A)$  — получается из 4) и 3) по правилу МР. □

**Теорема 3.2.** Для любых формул  $A$  и  $B$  имеет место эквивалентность:

$$\vdash (A \& B) \text{ тогда и только тогда, когда } \vdash A \text{ и } \vdash B.$$

*Доказательство.* Допустим, что  $\vdash (A \& B)$ . В соответствии с определением понятия выводимости формулы существует конечная последовательность формул

$$B_1, \dots, B_n,$$

являющаяся выводом формулы  $(A \& B)$ , поэтому, в частности,  $B_n = (A \& B)$ .

Следующая последовательность формул является выводом формулы  $A$

- 1)  $B_1,$
- ...
- $n$ )  $B_n = (A \& B),$
- $n + 1$ )  $((A \& B) \rightarrow A)$  — логическая аксиома II.1,
- $n + 2$ )  $A$  — следует из  $n$ ) и  $n + 1$ ) по правилу МР.



Значит,  $\vdash A$ .

Для доказательства  $\vdash B$  достаточно в пункте  $n + 1$ ) взять формулу  $((A \& B) \rightarrow B)$ .

Предположим теперь, что  $\vdash A$  и  $\vdash B$ .

Покажем, что тогда  $\vdash (A \& B)$ .

Пусть последовательность формул

$$B_1, \dots, B_n$$

является выводом формулы  $A$ , а последовательность формул

$$C_1, \dots, C_m,$$

является выводом формулы  $B$ .

Тогда, в частности,  $B_n = A$  и  $C_m = B$ .

Построим последовательность формул, являющуюся выводом формулы  $(A \& B)$ .

- 1)  $B_1,$
- $\dots$
- $n$ )  $B_n,$
- $n + 1$ )  $C_1,$
- $\dots$
- $n + m$ )  $C_m,$
- $n + m + 1$ )  $(A \rightarrow (B \rightarrow (A \& B)))$  — логическая аксиома II.3,
- $n + m + 2$ )  $(B \rightarrow (A \& B))$  — следует из  $n$ ) и  $n + m + 1$ ) по правилу МР,
- $n + m + 3$ )  $(A \& B)$  — следует из  $n + m$ ) и  $n + m + 2$ ) по правилу МР.

Тем самым доказано, что  $\vdash (A \& B)$ . □

Приведенные доказательства показывают, что установление выводимости даже достаточно простых фрмул — процесс весьма трудоемкий. С целью облегчения изучения отношения  $\vdash A$  введем и изучим более общее понятие, чем понятие Вывода — понятие **Вывода из множества гипотез**.

Пусть  $\Gamma$  — произвольное множество формул. Формулы из множества  $\Gamma$  будем называть **гипотезами**. Смысл этого названия прояснится позже.

**Определение 3.3.** Выводом из множества формул  $\Gamma$  называется любая конечная последовательность

$$B_1, \dots, B_n$$

формул Исчисления Высказываний, удовлетворяющая следующему условию:

- для любого  $i$  ( $i = 1, \dots, n$ )  
либо  
0)  $B_i \in \Gamma,$

либо

1) формула  $B_i$  является Логической Аксиомой Исчисления Высказываний, либо

2) найдутся числа  $j$  и  $k$  меньшие, чем  $i$ , такие, что формула  $B_i$  получается из формул  $B_j$  и  $B_k$  по правилу МР.

**Определение 3.4.** Формула  $B$  называется выводимой в Исчислении Высказываний из множества формул  $\Gamma$ , если существует Вывод в Исчислении Высказываний из множества формул  $\Gamma$

$$B_1, \dots, B_n,$$

оканчивающийся формулой  $B$ .

Выражение  $\Gamma \vdash_{\text{ИВ}} A$  служит сокращенной записью утверждения “формула  $A$  выводима в Исчислении Высказываний из множества формул  $\Gamma$ ”. И вновь индекс ИВ не будем писать.

Если  $\Gamma$  и  $\Delta$  — два произвольных множества формул, то запись  $\Gamma \vdash \Delta$  означает, что любая формула из множества  $\Delta$  выводима в Исчислении Высказываний из множества формул  $\Gamma$ .

**Теорема 3.3.** Если  $\Gamma \vdash A$  и  $\Gamma \subset \Gamma_1$ , то  $\Gamma_1 \vdash A$ .

Если  $\Gamma_1 \vdash A$ , то найдется конечное подмножество  $\Gamma$  множества  $\Gamma_1$  такое, что  $\Gamma \vdash A$ .

*Доказательство.* Если  $\Gamma \subset \Gamma_1$ , то любой вывод из множества формул  $\Gamma$  будет выводом и из множества формул  $\Gamma_1$ .

Если  $\Gamma_1 \vdash A$  и  $B_1, \dots, B_n$  — вывод формулы  $A$  из множества формул  $\Gamma_1$ , то в качестве  $\Gamma$  можно взять  $\Gamma_1 \cap \{B_1, \dots, B_n\}$ .  $\square$

**Теорема 3.4.** Если  $\Gamma_1 \vdash \Delta$  и  $\Gamma_2 \cup \Delta \vdash A$ , то  $\Gamma_1 \cup \Gamma_2 \vdash A$ .

*Доказательство.* В силу предыдущей теоремы можно считать, что множество  $\Delta$  конечное, поэтому доказательство легко получается индукцией по числу формул во множестве  $\Delta$ .  $\square$

**Замечание.** В дальнейшем по сложившейся традиции вместо записи  $\Gamma_1 \cup \Gamma_2 \vdash A$  будем использовать запись  $\Gamma_1, \Gamma_2 \vdash A$ , а вместо записи  $\Gamma_1, \{B\} \vdash A$  — запись  $\Gamma_1, B \vdash A$ .

Теперь мы докажем теорему, которая значительно облегчает изучение отношения  $\Gamma \vdash A$ . Эта теорема носит специальное название **Теорема Дедукции**.

**Теорема Дедукции.** Если  $\Gamma, A \vdash B$ , то  $\Gamma \vdash (A \rightarrow B)$ .

Обратно, если  $\Gamma \vdash (A \rightarrow B)$ , то  $\Gamma, A \vdash B$ .

*Д о к а з а т е л ь с т в о.* Предположим, что  $\Gamma, \mathcal{A} \vdash \mathcal{B}$ . Покажем, что  $\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B})$ .

Пусть  $\mathcal{B}_1, \dots, \mathcal{B}_n$  — вывод формулы  $\mathcal{B}$  из множества  $\Gamma \cup \{\mathcal{A}\}$ .

Индукцией по  $i$  покажем, что  $\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B}_i)$ .

В соответствии с определением понятия “Вывод из множества формул” возможны следующие три случая:

0)  $\mathcal{B}_i \in \Gamma \cup \{\mathcal{A}\}$ .

Если  $\mathcal{B}_i \in \Gamma$ , то  $\Gamma \vdash \mathcal{B}_i$ .

Кроме того,

$$\vdash (\mathcal{B}_i \rightarrow (\mathcal{A} \rightarrow \mathcal{B}_i)).$$

Так как

$$\mathcal{B}_i, (\mathcal{B}_i \rightarrow (\mathcal{A} \rightarrow \mathcal{B}_i)) \vdash (\mathcal{A} \rightarrow \mathcal{B}_i),$$

то по теоремам 3.3 и 3.4 получаем

$$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B}_i).$$

Если же  $\mathcal{B}_i \in \{\mathcal{A}\}$ , то  $\mathcal{B}_i \equiv \mathcal{A}$ .

Тогда по теореме 3.1

$$\vdash (\mathcal{A} \rightarrow \mathcal{B}_i).$$

1)  $\mathcal{B}_i$  — логическая аксиома.

Тогда  $\Gamma \vdash \mathcal{B}_i$ .

Кроме того,

$$\vdash (\mathcal{B}_i \rightarrow (\mathcal{A} \rightarrow \mathcal{B}_i)).$$

Так как

$$\mathcal{B}_i, (\mathcal{B}_i \rightarrow (\mathcal{A} \rightarrow \mathcal{B}_i)) \vdash (\mathcal{A} \rightarrow \mathcal{B}_i),$$

то по теоремам 3.3 и 3.4 получаем

$$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B}_i).$$

2) Найдутся числа  $j$  и  $k$ , меньшие  $i$ , такие, что формула  $\mathcal{B}_i$  получается из формул  $\mathcal{B}_j$  и  $\mathcal{B}_k$  по правилу вывода МР.

Тогда

$$\mathcal{B}_k \equiv (\mathcal{B}_j \rightarrow \mathcal{B}_i).$$

По индуктивному предположению имеем

$$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B}_j),$$

$$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B}_k),$$

т.е.

$$\Gamma \vdash (\mathcal{A} \rightarrow (\mathcal{B}_j \rightarrow \mathcal{B}_i)),$$

Так как

$$\vdash ((A \rightarrow (B_j \rightarrow B_i)) \rightarrow ((A \rightarrow B_j)) \rightarrow (A \rightarrow B_i))$$

и

$$(A \rightarrow (B_j \rightarrow B_i)), (A \rightarrow B_j) \vdash (A \rightarrow B_i)),$$

то по теореме 3.4 получаем

$$\Gamma \vdash (A \rightarrow B_i).$$

При  $i = n$  получаем

$$\Gamma \vdash (A \rightarrow B).$$

Для доказательства второй части теоремы предположим, что

$$\Gamma \vdash (A \rightarrow B).$$

Так как

$$A \vdash A$$

и

$$A, (A \rightarrow B) \vdash B,$$

то по теореме 3.4 получаем

$$\Gamma, A \vdash B.$$

Это завершает доказательство теоремы. □

Следующая теорема обобщает теорему 3.2.

**Теорема 3.5.** Для любых формул  $A$  и  $B$  и любого множества формул  $\Gamma$  имеет место эквивалентность:

$$\Gamma \vdash A \quad \text{и} \quad \Gamma \vdash B$$

тогда и только тогда, когда

$$\Gamma \vdash (A \& B).$$

*Д о к а з а т е л ь с т в о.* Используя логическую аксиому П.3, получаем

$$\vdash (A \rightarrow (B \rightarrow (A \& B))),$$

кроме того,

$$A, B, (A \rightarrow (B \rightarrow (A \& B))) \vdash (A \& B).$$

Откуда по теореме 3.4 получаем

$$A, B, \vdash (A \& B).$$

Если

$$\Gamma \vdash A \text{ и } \Gamma \vdash B,$$

то применив теорему 3.4, получим

$$\Gamma \vdash (A \& B).$$

Для доказательства обратного утверждения предположим, что

$$\Gamma \vdash (A \& B).$$

Используя логические аксиомы II.1 и II.2 и Теорему Дедукции, получаем

$$(A \& B) \vdash A \text{ и } (A \& B) \vdash B,$$

поэтому применив теорему 3.4, получим

$$\Gamma \vdash A \text{ и } \Gamma \vdash B.$$

□

**Теорема 3.6.** Для любой формулы  $A$

$$\vdash (A \rightarrow (\neg(\neg A))).$$

*Доказательство.* Логическая аксиома IV.1 дает

$$\vdash (((\neg A) \rightarrow (\neg A)) \rightarrow (A \rightarrow (\neg(\neg A)))).$$

Откуда по Теореме Дедукции получаем

$$((\neg A) \rightarrow (\neg A)) \vdash (A \rightarrow (\neg(\neg A))).$$

По теореме 3.1

$$\vdash ((\neg A) \rightarrow (\neg A)).$$

Применив теорему 3.4, получим

$$\vdash (A \rightarrow (\neg(\neg A))).$$

□

Для любых двух формул  $A$  и  $B$  запись  $A \leftrightarrow B$  будет служить сокращенным обозначением формулы  $((A \rightarrow B) \& (B \rightarrow A))$ .

**Следствие.** Для любой формулы  $A$  и любого множества формул  $\Gamma$  имеем

$$1) \ A \vdash (\neg(\neg A)),$$

$$2) \ (\neg(\neg A)) \vdash A,$$



$$3) \Gamma \vdash \mathcal{A} \iff \Gamma \vdash (\neg(\neg\mathcal{A})),$$

$$4) \vdash (\mathcal{A} \leftrightarrow (\neg(\neg\mathcal{A}))).$$

*Д о к а з а т е л ь с т в о.*

1) В силу предыдущей теоремы 3.6

$$\vdash (\mathcal{A} \rightarrow (\neg(\neg\mathcal{A}))),$$

поэтому по Теореме Дедукции получаем  $\mathcal{A} \vdash (\neg(\neg\mathcal{A}))$ .

2) Воспользовавшись логической аксиомой IV.2, получаем  $\vdash ((\neg(\neg\mathcal{A})) \rightarrow \mathcal{A})$ , применение Теоремы Дедукции дает  $(\neg(\neg\mathcal{A})) \vdash \mathcal{A}$ .

3) Пусть  $\Gamma \vdash \mathcal{A}$ . Так как  $\mathcal{A} \vdash (\neg(\neg\mathcal{A}))$ , то по теореме 3.4 получаем  $\Gamma \vdash (\neg(\neg\mathcal{A}))$ .

Аналогично доказывается обратное утверждение.

4) Так как

$$\vdash (\mathcal{A} \rightarrow (\neg(\neg\mathcal{A}))),$$

$$\vdash ((\neg(\neg\mathcal{A})) \rightarrow \mathcal{A}),$$

то по теореме 3.2 получаем, что

$$\vdash (\mathcal{A} \rightarrow (\neg(\neg\mathcal{A}))) \& ((\neg(\neg\mathcal{A})) \rightarrow \mathcal{A}),$$

т.е.

$$\vdash (\mathcal{A} \leftrightarrow (\neg(\neg\mathcal{A}))).$$

□

**Теорема 3.7.** Для любых формул  $\mathcal{A}$  и  $\mathcal{B}$

$$\mathcal{A}, (\neg\mathcal{A}) \vdash \mathcal{B}.$$

*Д о к а з а т е л ь с т в о.* Логическая аксиома I.1 дает

$$\vdash ((\neg\mathcal{A}) \rightarrow ((\neg\mathcal{B}) \rightarrow (\neg\mathcal{A}))),$$

по Теореме Дедукции получаем

$$(\neg\mathcal{A}) \vdash ((\neg\mathcal{B}) \rightarrow (\neg\mathcal{A})).$$

Логическая аксиома IV.1 дает

$$\vdash (((\neg\mathcal{B}) \rightarrow (\neg\mathcal{A})) \rightarrow (\mathcal{A} \rightarrow (\neg(\neg\mathcal{B})))),$$

по Теореме Дедукции получаем

$$((\neg\mathcal{B}) \rightarrow (\neg\mathcal{A})) \vdash (\mathcal{A} \rightarrow (\neg(\neg\mathcal{B}))).$$

Применяя теорему 3.4, получаем

$$(\neg A) \vdash (A \rightarrow (\neg(\neg B))).$$

По Теореме Дедукции получаем

$$A, (\neg A) \vdash (\neg(\neg B)).$$

В силу пункта 3) предыдущего следствия получаем

$$A, (\neg A) \vdash B.$$

□

**Определение 3.5.** Множество формул  $\Gamma$  называется **противоречивым**, если найдется такая формула  $A$ , что

$$\Gamma \vdash A \text{ и } \Gamma \vdash (\neg A),$$

в противном случае множество формул  $\Gamma$  называется **непротиворечивым**.

**Следствие.** Если  $\Gamma$  — противоречивое множество формул, то для любой формулы  $B$

$$\Gamma \vdash B.$$

*Д о к а з а т е л ь с т в о.* Если  $\Gamma$  — противоречивое множество формул, то найдется такая формула  $A$ , что

$$\Gamma \vdash A \text{ и } \Gamma \vdash (\neg A).$$

Пусть  $B$  — произвольная формула. По предыдущей теореме 3.7

$$A, (\neg A) \vdash B.$$

Поэтому по теореме 3.4

$$\Gamma \vdash B.$$

□

**Следствие.** Для любых формул  $A$  и  $B$

- |   |   |
|---|---|
| 1) $\vdash (A \rightarrow ((\neg A) \rightarrow B)),$ | 2) $\vdash ((\neg A) \rightarrow (A \rightarrow B)),$ |
| 3) $(A \& (\neg A)) \vdash B,$                        | 4) $\vdash ((A \& (\neg A)) \rightarrow B).$          |

*Д о к а з а т е л ь с т в о.* 1) Так как

$$A, (\neg A) \vdash B,$$

то, применяя два раза Теорему Дедукции, получаем

$$\vdash (A \rightarrow ((\neg A) \rightarrow B)).$$

2) Аналогичным образом устанавливается, что

$$\vdash ((\neg A) \rightarrow (A \rightarrow B)).$$

3) Так как

$$(A \& (\neg A)) \vdash A, \quad (A \& (\neg A)) \vdash (\neg A),$$

то из предыдущей теоремы 3.7 и теоремы 3.4 получаем

$$(A \& (\neg A)) \vdash B.$$

4) Применяя Теорему Дедукции, из предыдущего утверждения получаем

$$\vdash ((A \& (\neg A)) \rightarrow B).$$

□

**Теорема 3.8.** Множество формул  $\Gamma$  языка  $L_{ЛВ}$  является непротиворечивым тогда и только тогда, когда является непротиворечивым любое его конечное подмножество.

*Д о к а з а т е л ь с т в о.* Если некоторое подмножество  $\Gamma_1$  множества формул  $\Gamma$  языка  $L_{ЛВ}$  является противоречивым, то возьмем такую формулу  $A$ , что

$$\Gamma_1 \vdash A \quad \text{и} \quad \Gamma_1 \vdash (\neg A),$$

но тогда

$$\Gamma \vdash A \quad \text{и} \quad \Gamma \vdash (\neg A),$$

т.е. и само множество формул  $\Gamma$  является противоречивым.

Если противоречивым является само множество формул  $\Gamma$  языка  $L_{ЛВ}$ , то возьмем такую формулу  $A$ , что

$$\Gamma \vdash A \quad \text{и} \quad \Gamma \vdash (\neg A).$$

Пусть  $\mathcal{D}$  — вывод из множества формул  $\Gamma$  формулы  $A$ , а  $\mathcal{D}_1$  — вывод из множества формул  $\Gamma$  формулы  $(\neg A)$ .

Если  $\Gamma_1$  — это множество всех формул из множества  $\Gamma$ , входящих в  $\mathcal{D}$  или в  $\mathcal{D}_1$ , то, очевидно,

$$\Gamma_1 \vdash A \quad \text{и} \quad \Gamma_1 \vdash (\neg A).$$

Остается заметить, что  $\Gamma_1$  — конечное множество формул.

□

**Теорема 3.9.** Для любых формул  $A$ ,  $B$  и  $C$

$$(A \rightarrow B), (B \rightarrow C) \vdash (A \rightarrow C).$$

*Доказательство.* Покажем, что

$$A, (A \rightarrow B), (B \rightarrow C) \vdash C,$$

а затем применим Теорему Дедукции.

Обозначим через  $\Gamma$  множество формул

$$\{A, (A \rightarrow B), (B \rightarrow C)\}.$$

Так как

$$\Gamma \vdash A \quad \text{и} \quad \Gamma \vdash (A \rightarrow B),$$

то

$$\Gamma \vdash B.$$

А так как, кроме того,

$$\Gamma \vdash (B \rightarrow C),$$

то

$$\Gamma \vdash C.$$

Как уже отмечалось выше, для завершения доказательства остается воспользоваться Теоремой Дедукции.  $\square$

**Следствие.** Для любых формул  $A, B, C$  и любого множества формул  $\Gamma$ : если

$$\Gamma \vdash (A \rightarrow B) \quad \text{и} \quad \Gamma \vdash (B \rightarrow C),$$

то

$$\Gamma \vdash (A \rightarrow C).$$

*Доказательство.* Для доказательства достаточно воспользоваться только что доказанной теоремой 3.9 и теоремой 3.4.  $\square$

**Теорема 3.10.** Для любых формул  $A, B$  и  $C$

$$(A \rightarrow (B \rightarrow C)) \vdash (B \rightarrow (A \rightarrow C)).$$

*Доказательство.* Покажем, что

$$A, B, (A \rightarrow (B \rightarrow C)) \vdash C,$$

а затем два раза применим Теорему Дедукции.

Обозначим через  $\Delta$  множество формул

$$\{A, B, (A \rightarrow (B \rightarrow C))\}.$$

Тогда

$$\Delta \vdash A \quad \text{и} \quad \Delta \vdash (A \rightarrow (B \rightarrow C)),$$

поэтому

$$\Delta \vdash (B \rightarrow C).$$

Так как, кроме того,

$$\Delta \vdash B,$$

то

$$\Delta \vdash C.$$

Итак, доказано, что

$$A, B, (A \rightarrow (B \rightarrow C)) \vdash C,$$

поэтому по Теореме Дедукции

$$B, (A \rightarrow (B \rightarrow C)) \vdash (A \rightarrow C).$$

Еще раз применяя Теорему Дедукции, получаем

$$(A \rightarrow (B \rightarrow C)) \vdash (B \rightarrow (A \rightarrow C)).$$

□

**Следствие.** Для любых формул  $A, B$  и  $C$  и любого множества формул  $\Gamma$ : если

$$\Gamma \vdash (A \rightarrow (B \rightarrow C)),$$

то

$$\Gamma \vdash (B \rightarrow (A \rightarrow C)).$$

*Д о к а з а т е л ь с т в о* следует из предыдущей теоремы 3.10 и теоремы 3.4.  
□

**Следствие.** Для любых формул  $A, B, C$  и любого множества формул  $\Gamma$ : если

$$\Gamma \vdash (A \rightarrow (B \rightarrow C)),$$

то

$$\Gamma \vdash ((A \& B) \rightarrow C).$$

*Д о к а з а т е л ь с т в о.* Если

$$\Gamma \vdash (A \rightarrow (B \rightarrow C)),$$

то по Теореме Дедукции

$$\Gamma, A, B \vdash C.$$

Так как, кроме того,

$$A \& B \vdash A \quad \text{и} \quad A \& B \vdash B,$$



то применяя теорему 3.4, получаем

$$\Gamma, (A \& B) \vdash C.$$

Применив Теорему Дедукции, получим

$$\Gamma \vdash ((A \& B) \rightarrow C).$$

□

**Теорема 3.11.** Для любых формул  $A$  и  $B$

$$1. ((\neg B) \rightarrow (\neg A)) \vdash (A \rightarrow B),$$

$$2. (A \rightarrow B) \vdash ((\neg B) \rightarrow (\neg A)).$$

*Д о к а з а т е л ь с т в о.*

1. Используя логическую аксиому IV.1, получаем

$$\vdash (((\neg B) \rightarrow (\neg A)) \rightarrow (A \rightarrow (\neg(\neg B)))).$$

Применив два раза Теорему Дедукции, получим

$$((\neg B) \rightarrow (\neg A)), A \vdash (\neg(\neg B)).$$

Тогда в силу следствия теоремы 3.6 получаем

$$((\neg B) \rightarrow (\neg A)), A \vdash B.$$

Используя Теорему Дедукции, получаем

$$((\neg B) \rightarrow (\neg A)) \vdash A \rightarrow B.$$

2. Так как, очевидно, что

$$(A \rightarrow B), A \vdash B,$$

то в силу следствия теоремы 3.6, получаем

$$(A \rightarrow B), A \vdash (\neg(\neg B)).$$

По Теореме Дедукции получаем

$$(A \rightarrow B) \vdash (A \rightarrow (\neg(\neg B))).$$

Используя логическую аксиому II.1, получаем

$$\vdash ((A \rightarrow (\neg(\neg B))) \rightarrow ((\neg B) \rightarrow (\neg A))).$$

По Теореме Дедукции

$$(A \rightarrow (\neg(\neg B))) \vdash ((\neg B) \rightarrow (\neg A)).$$

Значит, по теореме 3.4

$$(A \rightarrow B) \vdash ((\neg B) \rightarrow (\neg A)).$$

□

**Следствие 1.** Для любых формул  $A$  и  $B$

$$1. \vdash (((\neg B) \rightarrow (\neg A)) \rightarrow (A \rightarrow B)),$$

$$2. \vdash ((A \rightarrow B) \rightarrow ((\neg B) \rightarrow (\neg A))).$$

*Д о к а з а т е л ь с т в о.* Получается применением Теоремы Дедукции.  $\square$

**Следствие 2.** Для любых формул  $A$ ,  $B$  и любого множества формул  $\Gamma$  имеют место эквивалентности

$$1. \Gamma \vdash (A \rightarrow B) \text{ тогда и только тогда, когда } \Gamma \vdash ((\neg B) \rightarrow (\neg A)).$$

$$2. \Gamma, A \vdash B \text{ тогда и только тогда, когда } \Gamma, (\neg B) \vdash (\neg A).$$

**Теорема 3.12.** Для любых формул  $A$  и  $B$

$$A, (\neg B) \vdash (\neg(A \rightarrow B)).$$

*Д о к а з а т е л ь с т в о.* Так как

$$A, (A \rightarrow B) \vdash B,$$

то по второму следствию предыдущей теоремы 3.11

$$A, (\neg B) \vdash (\neg(A \rightarrow B)).$$

$\square$

**Следствие.** Для любых формул  $A$  и  $B$

$$\vdash (A \rightarrow ((\neg B) \rightarrow (\neg(A \rightarrow B)))).$$

*Д о к а з а т е л ь с т в о.* Достаточно два раза применить Теорему Дедукции.  $\square$

**Теорема 3.13.** Для любых формул  $A$  и  $B$

$$(A \rightarrow B), ((\neg A) \rightarrow B) \vdash B.$$

*Д о к а з а т е л ь с т в о.* По теореме 3.11 получаем

$$((\neg A) \rightarrow B) \vdash ((\neg B) \rightarrow (\neg(\neg A))).$$

По Теореме Дедукции из этого следует, что

$$((\neg A) \rightarrow B), (\neg B) \vdash (\neg(\neg A)).$$

Применяя следствие теоремы 3.6, получаем

$$((\neg A) \rightarrow B), (\neg B) \vdash A.$$

Применив теорему 3.12 и теорему 3.4, получим

$$((\neg A) \rightarrow B), (\neg B) \vdash (\neg(A \rightarrow B)).$$

Применив второе следствие теоремы 3.11, получим

$$((\neg A) \rightarrow B), (A \rightarrow B) \vdash B.$$

□

**Следствие 1.** Для любых формул  $A$  и  $B$

$$\vdash ((A \rightarrow B) \rightarrow (((\neg A) \rightarrow B) \rightarrow B)).$$

*Доказательство.* Достаточно два раза применить Теорему Дедукции.  
□

**Следствие 2.** Для любой формулы  $A$

$$\vdash (A \vee (\neg A)).$$

*Доказательство.* Если в качестве формулы  $B$  взять формулу  $(A \vee (\neg A))$ , то получим

$$(A \rightarrow (A \vee (\neg A))), ((\neg A) \rightarrow (A \vee (\neg A))) \vdash (A \vee (\neg A)).$$

Заметим, что

$$\vdash (A \rightarrow (A \vee (\neg A))), \quad \vdash ((\neg A) \rightarrow (A \vee (\neg A))).$$

Поэтому по теореме 3.4 получаем

$$\vdash (A \vee (\neg A)).$$

□

**Следствие 3.** Если  $\Gamma, B \vdash A$  и  $\Gamma, (\neg B) \vdash A$ , то  $\Gamma \vdash A$ .

*Доказательство.* Если  $\Gamma, B \vdash A$  и  $\Gamma, (\neg B) \vdash A$ , то по Теореме Дедукции  $\Gamma \vdash (B \rightarrow A)$  и  $\Gamma \vdash ((\neg B) \rightarrow A)$ . И остается воспользоваться теоремой 3.4.  
□

**Теорема Кальмара.** Пусть все пропозициональные переменные, входящие в формулу  $A$ , содержатся в списке  $A_1, \dots, A_n$ .

Для произвольной интерпретации  $\varphi$  языка  $L_{ЛВ}$  и для произвольной формулы  $A$  этого языка полагаем

$$A' = \begin{cases} A, & \text{если } \varphi(A) = И, \\ (\neg A), & \text{если } \varphi(A) = Л. \end{cases}$$

Тогда

$$A'_1, \dots, A'_n \vdash A'.$$

*Доказательство.* Проведем индукцию по числу  $k$  логических связок, входящих в формулу  $A$ .

Если  $k = 0$ , то  $A$  — это некоторая пропозициональная переменная  $A_i$ .

Но тогда  $A' = A'_i$  и доказываемое утверждение принимает вид

$$A' \vdash A'.$$

Что, очевидно, верно.

Сделаем индуктивное предположение, что доказываемое утверждение выполняется для формул, содержащих менее чем  $k$  логических связок.

Пусть теперь формула  $A$  содержит  $k$  логических связок, причем  $k > 0$ .

Тогда формула  $A$  имеет один из следующих видов:

1.  $(\neg B)$ ,    2.  $(B \vee C)$ ,
3.  $(B \& C)$ ,    4.  $(B \rightarrow C)$ .

Для сокращения обозначений полагаем

$$\Gamma = \{A'_1, \dots, A'_n\}.$$

1. Пусть формула  $A$  имеет вид  $(\neg B)$ .

Если  $\varphi(A) = И$ , то  $A' = A$ .

Тогда  $\varphi(B) = Л$ , поэтому  $B' = (\neg B) = A$ .

По индуктивному предположению

$$\Gamma \vdash B',$$

т.е.

$$\Gamma \vdash A, \quad \Gamma \vdash A'.$$

Если  $\varphi(A) = Л$ , то  $A' = (\neg A)$ .

Тогда  $\varphi(B) = И$ , поэтому  $B' = B$ .

По индуктивному предположению

$$\Gamma \vdash B',$$

т.е.

$$\Gamma \vdash B.$$

Тогда по следствию теоремы 3.6

$$\Gamma \vdash (\neg(\neg B)).$$

Но  $\mathcal{A}' = (\neg(\neg B))$ , значит,

$$\Gamma \vdash \mathcal{A}'.$$

2.  $\mathcal{A} = (B \rightarrow C)$ .

Для большей наглядности построим следующую таблицу, в которой для сокращения вместо  $(\neg D)$  пишем  $\overline{D}$ .

$B$	$C$	$\mathcal{A}$	$B'$	$C'$	$\mathcal{A}'$	Инд. предпол.	Доказать
И	И	И	$B$	$C$	$\mathcal{A}$	$\Gamma \vdash B, \Gamma \vdash C,$	$\Gamma \vdash (B \rightarrow C)$
Л	И	И	$\overline{B}$	$C$	$\mathcal{A}$	$\Gamma \vdash \overline{B}, \Gamma \vdash C,$	$\Gamma \vdash (B \rightarrow C)$
И	Л	Л	$B$	$\overline{C}$	$\overline{\mathcal{A}}$	$\Gamma \vdash B, \Gamma \vdash \overline{C},$	$\Gamma \vdash \overline{(B \rightarrow C)}$
Л	Л	И	$\overline{B}$	$\overline{C}$	$\mathcal{A}$	$\Gamma \vdash \overline{B}, \Gamma \vdash \overline{C},$	$\Gamma \vdash (B \rightarrow C)$

В случаях 2.1 и 2.2 по индуктивному предположению  $\Gamma \vdash C$ . Так как  $\vdash (C \rightarrow (B \rightarrow C))$ , то  $C \vdash (B \rightarrow C)$ .

Поэтому по теореме 3.4 получаем,

$$\Gamma \vdash (B \rightarrow C).$$

В случае 2.3 воспользовавшись теоремой 3.12

$$B, (\neg C) \vdash (\neg(B \rightarrow C)),$$

индуктивным предположением

$$\Gamma \vdash B, \quad \Gamma \vdash (\neg C)$$

и теоремой 3.4 получим

$$\Gamma \vdash (\neg(B \rightarrow C)).$$

В случае 2.4 по индуктивному предположению  $\Gamma \vdash (\neg B)$ , что вместе с

$$\vdash ((\neg B) \rightarrow ((\neg C) \rightarrow (\neg B)))$$

дает

$$\Gamma \vdash ((\neg C) \rightarrow (\neg B)).$$

Отсюда по следствию 2 теоремы 3.11 получаем

$$\Gamma \vdash (B \rightarrow C).$$



3.  $A \equiv (B \& C)$ .

Вновь рассмотрим вспомогательную таблицу

$B$	$C$	$A$	$B'$	$C'$	$A'$	Инд. предпол.	Доказать
И	И	И	$B$	$C$	$A$	$\Gamma \vdash B, \Gamma \vdash C,$	$\Gamma \vdash (B \& C)$
Л	И	Л	$\bar{B}$	$C$	$\bar{A}$	$\Gamma \vdash \bar{B}, \Gamma \vdash C,$	$\Gamma \vdash \overline{(B \& C)}$
И	Л	Л	$B$	$\bar{C}$	$\bar{A}$	$\Gamma \vdash B, \Gamma \vdash \bar{C},$	$\Gamma \vdash \overline{(B \& C)}$
Л	Л	Л	$\bar{B}$	$\bar{C}$	$\bar{A}$	$\Gamma \vdash \bar{B}, \Gamma \vdash \bar{C},$	$\Gamma \vdash \overline{(B \& C)}$

В случае 3.1 по индуктивному предположению

$$\Gamma \vdash B, \quad \Gamma \vdash C,$$

по теореме 3.5 получаем

$$\Gamma \vdash (B \& C).$$

В случае 3.2 из того, что

$$\vdash ((B \& C) \rightarrow B)$$

по следствию 1 теоремы 3.11 получаем

$$\vdash ((\neg B) \rightarrow (\neg(B \& C))),$$

что вместе с индуктивным предположением  $\Gamma \vdash (\neg B)$  дает

$$\Gamma \vdash (\neg(B \& C)).$$

В случаях 3.3 и 3.4 из того, что

$$\vdash ((B \& C) \rightarrow C)$$

по следствию 1 теоремы 3.11 получаем

$$\vdash ((\neg C) \rightarrow (\neg(B \& C))),$$

что вместе с индуктивным предположением  $\Gamma \vdash (\neg C)$  дает

$$\Gamma \vdash (\neg(B \& C)).$$

4.  $A \equiv (B \vee C)$ .

Построим вспомогательную таблицу

$B$	$C$	$A$	$B'$	$C'$	$A'$	Инд. предпол.	Доказать
И	И	И	$B$	$C$	$A$	$\Gamma \vdash B, \Gamma \vdash C,$	$\Gamma \vdash (B \vee C)$
Л	И	И	$\bar{B}$	$C$	$A$	$\Gamma \vdash \bar{B}, \Gamma \vdash C,$	$\Gamma \vdash (B \vee C)$
И	Л	И	$B$	$\bar{C}$	$A$	$\Gamma \vdash B, \Gamma \vdash \bar{C},$	$\Gamma \vdash (B \vee C)$
Л	Л	Л	$\bar{B}$	$\bar{C}$	$\bar{A}$	$\Gamma \vdash \bar{B}, \Gamma \vdash \bar{C},$	$\Gamma \vdash \overline{(B \vee C)}$

В случаях 4.1 и 4.2 из

$$\vdash (C \rightarrow (B \vee C))$$

по Теореме Дедукции получаем

$$C \vdash (B \vee C).$$

Отсюда по индуктивному предположению  $\Gamma \vdash C$  с использованием теоремы 3.4 получаем

$$\Gamma \vdash (B \vee C).$$

В случае 4.3 из

$$\vdash (B \rightarrow (B \vee C))$$

и индуктивного предположения  $\Gamma \vdash B$  аналогичным образом получаем

$$\Gamma \vdash (B \vee C).$$

Рассмотрим случай 4.4. Воспользовавшись логической аксиомой III.3, получим

$$\vdash ((B \rightarrow A) \rightarrow ((C \rightarrow A) \rightarrow ((B \vee C) \rightarrow A))).$$

По Теореме Дедукции получаем

$$(B \rightarrow A), (C \rightarrow A) \vdash ((B \vee C) \rightarrow A).$$

По теореме 3.7  $(\neg B), B \vdash A$ , что вместе с индуктивным предположением  $\Gamma \vdash (\neg B)$  по теореме 3.4 дает

$$\Gamma, B \vdash A.$$

По Теореме Дедукции получаем

$$\Gamma \vdash (B \rightarrow A).$$

Аналогично показывается, что

$$\Gamma \vdash (C \rightarrow A).$$

Поэтому по теореме 3.4 получаем

$$\Gamma \vdash ((B \vee C) \rightarrow A).$$

Отсюда по следствию 2 теоремы 3.11 получаем

$$\Gamma \vdash ((\neg A) \rightarrow (\neg(B \vee C))).$$

Взяв в качестве формулы  $A$  формулу  $B$ , получим

$$\Gamma \vdash ((\neg B) \rightarrow (\neg(B \vee C))),$$

$$\Gamma, (\neg B) \vdash (\neg(B \vee C)).$$

По индуктивному предположению  $\Gamma \vdash (\neg B)$ , поэтому в силу теоремы 3.4

$$\Gamma \vdash (\neg(B \vee C)).$$

Это завершает доказательство теоремы. □

**Теорема Э. Поста.** Для любой формулы  $\mathcal{A}$  языка логики высказываний  $L_{ЛВ}$  имеет место эквивалентность:

$$\models \mathcal{A} \iff \vdash \mathcal{A}.$$

*Доказательство.* Предположим, что  $\models \mathcal{A}$ .

Пусть все пропозициональные переменные, входящие в формулу  $\mathcal{A}$ , содержатся среди  $A_1, \dots, A_n$ .

По Теореме Кальмара для любой интерпретации  $\varphi$

$$A'_1, \dots, A'_{n-1}, A_n \vdash \mathcal{A}, \quad A'_1, \dots, A'_{n-1}, (\neg A_n) \vdash \mathcal{A}.$$

Откуда по следствию 3 теоремы 3.13 получаем

$$A'_1, \dots, A'_{n-1} \vdash \mathcal{A}.$$

Продолжая рассуждение аналогичным образом, мы через  $n$  шагов получим

$$\vdash \mathcal{A}.$$

Тем самым установлено, что

$$\models \mathcal{A} \implies \vdash \mathcal{A}.$$

Чтобы показать, что

$$\vdash \mathcal{A} \implies \models \mathcal{A},$$

достаточно проверить, что для любой логической аксиомы  $\mathcal{A}$

$$\models \mathcal{A}$$

и, что, если

$$\models \mathcal{A}, \quad \models (\mathcal{A} \rightarrow B),$$

то

$$\models B.$$

Проведение указанных рассуждений предоставляется читателю в качестве простого, но полезного упражнения. □

## 4. Дополнительные вопросы Логике и Исчисления Высказываний

**Теорема адекватности.** Для любого множества формул  $\Gamma$  и любой формулы  $A$  имеет место эквивалентность:

$$\Gamma \models A \iff \Gamma \vdash A.$$

*Доказательство.* Индукцией по длине вывода формулы  $A$  из множества формул  $\Gamma$  убеждаемся в том, что если  $\Gamma \vdash A$ , то  $\Gamma \models A$ .

Для доказательства обратного утверждения рассмотрим сначала случай, когда  $\Gamma$  — конечное множество. Пусть оно состоит из формул

$$B_1, \dots, B_n$$

и  $\Gamma \models A$ , т.е.

$$B_1, \dots, B_n \models A,$$

Тогда

$$\models (B_1 \rightarrow (B_2 \rightarrow (\dots (B_n \rightarrow A) \dots))).$$

Откуда по теореме Э. Поста получаем

$$\vdash (B_1 \rightarrow (B_2 \rightarrow (\dots (B_n \rightarrow A) \dots))).$$

Применяя  $n$  раз Теорему Дедукции, получаем

$$B_1, \dots, B_n \vdash A,$$

т.е.  $\Gamma \vdash A$ .

Если  $\Gamma$  — бесконечное множество формул и  $\Gamma \models A$ , то воспользуемся следствием Теоремы Компактности, в соответствии с которым найдется конечное подмножество  $\Gamma_0$  множества  $\Gamma$  такое, что  $\Gamma_0 \models A$ . Тогда в силу уже доказанной части теоремы  $\Gamma_0 \vdash A$ , а значит, и  $\Gamma \vdash A$ . Это завершает доказательство теоремы.  $\square$

Мы дадим еще два доказательства Теоремы Адекватности, чтобы в рассматриваемой простой ситуации продемонстрировать применение двух важных приемов, используемых при изучении существенно более сложных языков, чем язык  $L_{\text{ИВ}}$  Исчисления Высказываний.

Начнем с более традиционного подхода.

**Определение 4.1.** Множество формул  $\Gamma$  языка  $L_{\text{ИВ}}$  исчисления высказываний называется **полным**, если оно непротиворечиво и для любой формулы  $A$  языка  $L_{\text{ИВ}}$

$$\Gamma \vdash A \quad \text{либо} \quad \Gamma \vdash (\neg A).$$

Предварительно докажем вспомогательную теорему.

**Теорема 4.1.** Если для множества формул  $\Gamma$  и формул  $A$  и  $B$  выполнены условия

$$\Gamma, (\neg A) \vdash B \quad \text{и} \quad \Gamma, (\neg A) \vdash (\neg B),$$

то

$$\Gamma \vdash A.$$

*Доказательство.* Если

$$\Gamma, (\neg A) \vdash B \quad \text{и} \quad \Gamma, (\neg A) \vdash (\neg B),$$

то по следствию 1 теоремы 3.7 для любой формулы  $C$  имеем

$$\Gamma, (\neg A) \vdash (\neg C).$$

Тогда по пункту 2 следствия 2 теоремы 3.11 получаем

$$\Gamma, C \vdash A.$$

Взяв в качестве формулы  $C$  любую такую формулу, что

$$\Gamma \vdash C,$$

например, в качестве такой формулы  $C$  можно взять любую логическую аксиому, получим по теореме 3.4

$$\Gamma \vdash A.$$

□

**Теорема о пополнении.** Для любого непротиворечивого множества формул  $\Gamma$  языка  $L_{\text{ИВ}}$  Исчисления Высказываний существует такое полное множество формул  $\Gamma^*$  языка  $L_{\text{ИВ}}$ , что

$$\Gamma \subseteq \Gamma^*.$$

*Доказательство.* Выше уже отмечалось, что так как алфавит языка  $L_{\text{ИВ}}$  Исчисления Высказываний счетен, то счетным является и множество  $F_{\text{ИВ}}$  всех формул **Исчисления Высказываний**.

Пусть  $F_{\text{ИВ}} = (\Phi_n)_{n \in \mathbb{N}}$ .

Определим последовательность  $(\Gamma_n)_{n \in \mathbb{N}}$  множеств формул.

Полагаем  $\Gamma_1 \Leftarrow \Gamma$ .

Если множество  $\Gamma_n$  уже определено, то полагаем

$$\Gamma_{n+1} \Leftarrow \begin{cases} \Gamma_n \cup \{\Phi_n\}, & \text{если } \Gamma_n \vdash \Phi_n \\ \Gamma_n \cup \{\neg \Phi_n\}, & \text{если } \Gamma_n \not\vdash \Phi_n \end{cases}.$$



Индукцией по  $n$  докажем, что каждое из множеств формул  $\Gamma_n$  является непротиворечивым.

Так как  $\Gamma_1 \Rightarrow \Gamma$ , то по условию теоремы множество формул  $\Gamma_1$  является непротиворечивым.

Предположим, что уже доказана непротиворечивость множества формул  $\Gamma_n$ .

Если множество формул  $\Gamma_{n+1}$  является противоречивым, то  $\Gamma_{n+1} \neq \Gamma_n$ , значит,  $\Gamma_{n+1} = \Gamma_n \cup \{(\neg\Phi_n)\}$ .

Из противоречивости множества формул  $\Gamma_{n+1}$  следует, что для любой формулы  $B$

$$\Gamma_{n+1} \vdash B \quad \text{и} \quad \Gamma_{n+1} \vdash (\neg B),$$

т.е.

$$\Gamma_n, (\neg\Phi_n) \vdash B \quad \text{и} \quad \Gamma_n, (\neg\Phi_n) \vdash (\neg B),$$

но тогда по теореме 4.1

$$\Gamma_n \vdash \Phi_n.$$

Но последнее противоречит определению множества формул  $\Gamma_{n+1}$ .

Тем самым доказано, что при любом  $n$  множество формул  $\Gamma_n$  является непротиворечивым.

Полагаем

$$\Gamma^* \Rightarrow \bigcup_{n=1}^{\infty} \Gamma_n.$$

Покажем, что  $\Gamma^*$  — полное множество формул и

$$\Gamma \subseteq \Gamma^*.$$

Последнее очевидно, так как

$$\Gamma = \Gamma_1 \subseteq \Gamma^*.$$

Если бы множество формул  $\Gamma^*$  было противоречивым, то для некоторой формулы  $B$  мы имели бы

$$\Gamma^* \vdash B \quad \text{и} \quad \Gamma^* \vdash (\neg B).$$

Но тогда найдется **конечное** множество формул  $T \subseteq \Gamma^*$  такое, что

$$T \vdash B \quad \text{и} \quad T \vdash (\neg B).$$

Так как

$$\Gamma_1 \subseteq \Gamma_2 \subseteq \dots \subseteq \Gamma_n \subseteq \Gamma_{n+1} \subseteq \dots,$$

то найдется такое число  $n$ , что  $T \subseteq \Gamma_n$ .

Но тогда

$$\Gamma_n \vdash B \quad \text{и} \quad \Gamma_n \vdash (\neg B),$$

что противоречит установленной выше непротиворечивости каждого множества формул  $\Gamma_n$ .

Докажем, что  $\Gamma^*$  — полное множество формул.

Пусть  $\mathcal{A}$  — произвольная формула. Тогда найдется такое число  $n$ , что

$$\mathcal{A} \equiv \Phi_n.$$

Если

$$\Gamma_n \vdash \Phi_n,$$

то

$$\Gamma^* \vdash \Phi_n,$$

а значит,

$$\Gamma^* \vdash \mathcal{A}.$$

Если же

$$\Gamma_n \not\vdash \Phi_n,$$

то

$$(\neg\Phi_n) \in \Gamma_{n+1},$$

поэтому

$$\Gamma_{n+1} \vdash (\neg\Phi_n),$$

значит,

$$\Gamma^* \vdash (\neg\Phi_n),$$

т.е.

$$\Gamma^* \vdash (\neg\mathcal{A}).$$

Итак, доказано, что  $\Gamma^*$  — полное (непротиворечивое) множество формул языка  $L_{\text{ИВ}}$  такое, что

$$\Gamma \subseteq \Gamma^*.$$

□

**Теорема непротиворечивости.** Для любого множества формул  $\Gamma$  языка  $L_{\text{ИВ}}$  Исчисления Высказываний имеет место эквивалентность:

множество формул  $\Gamma$  является непротиворечивым тогда и только тогда, когда оно совместно.

*Доказательство.* Начнем с доказательства более простой части теоремы: каждое совместное множество формул является непротиворечивым.

Предположим противное, т.е. что существует совместное множество формул  $\Gamma$ , являющееся противоречивым.

Тогда для некоторой формулы  $\mathcal{B}$

$$\Gamma \vdash \mathcal{B} \text{ и } \Gamma \vdash (\neg\mathcal{B}).$$

Индукцией по длине вывода из множества формул устанавливаем, что для любого множества формул  $\Gamma$  и любой формулы  $\mathcal{A}$  из

$$\Gamma \vdash \mathcal{A}$$

следует

$$\Gamma \models \mathcal{A}.$$

Так как по предположению  $\Gamma$  — совместное множество формул, то найдется такая интерпретация  $\varphi$ , что

$$\varphi(\Gamma) = \text{И}.$$

Но тогда

$$\varphi(\mathcal{B}) = \text{И} \quad \text{и} \quad \varphi(\neg \mathcal{B}) = \text{И},$$

что невозможно.

Теперь докажем более сложную часть теоремы: *каждое непротиворечивое множество формул  $\Gamma$  является совместным*.

По теореме о пополнении существует **полное** (непротиворечивое) множество формул  $\Gamma^*$  такое, что

$$\Gamma \subseteq \Gamma^*.$$

Покажем, что множество формул  $\Gamma^*$  является совместным. Отсюда, конечно, сразу будет следовать совместность и множества формул  $\Gamma$ .

Построим интерпретацию  $\varphi$  такую, что

$$\varphi(\Gamma^*) = \text{И}.$$

Полагаем для произвольной пропозициональной переменной  $A_n$

$$\varphi(A_n) = \begin{cases} \text{И}, & \text{если } \Gamma^* \vdash A_n, \\ \text{Л}, & \text{если } \Gamma^* \vdash (\neg A_n). \end{cases}$$

Напомним, что  $\Gamma^*$  — полное (непротиворечивое) множество формул, поэтому для любой формулы  $\mathcal{A}$

$$\Gamma^* \vdash \mathcal{A} \quad \text{или} \quad \Gamma^* \vdash (\neg \mathcal{A}),$$

но не то и другое одновременно, в частности, это верно и для произвольной пропозициональной переменной  $A_n$ , поэтому интерпретация  $\varphi$  определена корректно.

Обычным образом продолжаем отображение  $\varphi$ , заданное на множестве  $\Sigma_1$  пропозициональных переменных, до отображения, заданного на множестве  $F_{\text{ИВ}}$  всех формул языка  $L_{\text{ИВ}}$  Исчисления Высказываний.

Индукцией по построению формул докажем, что для произвольной формулы  $\mathcal{A}$  имеет место эквивалентность:

$$\Gamma^* \vdash \mathcal{A} \iff \varphi(\mathcal{A}) = \text{И}.$$

(i) Для элементарных формул  $\mathcal{A}$  указанная эквивалентность имеет место по определению интерпретации  $\varphi$ .

(ii) Предположим, что указанная эквивалентность имеет место для формул  $\mathcal{A}$  и  $\mathcal{B}$  и докажем, что тогда она выполняется и для формул

$$\begin{aligned} &(\neg \mathcal{A}), \quad (\mathcal{A} \& \mathcal{B}), \\ &(\mathcal{A} \vee \mathcal{B}), \quad (\mathcal{A} \rightarrow \mathcal{B}). \end{aligned}$$

Так как

$$\begin{aligned} \Gamma^* \vdash (\neg \mathcal{A}) &\iff \Gamma^* \not\vdash \mathcal{A}, \\ \Gamma^* \not\vdash \mathcal{A} &\iff \varphi(\mathcal{A}) = \text{Л} \end{aligned}$$

и

$$\varphi(\mathcal{A}) = \text{Л} \iff \varphi((\neg \mathcal{A})) = \text{И},$$

то

$$\Gamma^* \vdash (\neg \mathcal{A}) \iff \varphi((\neg \mathcal{A})) = \text{И}.$$

Так как по теореме 3.5

$$\Gamma^* \vdash (\mathcal{A} \& \mathcal{B}) \iff \Gamma^* \vdash \mathcal{A} \text{ и } \Gamma^* \vdash \mathcal{B}$$

и

$$\varphi(\mathcal{A}) = \text{И} \text{ и } \varphi(\mathcal{B}) = \text{И} \iff \varphi(\mathcal{A} \& \mathcal{B}) = \text{И},$$

то

$$\Gamma^* \vdash (\mathcal{A} \& \mathcal{B}) \iff \varphi(\mathcal{A} \& \mathcal{B}) = \text{И}.$$

Покажем, что для полного непротиворечивого множества формул  $\Gamma^*$  и произвольных формул  $\mathcal{A}$  и  $\mathcal{B}$  имеет место эквивалентность

$$\Gamma^* \vdash (\mathcal{A} \vee \mathcal{B}) \iff \Gamma^* \vdash \mathcal{A} \text{ или } \Gamma^* \vdash \mathcal{B}$$

В самом деле, если

$$\Gamma^* \vdash \mathcal{A} \text{ или } \Gamma^* \vdash \mathcal{B},$$

то, используя

$$\mathcal{A} \vdash (\mathcal{A} \vee \mathcal{B})$$

или

$$\mathcal{B} \vdash (\mathcal{A} \vee \mathcal{B}),$$

получаем, что

$$\Gamma^* \vdash (\mathcal{A} \vee \mathcal{B}).$$

Обратно, предположим, что

$$\Gamma^* \vdash (\mathcal{A} \vee \mathcal{B}).$$

Покажем, что тогда

$$\Gamma^* \vdash \mathcal{A} \text{ или } \Gamma^* \vdash \mathcal{B}.$$

Предположим противное, т.е. что

$$\Gamma^* \not\vdash \mathcal{A} \text{ и } \Gamma^* \not\vdash \mathcal{B}.$$

Так как  $\Gamma^*$  — **полное** множество формул, то тогда

$$\Gamma^* \vdash (\neg \mathcal{A}) \text{ и } \Gamma^* \vdash (\neg \mathcal{B}).$$

Воспользовавшись логической аксиомой III.3, получим

$$\vdash ((\mathcal{A} \rightarrow \mathcal{A}) \rightarrow ((\mathcal{B} \rightarrow \mathcal{A}) \rightarrow ((\mathcal{A} \vee \mathcal{B}) \rightarrow \mathcal{A}))).$$

Применяя два раза Теорему Дедукции, получим

$$(\mathcal{A} \rightarrow \mathcal{A}), (\mathcal{B} \rightarrow \mathcal{A}) \vdash ((\mathcal{A} \vee \mathcal{B}) \rightarrow \mathcal{A}).$$

Применив теорему 3.1 и теорему 3.4, получим

$$(\mathcal{B} \rightarrow \mathcal{A}) \vdash ((\mathcal{A} \vee \mathcal{B}) \rightarrow \mathcal{A}).$$

Так как по теореме 3.7

$$(\neg \mathcal{B}), \mathcal{B} \vdash \mathcal{A},$$

то применив Теорему Дедукции, получим

$$(\neg \mathcal{B}) \vdash (\mathcal{B} \rightarrow \mathcal{A}).$$

Так как

$$\Gamma^* \vdash (\neg \mathcal{B}),$$

то по теореме 3.4 получаем

$$\Gamma^* \vdash (\mathcal{B} \rightarrow \mathcal{A}),$$

что вместе с

$$(\mathcal{B} \rightarrow \mathcal{A}) \vdash ((\mathcal{A} \vee \mathcal{B}) \rightarrow \mathcal{A})$$

по теореме 3.4 дает

$$\Gamma^* \vdash ((\mathcal{A} \vee \mathcal{B}) \rightarrow \mathcal{A}).$$

По следствию 2 теоремы 3.12 получаем

$$\Gamma^* \vdash ((\neg \mathcal{A}) \rightarrow (\neg(\mathcal{A} \vee \mathcal{B}))).$$

По Теореме Дедукции получаем

$$\Gamma^*, (\neg \mathcal{A}) \vdash (\neg(\mathcal{A} \vee \mathcal{B})).$$

Так как

$$\Gamma^* \vdash (\neg \mathcal{A}),$$



то по теореме 3.4 получаем

$$\Gamma^* \vdash (\neg(\mathcal{A} \vee \mathcal{B})).$$

А так как выше мы предположили, что

$$\Gamma^* \vdash (\mathcal{A} \vee \mathcal{B}),$$

то получаем противоречие с предположением о непротиворечивости множества формул  $\Gamma^*$ .

В итоге получаем

$$\Gamma^* \vdash (\mathcal{A} \vee \mathcal{B}) \iff \Gamma^* \vdash \mathcal{A} \text{ или } \Gamma^* \vdash \mathcal{B}$$

и

$$\varphi(\mathcal{A}) = \text{И} \text{ или } \varphi(\mathcal{B}) = \text{И} \iff \varphi((\mathcal{A} \vee \mathcal{B})) = \text{И},$$

поэтому

$$\Gamma^* \vdash (\mathcal{A} \vee \mathcal{B}) \iff \varphi((\mathcal{A} \vee \mathcal{B})) = \text{И}.$$

Остается доказать эквивалентность

$$\Gamma^* \vdash (\mathcal{A} \rightarrow \mathcal{B}) \iff \varphi((\mathcal{A} \rightarrow \mathcal{B})) = \text{И}.$$

В силу полноты и непротиворечивости множества формул  $\Gamma^*$  эта эквивалентность равносильна эквивалентности

$$\Gamma^* \vdash (\neg(\mathcal{A} \rightarrow \mathcal{B})) \iff \varphi((\mathcal{A} \rightarrow \mathcal{B})) = \text{Л}.$$

Предположим, что

$$\Gamma^* \vdash (\neg(\mathcal{A} \rightarrow \mathcal{B})).$$

Покажем, что тогда

$$\Gamma^* \vdash (\neg \mathcal{B}) \quad \text{и} \quad \Gamma^* \vdash \mathcal{A}.$$

Используя логическую аксиому I.1, получаем

$$\vdash (\mathcal{B} \rightarrow (\mathcal{A} \rightarrow \mathcal{B})).$$

Применив Теорему Дедукции, получим

$$\mathcal{B} \vdash (\mathcal{A} \rightarrow \mathcal{B}).$$

По пункту 2 следствия 2 теоремы 3.11 получаем

$$(\neg(\mathcal{A} \rightarrow \mathcal{B})) \vdash (\neg \mathcal{B}),$$

что вместе с

$$\Gamma^* \vdash (\neg(\mathcal{A} \rightarrow \mathcal{B}))$$

по теореме 3.4 дает

$$\Gamma^* \vdash (\neg B).$$

По теореме 3.7

$$(\neg A), A \vdash B.$$

Применив Теорему Дедукции, получим

$$(\neg A) \vdash (A \rightarrow B).$$

Тогда по пункту 2 следствия 2 теоремы 3.11 получаем

$$(\neg(A \rightarrow B)) \vdash (\neg(\neg A)),$$

что вместе с

$$\Gamma^* \vdash (\neg(A \rightarrow B))$$

по теореме 3.4 дает

$$\Gamma^* \vdash (\neg(\neg A)).$$

Тогда по следствию теоремы 3.6 получаем

$$\Gamma^* \vdash A.$$

Итак, если

$$\Gamma^* \vdash (\neg(A \rightarrow B)),$$

то

$$\Gamma^* \vdash A$$

и

$$\Gamma^* \vdash (\neg B).$$

По индуктивному предположению тогда получаем

$$\varphi(A) = \text{И} \quad \text{и} \quad \varphi(B) = \text{Л}.$$

Значит,

$$\varphi((A \rightarrow B)) = \text{Л}.$$

Тем самым показано, что

$$\Gamma^* \vdash (\neg(A \rightarrow B)) \implies \varphi((A \rightarrow B)) = \text{Л}.$$

Чтобы доказать, что

$$\varphi((A \rightarrow B)) = \text{Л} \implies \Gamma^* \vdash (\neg(A \rightarrow B)),$$

предположим, что

$$\varphi((A \rightarrow B)) = \text{Л}.$$

Но тогда

$$\varphi(A) = И \quad и \quad \varphi(B) = Л.$$

Отсюда по индуктивному предположению получаем

$$\Gamma^* \vdash A$$

и

$$\Gamma^* \vdash (\neg B).$$

По теореме 3.12

$$A, (\neg B) \vdash (\neg(A \rightarrow B)),$$

что вместе с двумя предыдущими фактами по теореме 3.4 дает

$$\Gamma^* \vdash (\neg(A \rightarrow B)).$$

Тем самым доказано, что

$$\varphi((A \rightarrow B)) = Л \implies \Gamma^* \vdash (\neg(A \rightarrow B)).$$

В итоге доказано, что для произвольной формулы  $A$  имеет место эквивалентность:

$$\Gamma^* \vdash A \iff \varphi(A) = И.$$

Если  $A$  — произвольная формула из множества  $\Gamma^*$ , то, очевидно,

$$\Gamma^* \vdash A,$$

поэтому

$$\varphi(A) = И.$$

Значит,

$$\varphi(\Gamma^*) = И,$$

поэтому множество формул  $\Gamma^*$  является совместным. □

**Теорема адекватности.** Для любой формулы  $A$  языка  $L_{ЛВ}$  и для любого множества формул  $\Gamma$  этого языка имеет место следующая эквивалентность: формула  $A$  является логическим следствием множества формул  $\Gamma$  тогда и только тогда, когда формула  $A$  выводима из этого множества формул  $\Gamma$ .

*Доказательство.* В ходе доказательства Теоремы Непротиворечивости было показано, что если формула  $A$  выводима из множества формул  $\Gamma$ , то формула  $A$  является логическим следствием этого множества формул  $\Gamma$ .

Докажем, что верно и обратное:

если формула  $A$  является логическим следствием множества формул  $\Gamma$ , то формула  $A$  выводима из этого множества формул  $\Gamma$ .

Пусть формула  $A$  является логическим следствием множества формул  $\Gamma$ .

Тогда множество формул  $\Gamma \cup \{(\neg \mathcal{A})\}$  не является совместным. Поэтому по Теореме Непротиворечивости это множество формул является **противоречивым**, значит, для некоторой формулы  $\mathcal{B}$  имеем

$$\Gamma, (\neg \mathcal{A}) \vdash \mathcal{B} \quad \text{и} \quad \Gamma, (\neg \mathcal{A}) \vdash (\neg \mathcal{B}).$$

Но тогда по теореме 4.1

$$\Gamma \vdash \mathcal{A}.$$

□

## 5. Алгебра Линденбаума для Исчисления Высказываний

На множестве  $F_{\text{ИВ}}$  всех формул Исчисления Высказываний определим отношение  $\equiv$  полагая

$$\mathcal{A} \equiv \mathcal{B} \iff \vdash (\mathcal{A} \longleftrightarrow \mathcal{B}).$$

Используя выше доказанные теоремы (кроме теорем непротиворечивости и адекватности), нетрудно показать, что отношение  $\equiv$  является отношением эквивалентности и фактормножество множества  $F_{\text{ИВ}}$  всех формул Исчисления Высказываний по этому отношению эквивалентности превращается в булеву алгебру, если положить

$$\begin{aligned} [\mathcal{A}] \cup [\mathcal{B}] &\equiv [\mathcal{A} \vee \mathcal{B}], \\ [\mathcal{A}] \cap [\mathcal{B}] &\equiv [\mathcal{A} \& \mathcal{B}], \\ \overline{[\mathcal{A}]} &\equiv [(\neg \mathcal{A})], \\ 0 &\equiv [(\neg(\mathcal{A}_1 \vee (\neg \mathcal{A}_1)))], \\ 1 &\equiv [(\mathcal{A}_1 \vee (\neg \mathcal{A}_1))]. \end{aligned}$$

Для произвольного множества формул  $\Gamma$  полагаем

$$[\Gamma] \equiv \{[\mathcal{A}] \mid \mathcal{A} \in \Gamma\}.$$

**Теорема адекватности.** Если  $\Gamma$  — непротиворечивое множество формул и

$$\mathcal{A}_1 \in \Gamma, \dots, \mathcal{A}_n \in \Gamma,$$

то  $[\mathcal{A}_1] \cap \dots \cap [\mathcal{A}_n] \neq 0$ .

*Доказательство.* Пусть  $[\mathcal{A}_1] \in [\Gamma], \dots, [\mathcal{A}_n] \in [\Gamma]$ . Предположим, что  $[\mathcal{A}_1] \cap \dots \cap [\mathcal{A}_n] = 0$ . Тогда  $[\mathcal{A}_1 \& \dots \& \mathcal{A}_n] = 0 = [(\neg(\mathcal{A}_1 \vee (\neg \mathcal{A}_1)))]$ , поэтому

$$\Gamma \vdash ((\mathcal{A}_1 \& \dots \& \mathcal{A}_n) \longleftrightarrow (\neg(\mathcal{A}_1 \vee (\neg \mathcal{A}_1)))).$$

Значит,

$$\Gamma \vdash ((\mathcal{A}_1 \& \dots \& \mathcal{A}_n) \rightarrow (\neg(\mathcal{A}_1 \vee (\neg \mathcal{A}_1)))).$$

Тогда по следствию 2 теоремы 3.11

$$\Gamma \vdash ((\mathcal{A}_1 \vee (\neg \mathcal{A}_1)) \rightarrow (\neg(\mathcal{A}_1 \& \dots \& \mathcal{A}_n))).$$

А по Теореме Дедукции

$$\Gamma, (\mathcal{A}_1 \vee (\neg \mathcal{A}_1)) \vdash (\neg(\mathcal{A}_1 \& \dots \& \mathcal{A}_n)).$$

По следствию 2 теоремы 3.13  $\Gamma \vdash (\mathcal{A}_1 \vee (\neg \mathcal{A}_1))$ , поэтому по теореме 3.4 получаем

$$\Gamma \vdash (\neg(\mathcal{A}_1 \& \dots \& \mathcal{A}_n)).$$

Так как при любом  $i$  ( $i = 1, \dots, n$ ):  $\mathcal{A}_i \in \Gamma$ , то  $\Gamma \vdash \mathcal{A}_i$ , значит,

$$\Gamma \vdash (\mathcal{A}_1 \& \dots \& \mathcal{A}_n).$$

Но это противоречит предположению о непротиворечивости множества  $\Gamma$ .  
□

Докажем совместность любого непротиворечивого множества формул  $\Gamma$ .

Пусть  $D$  — ультрафильтр, содержащий множество  $[\Gamma]$ .

Полагаем  $\varphi(\mathcal{A}_i) = \text{И}$  тогда и только тогда, когда  $[\mathcal{A}_i] \in D$ .

По той же схеме, что и выше, доказываем справедливость эквивалентности

$$\varphi(\mathcal{A}) = \text{И} \text{ тогда и только тогда, когда } [\mathcal{A}] \in D,$$

где  $\mathcal{A}$  — произвольная формула. Проведение соответствующих рассуждений предоставляется читателю в качестве несложного полезного упражнения.

Пусть  $\mathcal{A} \in \Gamma$ , тогда  $[\mathcal{A}] \in [\Gamma] \subseteq D$ . Значит,  $\varphi(\mathcal{A}) = \text{И}$ , поэтому  $\varphi(\Gamma) = \text{И}$ . Следовательно, множество формул  $\Gamma$  совместно.





## ГЛАВА III.

# ДОПОЛНЕНИЕ

### 1. Булевы алгебры

**Определение 1.1.** Булевой алгеброй называется непустое множество  $B$ , называемое основным множеством булевой алгебры, вместе с двумя выделенными в нем элементами, обозначаемыми обычно через  $0$  и  $1$ , и с определенными на нем тремя алгебраическими операциями, одна из которых — одноместная и традиционно обозначается через  $\neg$ , а две другие — двуместные и традиционно обозначаются через  $\cap$  и  $\cup$ , для которых выполняются следующие аксиомы:

**1. Аксиомы ассоциативности:**

для любых элементов  $a, b$  и  $c$  из множества  $B$  выполняются равенства

$$a \cap (b \cap c) = (a \cap b) \cap c, \quad a \cup (b \cup c) = (a \cup b) \cup c.$$

**2. Аксиомы коммутативности:**

для любых элементов  $a$  и  $b$  из множества  $B$  выполняются равенства

$$a \cap b = b \cap a, \quad a \cup b = b \cup a.$$

**3. Аксиомы дистрибутивности:**

для любых элементов  $a, b$  и  $c$  из множества  $B$  выполняются равенства

$$a \cap (b \cup c) = (a \cap b) \cup (a \cap c), \quad a \cup (b \cap c) = (a \cup b) \cap (a \cup c).$$

**4. Аксиомы для нейтральных элементов:**

для любого элемента  $a$  из множества  $B$  выполняются равенства

$$a \cap 1 = a, \quad a \cup 0 = a.$$

**5. Аксиомы дополнения:**

для любого элемента  $a$  из множества  $B$  выполняются равенства

$$a \cap \bar{a} = 0, \quad a \cup \bar{a} = 1.$$

Обычно саму булеву алгебру обозначают через  $\mathcal{B}$ , т.е. так же как и ее основное множество, но иногда, желая подчеркнуть, что булева алгебра — это не только множество, но и выделенные в нем два элемента и определенные на нем три алгебраические операции, используют следующее обозначение

$$\langle\langle \mathcal{B} \mid \{0, 1\}, \{-\}, \{\cap, \cup\} \rangle\rangle.$$

А для сокращения указанный набор, состоящий из множества, элементов и операций, обозначают, например, через  $\mathfrak{B}$ .

Чтобы упростить обозначения, мы обычно будем обозначать булеву алгебру

$$\langle\langle \mathcal{B} \mid \{0, 1\}, \{-\}, \{\cap, \cup\} \rangle\rangle$$

через  $\mathcal{B}$ , т.е. так же, как и ее основное множество. Это не приведет к недоразумениям.

Приведем важные примеры булевых алгебр.

Зафиксируем произвольное множество  $U$ . Через  $\mathcal{P}(U)$  обозначим множество всех подмножеств множества  $U$ . Множество  $\mathcal{P}(U)$  часто называется **множеством-степенью** множества  $U$ .

Через  $0$  обозначим пустое подмножество  $\emptyset$  множества  $\mathcal{P}(U)$ , а через  $1$  — само множество  $U$ .

Операции  $\bar{\phantom{x}}$ ,  $\cap$  и  $\cup$  определим естественным образом, полагая для произвольных подмножеств  $A$  и  $B$  множества  $\mathcal{P}(U)$

$$\bar{A} \doteq U \setminus A,$$

$A \cap B$  — пересечение множеств  $A$  и  $B$ ,

$A \cup B$  — объединение множеств  $A$  и  $B$ .

Легко проверяется выполнимость аксиом булевой алгебры.

Построенная булева алгебра называется *алгеброй подмножеств* множества  $U$ .

Другие аналогичные примеры булевых алгебр получаются, если в качестве основного множества  $\mathcal{B}$  булевой алгебры взять не все множество  $\mathcal{P}(U)$ , а лишь такое его подмножество  $\mathcal{B}$ , для которого выполняются условия замкнутости относительно необходимых операций, т.е.

$$1. \emptyset \in \mathcal{B}, \quad U \in \mathcal{B},$$

$$2. \text{ если } A, B \in \mathcal{B}, \text{ то } \bar{A} \in \mathcal{B}, A \cap B \in \mathcal{B} \text{ и } A \cup B \in \mathcal{B}.$$

Например, в качестве  $\mathcal{B}$  можно взять систему, состоящую лишь из двух подмножеств  $\emptyset$  и  $U$  множества  $U$ . В этом случае мы получим важную *двуэлементную булеву алгебру*.

Покажем, что в любой булевой алгебре выполняются следующие важные равенства:

**равенства идемпотентности:**

для любого элемента  $a$  из множества  $\mathcal{B}$  выполняются равенства

$$a \cup a = a, \quad a \cap a = a$$

**и равенства поглощения:**

для любых элементов  $a$  и  $b$  из множества  $\mathcal{B}$  выполняются равенства

$$a \cap (a \cup b) = a, \quad a \cup (a \cap b) = a.$$

Доказательства равенств идемпотентности:

$$a \cup a = (a \cup a) \cap 1 = (a \cup a) \cap (a \cup \bar{a}) = a \cup (a \cap \bar{a}) = a \cup 0 = a,$$

$$a \cap a = (a \cap a) \cup 0 = (a \cap a) \cup (a \cap \bar{a}) = a \cap (a \cup \bar{a}) = a \cap 1 = a.$$

Доказательства равенств поглощения:

$$\begin{aligned} a \cap (a \cup b) &= (a \cup (b \cap \bar{b})) \cap (a \cup b) = (a \cup b) \cap (a \cup \bar{b}) \cap (a \cup b) = \\ &= (a \cup \bar{b}) \cap (a \cup b) = a \cup (\bar{b} \cap b) = a \cup 0 = a, \end{aligned}$$

$$\begin{aligned} a \cup (a \cap b) &= (a \cap (b \cup \bar{b})) \cup (a \cap b) = (a \cap b) \cup (a \cap \bar{b}) \cup (a \cap b) = \\ &= (a \cap \bar{b}) \cup (a \cap b) = a \cap (\bar{b} \cup b) = a \cap 1 = a. \end{aligned}$$

Используя равенства поглощения, покажем, что для произвольных элементов  $a$  и  $b$  булевой алгебры имеет место эквивалентность:

$$a \cap b = a \iff a \cup b = b.$$

Если  $a \cap b = a$ , то получаем  $a \cup b = (a \cap b) \cup b = b$ . Обратно, если  $a \cup b = b$ , то получаем  $a \cap b = a \cap (a \cup b) = a$ .

В произвольной булевой алгебре  $\mathcal{B}$  можно определить отношение  $\leq$  частичного порядка, положив для произвольных элементов  $a$  и  $b$  этой алгебры

$$a \leq b \iff a = a \cap b.$$

Так определенное отношение действительно является отношением частичного порядка, т.е. обладает свойствами рефлексивности, транзитивности и антисимметричности, причем  $0$  является наименьшим элементом этой алгебры, а  $1$  — ее наибольшим элементом.

1) Рефлексивность: так как  $a = a \cap a$ , то  $a \leq a$ .

2) Транзитивность: если  $a \leq b$  и  $b \leq c$ , то  $a = a \cap b$  и  $b = b \cap c$ , поэтому

$$a \cap c = (a \cap b) \cap c = a \cap (b \cap c) = a \cap b = a,$$

значит,  $a \leq c$ .

3) Антисимметричность: если  $a \leq b$  и  $b \leq a$ , то  $a = a \cap b$  и  $b = a \cap b$ , поэтому  $a = b$ .

4) В силу аксиом для нейтральных элементов: для любого элемента  $a$  из множества  $B$  выполняются равенства

$$a \cap 1 = a, \quad a \cup 0 = a,$$

значит,  $a \leq 1$  и  $0 \leq a$ .

Поэтому, если элемент  $e$  обладает свойством:  
для любого элемента  $a$  из множества  $B$  выполняются равенства

$$a \cap e = a,$$

то  $e = 1$ .

Симметричным образом, если элемент  $e$  обладает свойством:  
для любого элемента  $a$  из множества  $B$  выполняются равенства

$$a \cup e = a,$$

то  $e = 0$ .

Кроме того, для любого элемента  $a$  из множества  $B$  выполняются равенства

$$a \cup 1 = 1, \quad a \cap 0 = 0.$$

Покажем, что если для элементов  $a$  и  $b$  из множества  $B$  выполняются равенства

$$a \cap b = 0, \quad a \cup b = 1,$$

то  $b = \bar{a}$ . Это следует из следующих равенств и неравенств

$$\bar{a} = 0 \cup \bar{a} = (a \cap b) \cup \bar{a} = (a \cup \bar{a}) \cap (b \cup \bar{a}) = 1 \cap (b \cup \bar{a}) = b \cup \bar{a},$$

значит,  $b \leq \bar{a}$ ,

$$\bar{a} = 1 \cap \bar{a} = (a \cup b) \cap \bar{a} = (a \cap \bar{a}) \cup (b \cap \bar{a}) = 0 \cup (b \cap \bar{a}) = b \cap \bar{a},$$

значит,  $\bar{a} \leq b$ , поэтому  $b = \bar{a}$ .

Кроме того, выполняются равенства

$$\bar{\bar{a}} = a, \quad \overline{a \cup b} = \bar{a} \cap \bar{b}, \quad \overline{a \cap b} = \bar{a} \cup \bar{b}.$$

Это следует из следующих равенств:

$$(a \cup b) \cap (\bar{a} \cap \bar{b}) = (a \cap (\bar{a} \cap \bar{b})) \cup (b \cap (\bar{a} \cap \bar{b})) = 0,$$

$$(a \cup b) \cup (\bar{a} \cap \bar{b}) = ((a \cup b) \cup \bar{a}) \cap ((a \cup b) \cup \bar{b}) = 1.$$

Покажем, что имеют место эквивалентности

$$a \leq b \iff a \cap \bar{b} = 0$$

и

$$a \leq b \iff b \cup \bar{a} = 1.$$

Если  $a \leq b$ , то  $a \cap b = a$ , поэтому  $a \cap \bar{b} = (a \cap b) \cap \bar{b} = 0$ . Пусть  $a \cap \bar{b} = 0$ , тогда  $a = a \cap (b \cup \bar{b}) = (a \cap b) \cup (a \cap \bar{b}) = (a \cap b)$ , т.е.  $a \leq b$ .

Остается заметить, что

$$a \cap \bar{b} = 0 \iff b \cup \bar{a} = 1.$$

**Определение 1.2.** *Фильтром на булевой алгебре  $\mathfrak{B}$  называется любое непустое множество  $D$  элементов этой алгебры, для которого выполнены следующие условия:*

- 1) если  $a \in D$  и  $b \in D$ , то  $a \cap b \in D$ ;
- 2) если  $a \in D$  и  $a \leq b$ , то  $b \in D$ ;
- 3) если  $a \in D$ , то  $\bar{a} \notin D$ .

Легко понять, что условие 3) равносильно любому из следующих двух условий:

- а)  $0 \notin D$ ;
- б)  $D$  отлично от множества всех элементов булевой алгебры.

Так как для любого элемента  $a$  булевой алгебры выполнено неравенство  $a \leq 1$ , любой фильтр  $D$  содержит 1.

Приведем важные примеры фильтров в произвольной булевой алгебре  $\mathfrak{B}$ . Пусть  $a$  — произвольный, отличный от 0, элемент этой алгебры.

Через  $D(a)$  обозначим следующее множество

$$\{x \mid x \in \mathfrak{B}, a \leq x\}.$$

Легко проверить выполнимость условий 1) — 3). Фильтр  $D(a)$  называется *фильтром, порожденным элементом  $a$* . Фильтры вида  $D(a)$  называются *главными фильтрами*.

Рассмотренная конструкция обобщается следующим образом. Пусть множество  $A$  элементов булевой алгебры удовлетворяет условию:

для любого  $n > 0$  и любых элементов  $a_1, \dots, a_n$  из  $A$  элемент  $a_1 \cap \dots \cap a_n$  отличен от элемента 0.

Обозначим через  $D(A)$  следующее множество

$$\{x \mid x \in \mathfrak{B} \text{ и найдутся такое } n$$

$$\text{и такие элементы } a_1, \dots, a_n \text{ в } A, \text{ что } a_1 \cap \dots \cap a_n \leq x\}.$$

Читателю предоставляется простая проверка выполнимости условий 1) – 3). Фильтр  $D(A)$  называется *фильтром, порожденным множеством  $A$* .

Важный пример фильтра на булевой алгебре  $\mathcal{P}(U)$  подмножеств произвольного бесконечного множества  $U$  дает следующая конструкция.

Обозначим через  $\mathcal{P}_{fin-com}(U)$  множество всех подмножеств бесконечного множества  $U$ , имеющих *конечные дополнения*. Легко проверяется, что  $\mathcal{P}_{fin-com}(U)$  является фильтром.

**Определение 1.3.** Фильтр, не содержащийся ни в каком отличном от него фильтре, называется **максимальным**.

**Теорема 1.1.** Любой фильтр содержится в некотором максимальном фильтре.

*Д о к а з а т е л ь с т в о.* Для доказательства воспользуемся уже известной нам из теории множеств *Леммой Цорна*, являющейся утверждением, эквивалентным *Аксиоме Выбора*. Напомним формулировку Леммы Цорна: *если в частично упорядоченном множестве для каждого линейно упорядоченного подмножества существует верхняя грань, то в этом множестве существует максимальный элемент*.

Пусть  $D$  — фильтр на булевой алгебре  $\mathfrak{B}$ . Обозначим через  $M$  множество всех фильтров на булевой алгебре  $\mathfrak{B}$ , содержащих фильтр  $D$ . Множество  $M$  частично упорядочено отношением  $\subseteq$ . Покажем, что  $M$  удовлетворяет условию Леммы Цорна.

Пусть  $K$  — линейно упорядоченное подмножество в  $M$ . Полагаем

$$F = \bigcup_{U \in K} U.$$

Легко проверяется, что  $F$  — фильтр, являющийся расширением фильтра  $D$ , т.е.  $F \in M$ .

Очевидно,  $F$  — верхняя грань для подмножества  $K$ .

По Лемме Цорна множество  $M$  имеет максимальный элемент  $\bar{D}$ . Он и будет максимальным фильтром, содержащим фильтр  $D$ .  $\square$

**Определение 1.4.** Фильтр  $D$  на булевой алгебре называется **ультрафильтром**, если для любого элемента  $a$  этой алгебры или он сам, или его дополнение  $\bar{a}$  содержится в  $D$ .

**Определение 1.5.** Фильтр  $D$  на булевой алгебре называется **простым**, если для любых элементов  $a$  и  $b$  этой алгебры из  $a \cup b \in D$  следует, что или  $a \in D$ , или  $b \in D$ .

**Теорема 1.2.** Фильтр  $D$  на булевой алгебре является максимальным тогда и только тогда, когда он является простым, а последнее выполнено тогда и только тогда, когда фильтр  $D$  является ультрафильтром.



*Доказательство.* Покажем, что каждый максимальный фильтр  $D$  является простым.

Пусть  $D$  — максимальный фильтр. Если он не является простым, то найдутся такие элементы  $a$  и  $b$  в булевой алгебре, что

$$a \cup b \in D, \quad a \notin D, \quad b \notin D.$$

Тогда  $a \neq 0$  и  $b \neq 0$ .

Рассмотрим множество  $D_a = D \cup \{a\}$ . Покажем, что либо для любого конечного числа элементов  $a_1, \dots, a_n$  множества  $D_a$   $a_1 \cap \dots \cap a_n \neq 0$ , либо для любого конечного числа элементов  $a_1, \dots, a_n$  множества  $D_b$   $a_1 \cap \dots \cap a_n \neq 0$ .

Так как для любого конечного числа элементов  $c_1, \dots, c_m$  из  $D$   $c_1 \cap \dots \cap c_m \in D$ , то достаточно показать, что либо для любого элемента  $c$  из  $D$   $c \cap a \neq 0$ , либо для любого элемента  $c$  из  $D$   $c \cap b \neq 0$ .

Если это не так, то найдутся такие элементы  $c$  и  $d$  в  $D$ , что  $c \cap a = 0$  и  $d \cap b = 0$ . Тогда  $c = c \cap \bar{a}$ , значит,  $c \leq \bar{a}$ , что вместе с  $c \in D$  дает  $\bar{a} \in D$ .

Аналогичным образом получаем, что  $\bar{b} \in D$ .

Но тогда  $(a \cup b) = \bar{a} \cap \bar{b} \in D$ , что вместе с  $a \cup b \in D$  противоречит пункту 3) из определения фильтра.

Значит, либо для любого конечного числа элементов  $a_1, \dots, a_n$  множества  $D_a$   $a_1 \cap \dots \cap a_n \neq 0$ , либо для любого конечного числа элементов  $a_1, \dots, a_n$  множества  $D_b$   $a_1 \cap \dots \cap a_n \neq 0$ .

Допустим, что для любого конечного числа элементов  $a_1, \dots, a_n$  множества  $D_a$   $a_1 \cap \dots \cap a_n \neq 0$ .

Рассмотрим фильтр  $D(D_a)$ , порожденный множеством  $D_a$ . Тогда  $a \in D(D_a)$ . Но  $D \subseteq D(D_a)$ , а  $D$  — максимальный фильтр, значит,  $D(D_a) = D$ , а поэтому  $a \in D$ . Что противоречит предположению  $a \notin D$ . Значит, фильтр  $D$  — простой.

*Покажем, что каждый простой фильтр является ультрафильтром.*

Пусть  $D$  — простой фильтр, а  $a$  — произвольный элемент булевой алгебры. Так как  $a \cup \bar{a} = 1 \in D$ , то в силу простоты фильтра  $D$  либо  $a \in D$ , либо  $\bar{a} \in D$ , т.е. фильтр  $D$  является ультрафильтром.

*Покажем, что каждый ультрафильтр является максимальным фильтром.*

Пусть  $D$  — ультрафильтр, а  $D_1$  — содержащий его фильтр. Если  $D_1 \neq D$ , то пусть  $a \in D_1$ ,  $a \notin D$ . Так как  $D$  — ультрафильтр и  $a \notin D$ , то  $\bar{a} \in D$ , а значит,  $\bar{a} \in D_1$ , но это вместе с  $a \in D_1$  противоречит пункту 3) из определения фильтра. Тем самым теорема доказана.  $\square$

## 2. Понятие о нестандартном, или неархимедовом, анализе

Созданные более трехсот лет тому назад Исааком Ньютоном и Готфридом Вильгельмом фон Лейбницем дифференциальное и интегральное исчисления в

течение почти двух веков опирались на интуитивные представления о *бесконечно малых* и *бесконечно больших величинах*.

Г.В. Лейбниц рассматривал бесконечно малые величины как постоянные величины особого рода, сформулировал основные правила исчисления этих величин, смотрел на них как на “актуальные”, а не “потенциальные, становящиеся”. Он рассматривал бесконечно малые величины как “полезную фикцию”, не как метафизический факт, был занят изучением правил, которым они подчиняются. Г.В. Лейбниц сформулировал принцип, называемый теперь “принципом переноса Г.В. Лейбница”, в соответствии с которым “идеальные числа” должны обладать теми же свойствами, что и “конечные числа”.

Введение в математику в конце XVII века (работа Г.В. Лейбница была опубликована в 1684 году) бесконечно малых и бесконечно больших величин явилось одним из источников *второго кризиса оснований математики*, вызвало многочисленные споры и дискуссии по вопросу законности и обоснованности использования этих понятий. Последователи И. Ньютона и Г.В. Лейбница весьма свободно обращались с расплывчатыми понятиями бесконечно малых и бесконечно больших величин, складывали бесконечные суммы слагаемых по правилам, верным для конечных сумм, например, свободно пользовались коммутативностью и ассоциативностью для бесконечных рядов. С другой стороны, основные понятия дифференциального и интегрального исчисления казались весьма туманными математикам, воспитанным на античной строгости. В качестве примера рассмотрим вычисление производной функции  $y = x^2$  в точке  $x$ . Дадим  $x$  *бесконечно малое* приращение  $dx$ , т.е. перейдем от точки  $x$  к точке  $x + dx$ , вычислим отношение  $dy/dx$  *бесконечно малого* приращения  $dy$  функции  $y$  к *бесконечно малому* приращению  $dx$  аргумента  $x$ , получим  $dy/dx = 2x + dx$ . Так как  $dx$  бесконечно мало, то, отбросив его, получим  $dy/dx = 2x$ . Критики этого рассуждения могли сказать, что отбрасывание слагаемого  $dx$  — это просто приравнивание его нулю, но тогда и  $dy$  равно нулю и отношение  $dy/dx$  теряет смысл, откуда же тогда возникает производная? Однако успехи нового исчисления в решении старых, казавшихся неприступными, математических проблем заставляли отбрасывать сомнения. Характерно в этом отношении высказывание Жана Д’Аламбера (1717–1783 гг.) “Идите вперед, и вера к вам придет”. Дифференциальное и интегральное исчисления позволили решить разнообразные как чисто математические, так и прикладные задачи. В качестве примеров первого типа можно указать на задачи, связанные с нахождением экстремальных значений функций, вычислением площадей и объемов, а в качестве примеров второго типа — расчет траектории артиллерийского снаряда, предсказание движения планет и комет. Однако основа тогдашнего математического анализа — понятие *бесконечно малой величины* казалось стоящим на грани бытия и небытия, чем-то вроде нуля, но не нуля. В конце XVIII века появились первые признаки неблагополучия — некорректное использование бесконечно малых и бесконечно больших величин стало приводить к противоречиям.

В конце XVIII века Д’Аламбер для разрешения противоречий предпринял попытку обоснования исчисления бесконечно малых на основе понятия предела.

В конце XIX века под влиянием авторитета К. Вейерштрасса (1815–1897) метод “ $\varepsilon - \delta$ ” стал основным инструментом “взятия пределов” в математическом анализе. Хотя Б. Больцано (1781–1848) на пятьдесят лет раньше предложил аналогичный метод, по ему не было в то время уделено достаточно внимания.

К концу XIX века понятия *актуально* бесконечно большой и бесконечно малой величин были заменены идеей предела и понятиями *потенциально* бесконечно большой и бесконечно малой величин. Разносторонняя деятельность Огюстена Коши (1789–1857 гг.), систематически использовавшего пределы, которые он определял на основе бесконечно малых величин, обеспечила определенную связь между позицией автора первого руководства по исчислению бесконечно малых Лопиталя, трактовавшего бесконечно малые величины как “метафизический” факт, и “ $\varepsilon - \delta$ ”-позицией К. Вейерштрасса. Многие годы после К. Вейерштрасса безраздельно господствовал “ $\varepsilon - \delta$ ”-метод, сложилось представление о невозможности непротиворечивой трактовки бесконечно малых величин. Однако в середине XX века подход Г.В. Лейбница был “реабилитирован” — в работах Абрахама Робинсона под понятие бесконечно малой величины был подведен достаточно прочный фундамент современной математической логики. При этом А. Робинсону удалось сохранить интуитивную привлекательность бесконечно малых величин. По мнению ряда математиков, обоснования А. Робинсоном лейбницевого понятия бесконечно малой величины является одним из величайших результатов математики XX века. Язык и методы нестандартного анализа позволяют сделать доказательства ряда теорем короче и прозрачнее. Кроме того, язык нестандартного анализа — удобное средство для построения математических моделей физических явлений.

Рассмотрим один из вариантов расширения поля действительных чисел  $\mathbb{R}$  до поля  $\mathbb{R}^*$  гипердействительных чисел, содержащего бесконечно малые и бесконечно большие величины и удовлетворяющего уточненному варианту принципа переноса Лейбница.

Пусть  $F$  — *неглавный ультрафильтр* на множестве  $\mathbb{N}$  натуральных чисел.

Обозначим через  $\mathbb{R}^{\mathbb{N}}$  множество всех последовательностей действительных чисел. Элементы из  $\mathbb{R}^{\mathbb{N}}$  будем обозначать через  $f$ ,  $(f_n)_{n \in \mathbb{N}}$  или через  $(f(n))_{n \in \mathbb{N}}$ .

На множестве  $\mathbb{R}^{\mathbb{N}}$  всех последовательностей действительных чисел введем отношение  $\equiv_F$ :

для  $f \in \mathbb{R}^{\mathbb{N}}$  и  $g \in \mathbb{R}^{\mathbb{N}}$  полагаем

$$f \equiv_F g \iff \{n \mid f(n) = g(n)\} \in F.$$

Очевидно, отношение  $\equiv_F$  обладает свойствами рефлексивности и симметричности.

Для установления транзитивности предположим, что  $f \equiv_F g$  и  $g \equiv_F h$ . Тогда

$$\{n \mid f(n) = g(n)\} \in F \ \& \ \{n \mid g(n) = h(n)\} \in F.$$

Поэтому

$$\{n \mid f(n) = g(n)\} \cap \{n \mid g(n) = h(n)\} \in F.$$

Но

$$\{n \mid f(n) = g(n)\} \cap \{n \mid g(n) = h(n)\} \subseteq \{n \mid f(n) = h(n)\},$$

значит,

$$\{n \mid f(n) = h(n)\} \in F,$$

т.е.  $f \equiv_F h$ .

Обозначим через  $\mathbb{R}^*$  фактормножество множества  $\mathbb{R}^{\mathbb{N}}$  всех последовательностей действительных чисел по отношению эквивалентности  $\equiv_F$ .

Для произвольного действительного числа  $a$  через  $f_a$  обозначим постоянную последовательность, все члены которой равны  $a$ . Чтобы не усложнять обозначений соответствующий класс эквивалентности  $[f_a]_{\equiv_F}$  будем обозначать через  $a$ .

Через  $-[f]$  обозначим класс  $[-f]$ .

На множестве  $\mathbb{R}^*$  естественным образом определяются операция сложения  $+$  и операция умножения  $\cdot$ .

$$[f] + [g] = [f + g], \quad [f] \cdot [g] = [f \cdot g].$$

В качестве упражнения читателю предоставляется проверить, что система

$$\langle \langle \mathbb{R}^*, 0, 1, +, \cdot \rangle \rangle$$

является полем, т.е. выполнены аксиомы поля

- I. 1.1.  $\alpha + \beta = \beta + \alpha$ .  
 1.2.  $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ .  
 1.3.  $\alpha + 0 = \alpha$ .  
 1.4.  $\alpha + (-\alpha) = 0$ .

Если  $[f] \neq 0$ , то  $\{n \mid f(n) = 0\} \notin F$ .

Так как  $F$  — ультрафильтр, то  $\{n \mid f(n) \neq 0\} \in F$ .

Для произвольной последовательности действительных чисел  $f$  полагаем

$$\bar{f}(n) = \begin{cases} 1/f(n), & \text{если } f(n) \neq 0, \\ 1, & \text{в противном случае.} \end{cases}$$

Для произвольного  $[f] \neq 0$  обозначим через  $[f]^{-1}$  класс  $[\bar{f}]$ . Читателю предоставляется проверка, что определение класса  $[f]^{-1}$  не зависит от выбора в нем представителя  $f$ .

- II. 2.1.  $\alpha \cdot \beta = \beta \cdot \alpha$ .  
 2.2.  $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$ .  
 2.3.  $\alpha \cdot 1 = \alpha$ .  
 2.4.  $\alpha \cdot (\alpha^{-1}) = 1$ .
- III. 3.1.  $(\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma$ .

Введем на поле  $\mathbb{R}^*$  отношение  $<$  полагая

$$[f] < [g] \iff \{n \mid f(n) < g(n)\} \in F.$$

Читателю предоставляется проверить, что определение отношения  $<$  не зависит от выбора представителей  $f$  и  $g$  в классах  $[f]$  и  $[g]$ . При этом выполняются следующие свойства

- IV. 4.1.  $\alpha \not< \alpha$ .  
 4.2. Если  $\alpha < \beta$  и  $\beta < \gamma$ , то  $\alpha < \gamma$ .  
 4.3. Для любых  $\alpha$  и  $\beta$ : или  $\alpha < \beta$ , или  $\alpha = \beta$ , или  $\beta < \alpha$ .  
 4.4. Если  $\alpha < \beta$ , то  $\alpha + \gamma < \beta + \gamma$ .  
 4.5. Если  $\alpha < \beta$  и  $0 < \gamma$ , то  $\alpha \cdot \gamma < \beta \cdot \gamma$ .

Выполнимость условий I–IV означает, что система

$$\langle \langle \mathbb{R}^*, 0, 1, +, \cdot, < \rangle \rangle$$

является упорядоченным полем. Элементы этого поля называются гипердействительными числами.

Отображение  $a \mapsto [f_a]$  является изоморфным вложением упорядоченного поля действительных чисел

$$\langle \langle \mathbb{R}, 0, 1, +, \cdot, < \rangle \rangle$$

в упорядоченное поле гипердействительных чисел

$$\langle \langle \mathbb{R}^*, 0, 1, +, \cdot, < \rangle \rangle.$$

Наличие указанного вложения позволяет нам, как это часто делается в математике, отождествить действительное число  $a$  с гипердействительным числом  $[f_a]$ , в частности, мы отождествляем натуральное число  $n$  с гипердействительным числом  $[f_n]$ .

Для произвольного натурального числа  $n$  и произвольного действительного (гипердействительного) числа  $\alpha$  через  $n\alpha$  будем обозначать сумму  $n$  слагаемых, каждое из которых равно  $\alpha$ .

Для действительных чисел выполняется **Аксиома Архимеда**: для любого положительного действительного числа  $\alpha$  и любого действительного числа  $\beta$  найдется такое натуральное число  $n$ , что  $n\alpha > \beta$ .

Поэтому говорят, упорядоченное поле действительных чисел

$$\langle \langle \mathbb{R}, 0, 1, +, \cdot, < \rangle \rangle$$

является архимедовым.

Покажем, что упорядоченное поле гипердействительных чисел

$$\langle \langle \mathbb{R}^*, 0, 1, +, \cdot, < \rangle \rangle$$

не является архимедовым.

Докажем, что для любого конечного подмножества  $K$  множества  $\mathbb{N}$  натуральных чисел  $K \not\subseteq F$ .



Допустим противное, пусть  $K = \{a_1, \dots, a_n\}$  — конечное подмножество множества  $\mathbb{N}$  натуральных чисел и  $K \in F$ . Значит,

$$\{a_1\} \cup \dots \cup \{a_n\} \in F.$$

Так как  $F$  — простой фильтр, то найдется такое  $i$ , что  $\{a_i\} \in F$ . Нетрудно понять, что тогда  $F = D(\{a_i\})$ , т.е. фильтр  $F$  является главным. А это противоречит выбору фильтра  $F$ .

Так как  $F$  — ультрафильтр, то любое множество натуральных чисел, имеющее конечное дополнение, принадлежит  $F$ .

Пусть  $\alpha = 1 = [f_1]$ , где при любом  $m$   $f_1(m) = 1$ ,  $\beta = [g]$ , где при любом  $m$   $g(m) = m$ . Ясно, что  $\alpha > 0$ .

Заметим, что  $n\alpha = [f_n]$ . Если  $n$  — произвольное натуральное число, то множество

$$\{m \mid f_n(m) = n < m = g(m)\}$$

имеет конечное дополнение, значит, лежит в  $F$ . Следовательно, при любом  $n$  выполняется неравенство  $n\alpha < \beta$ . А это означает, что аксиома Архимеда не выполнена для упорядоченного поля гипердействительных чисел.

Гипердействительное число  $\beta$  естественно назвать *бесконечно большим*.

Полагаем  $\varepsilon = \beta^{-1} = [\bar{g}]$ , где при любом  $m$   $\bar{g}(m) = 1/m$ . Пусть  $1/n = [f_{1/n}]$ . Тогда  $\varepsilon > 0$  и для любого натурального числа  $n$  выполняется неравенство

$$0 < \varepsilon < 1/n.$$

Гипердействительное число  $\varepsilon$  естественно назвать *бесконечно малым* положительным гипердействительным числом.

Так как при любом натуральном  $n$  выполняется неравенство  $n < 1/\varepsilon$ , то множество натуральных чисел в  $\mathbb{R}^*$  ограничено сверху, в то время, как в  $\mathbb{R}$  оно не было ограничено сверху.

Любую  $m$ -местную функцию  $f(x_1, \dots, x_m)$ , определенную на  $\mathbb{R}^m$  и принимающую значения в  $\mathbb{R}$ , можно преобразовать в  $m$ -местную функцию  $f^*(x_1, \dots, x_m)$ , определенную на  $(\mathbb{R}^*)^m$  и принимающую значения в  $\mathbb{R}^*$ . Для этого полагаем

$$f^*([(g^{(1)}(n))_{n \in \mathbb{N}}], \dots, [(g^{(m)}(n))_{n \in \mathbb{N}}]) \Rightarrow [(f(g^{(1)}(n)), \dots, f(g^{(m)}(n)))_{n \in \mathbb{N}}].$$

При этом любое равенство  $A(f_1, \dots, f_k) = B(f_1, \dots, f_k)$ , справедливое для обычных числовых функций  $f_1, \dots, f_k$ , преобразуется в равенство  $A(f_1^*, \dots, f_k^*) = B(f_1^*, \dots, f_k^*)$ , связывающее гиперфункции  $f_1^*, \dots, f_k^*$ .

Любой  $m$ -местный предикат  $p(x_1, \dots, x_m)$ , определенный на  $\mathbb{R}^m$ , можно преобразовать в  $m$ -местный предикат  $p^*(x_1, \dots, x_m)$ , определенный на  $(\mathbb{R}^*)^m$ :

$$p^*([(g^{(1)}(n))_{n \in \mathbb{N}}], \dots, [(g^{(m)}(n))_{n \in \mathbb{N}}]) = \text{И} \iff \{n \mid p(g^{(1)}(n), \dots, g^{(m)}(n)) = \text{И}\} \in F.$$

Предикат  $p^*$  называется *гиперрасширением* предиката  $p$ .



Для произвольной формулы  $\Phi$ , построенной из элементарных формул вида  $f(x_1, \dots, x_n) = g(x_1, \dots, x_n)$ , где  $f(x_1, \dots, x_n)$  и  $g(x_1, \dots, x_n)$  — произвольные определенные на  $\mathbb{R}$   $n$ -местные функции, и вида  $p(x_1, \dots, x_m)$ , где  $p(x_1, \dots, x_m)$  — определенный на  $\mathbb{R}$   $m$ -местный предикат, с помощью пропозициональных связок  $\neg$ ,  $\wedge$  и  $\vee$  и кванторов  $\forall$  и  $\exists$  обозначим через  $\Phi^*$  формулу, полученную из формулы  $\Phi$  заменой элементарных подформул вида  $f(x_1, \dots, x_n) = g(x_1, \dots, x_n)$  на  $f^*(x_1, \dots, x_n) = g^*(x_1, \dots, x_n)$ , а вида  $p(x_1, \dots, x_m)$  — на  $p^*(x_1, \dots, x_m)$ .

**Принцип переноса Г.В. Лейбница.** Если все свободные переменные формулы  $\Phi$  входят в список  $x_1, \dots, x_n$ , а  $\alpha_1, \dots, \alpha_n$  — произвольные действительные числа, то формула  $\Phi_{x_1, \dots, x_n}[\alpha_1, \dots, \alpha_n]$  истинна на  $\mathbb{R}$  тогда и только тогда, когда на  $\mathbb{R}^*$  истинна формула  $\Phi_{x_1, \dots, x_n}^*[\alpha_1, \dots, \alpha_n]$

Доказательство этой теоремы требует введения ряда понятий математической логики, что будет сделано в следующей части пособия.

## ПОСЛЕСЛОВИЕ

В планах автора написание в следующем году продолжения пособия, в котором будут рассмотрены логика и исчисление предикатов, включая знаменитые теоремы К. Геделя о полноте и о неполноте, приведены некоторые сведения о нестандартном, или неархимедовом, анализе.

Завершить пособие мне хотелось бы теми же словами, которыми Алексей Иванович Кострикин завершил свою прекрасную книгу “Введение в алгебру. Часть I. Основы алгебры”:

*“Еще многое имею сказать вам,  
но вы теперь не можете вместить”.*

Евангелие от Иоанна, 16:12

# Литература

- [1] *Адян С.И., Дурнев В.Г.* Алгоритмические проблемы для групп и полугрупп // Успехи матем. наук. 2000. Том 55. В2. С.3–94.
- [2] *Архангельский А.В.* Канторовская теория множеств. М.: Изд-во МГУ, 1988.
- [3] *Ахо А., Хопкрофт Дж., Ульман Дж.* Построение и анализ вычислительных алгоритмов. М.: Мир, 1983.
- [4] *Булос Дж., Джефффри Р.* Вычислимость и логика. М.: Мир, 1994.
- [5] *Бурбаки Н.* Начала математики. Первая часть. Основные структуры анализа. Книга первая. Теория множеств. М.: Мир, 1965.
- [6] *Верецагин Н.К., Шень А.* Начала теории множеств. М.: Изд-во МЦНМО, 1999.
- [7] *Верецагин Н.К., Шень А.* Языки и исчисления. М.: Изд-во МЦНМО, 2000.
- [8] *Гордон Е.И., Полотовский Г.М.* Мощность бесконечных множеств. Нижний Новгород: Изд-во НГУ, 1998.
- [9] *Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. М.: Мир, 1979.
- [10] *Девис М.* Прикладной нестандартный анализ. М.: Мир, 1980.
- [11] *Дурнев В.Г.* Элементы теории множеств и математической логики. Ярославль, 1978.
- [12] *Ершов Ю.Л., Палютин Е.А.* Математическая логика. М.: Наука, 1979.
- [13] *Ивс Г., Ньюсом К.В.* О математической логике и философии математики. М.: Изд-во Знание, 1968.
- [14] *Йех Т.Дж.* Об аксиоме выбора // Справочная книга по математической логике. Часть II. Теория множеств. Под редакцией Дж. Барвайса. М.: Наука, 1982. С.35–63.
- [15] *Столл Р.* Множества, логика, аксиоматические теории. М.: Просвещение, 1968.

- [16] *Катленд Н.* Вычислимость. Введение в теорию рекурсивных функций. М.: Мир, 1983.
- [17] *Клини С.К.* Математическая логика. М.: Мир, 1973.
- [18] *Клини С.К.* Введение в метаматематику. М.: ИЛ, 1957.
- [19] *Косовский Н.К.* Элементы математической логики и ее приложения к теории субрекурсивных предикатов. Л.: Изд-во ЛГУ, 1981.
- [20] *Колмогоров А.Н., Драгалин А.Г.* Введение в математическую логику. М.: Изд-во МГУ, 1982.
- [21] *Колмогоров А.Н., Драгалин А.Г.* Математическая логика. Дополнительные главы. М.: Изд-во МГУ, 1984.
- [22] *Козн П.Джс.* Теория множеств и континуум-гипотеза. М.: Мир, 1969.
- [23] *Куратовский К., Мостовский А.* Теория множеств. М.: Мир, 1970.
- [24] *Лавров И.А., Максимова Л.Л.* Задачи по теории множеств, математической логике и теории алгоритмов. М.: Наука, 1975.
- [25] *Мальцев А.И.* Алгоритмы и рекурсивные функции. М.: Наука, 1986.
- [26] *Манин Ю.И.* Доказуемое и недоказуемое. М.: Советское радио, 1979.
- [27] *Манин Ю.И.* Вычислимое и невычислимое. М.: Советское радио, 1979.
- [28] *Марков А.А., Нагорный Н.М.* Теория алгоритмов. М.: Наука, 1984.
- [29] *Марков А.А.* Элементы математической логики. М.: Изд-во МГУ, 1984.
- [30] *Мендельсон Э.* Введение в математическую логику. М.: Наука, 1976.
- [31] *Натансон И.П.* Теория функций вещественной переменной. М.: Наука, 1974.
- [32] *Новиков П.С.* Элементы математической логики. М.: Наука, 1973.
- [33] *Серпинский В.* О теории множеств. М.: Просвещение, 1966.
- [34] *Трахтенброт Б.А.* Алгоритмы и вычислительные автоматы. М.: Советское радио, 1974.
- [35] *Успенский В.А.* Нестандартный, или неархимедов, анализ. М.: Знание, 1983.
- [36] *Успенский В.А.* Нестандартный, или неархимедов, анализ. М.: Наука, 1988.
- [37] *Фефферман С.* Числовые системы. М.: Наука, 1971.

- [38] *Френкель А., Бар-Хиллел И.* Основания теории множеств. М.: Мир, 1966.
- [39] *Шенфилд Дж.* Математическая логика. М.: Наука, 1975.
- [40] *Чень Ч., Ли Р.* Математическая логика и автоматическое доказательство теорем. М.: Наука, 1983.
- [41] *Черч А.* Введение в математическую логику. Т.1. М.: ИЛ, 1960.
- [42] *Эббингауз Г.Д., Якобс К., Ман Ф.К., Хермес Г.* Машины Тьюринга и рекурсивные функции. М.: Мир, 1972.
- [43] *Энгелер Э.* Метаматематика элементарной математики. М.: Мир, 1987.
- [44] *Jech T.* The Axiom of Choice. Amsterdam: North-Holland, 1973.
- [45] *Churh A.* An unsolvable problem of elementary number theory // Amer. J. Math. 1936. Vol.58. B2. P.345–363.
- [46] *Churh A.* A note on the Entscheidungsproblem // J. Symbolic Logic. 1936. Vol.1. B1. P.40–41.
- [47] *Post E.L.* Finite combinatory processes — formulation 1 // Journal of Symbolic Logic. 1936. Vol.1. B3. P.103–105.
- [48] *Quine W.* Concatenation as a basis for arithmetic // J. Symbol Log. 1946. Vol.11. P.105–114.
- [49] *Turing A.M.* On computable numbers, with an application to the Entscheidungsproblem // Proceedings of London Mathematical Society. Ser.2. 1936. Vol.42. B3, 4. P.230–265.

УЧЕБНОЕ ИЗДАНИЕ

Дурнев Валерий Георгиевич

ВВЕДЕНИЕ В МАТЕМАТИЧЕСКУЮ ЛОГИКУ

Учебное пособие

Редактор, корректор А.А. Аладьева

Компьютерная верстка М.А. Башкин

Подписано в печать 09.06.05. Формат 60 × 84 1/8.

Бумага тип. Офсетная печать.

Усл. печ. л. 21,85. Уч.-изд. л. 10,0. Тираж 150 экз.

Заказ 157.

Оригинал-макет подготовлен в редакционно-издательском отделе ЯрГУ  
150000 Ярославль, ул. Советская, 14

Отпечатано ООО "Ремдер" ЛР ИД 06151 от 26.10.01  
г. Ярославль, пр. Октября, 94, оф. 37, тел. (0852) 73-35-03