

[section]

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

В. Г. ДУРНЕВ

ЭЛЕМЕНТЫ ТЕОРИИ МНОЖЕСТВ И МАТЕМАТИЧЕСКОЙ ЛОГИКИ

УЧЕБНОЕ ПОСОБИЕ

*Рекомендовано Учебно-методическим советом по математике и механике
Учебно-методического объединения по классическому университетскому
образованию РФ*

*в качестве учебного пособия для студентов высших учебных заведений,
обучающихся по специальности "Математика" и по направлениям
"Математика" и "Математика. Прикладная математика."*

ЯРОСЛАВЛЬ 2009

УДК 51 + 519.2
ББК В 12 я 73
Д 84

Рекомендовано
Редакционно-издательским советом университета
в качестве учебного издания. План 2009 года

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

Дурнев, В.Г. Элементы теории множеств и математической логики: учеб.
пособие / В. Г. Дурнев; Яросл. гос. ун-т. им. П. Г. Демидова. Ярославль, 2009.
457 с.

ISBN 978-5-8397-0660-6

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

Пособие предназначено для студентов, обучающихся по направлениям 510100 "Математика" и 511200 "Математика. Прикладная 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 и математическая логика" (блок ОПД, ЕН), а также специальных дисциплин.

Библиогр.: 48 назв.

ISBN 978-5-8397-0660-6
УДК 51 + 519.2
ББК В 12 я 73
Д 84

©Ярославский государственный университет
им. П. Г. Демидова, 2009
©В. Г. Дурнев, 2009

ОГЛАВЛЕНИЕ

Предисловие	5
I. ЭЛЕМЕНТЫ ТЕОРИИ МНОЖЕСТВ	11
1.1. Множества и операции над ними	11
1.2. Соответствия, отношения и функции	18
1.3. Некоторые специальные отношения	31
1.4. Равномощность множеств	42
1.5. Конечные и счетные множества	49
1.6. Множества мощности континуум	54
1.7. Операции над кардинальными числами	59
1.8. Вполне упорядоченные множества	61
1.9. Натуральные числа. Системы Пеано	84
1.9.1. Системы Пеано	84
1.9.2. Рекурсивные определения в системах Пеано	89
1.9.3. Определения сложения и умножения натуральных чисел	92
1.10. Некоторые приложения аксиомы выбора	94
II. ЛОГИКА И ИСЧИСЛЕНИЕ ВЫСКАЗЫВАНИЙ	111
2.1. Алфавиты. Слова	111
2.2. Логика Высказываний	113
2.3. Исчисление Высказываний	131
2.4. Дополнительные вопросы Логике и Исчисления Высказываний	152
2.5. Алгебра Линденбаума для Исчисления Высказываний	163
2.6. Метод резолюций для Логике Высказываний	164
2.7. Независимость систем аксиом	167
2.8. Исчисление Секвенций	173
2.9. Другие аксиоматизации для Логике Высказываний	178
2.10. Интуиционистское Исчисление Высказываний	182
III. ЛОГИКА И ИСЧИСЛЕНИЕ ПРЕДИКАТОВ	199
3.1. Языки первого порядка	199
3.2. Логика Предикатов	206
3.3. Фильтрованные произведения	228
3.4. Понятие о нестандартном, или неархимедовом, анализе	236
3.5. Исчисление Предикатов	242
3.5.1. Логические аксиомы и правила вывода	242
3.5.2. Теорема дедукции	250
3.5.3. Теорема К. Геделя о полноте	265
3.6. Логика первого порядка с равенством	285
3.7. Исчисление Предикатов с равенством	304
3.7.1. Логические аксиомы и правила вывода	304
3.7.2. Теорема адекватности для Исчисления Предикатов с равенством	309

3.8. Аксиоматическая теория множеств и формальная арифметика . .	314
3.9. Теоремы Д. Кенига и Ф. Рамсея	319
3.10. Разрешимость логики одноместных предикатов	339
3.11. Неразрешимость логики двуместных предикатов	346
IV. ДОПОЛНЕНИЕ	359
4.1. Булевы алгебры	359
4.2. Фильтры на булевых алгебрах	366
4.3. Псевдобулевы алгебры	370
4.4. Из истории математики и логики	374
4.4.1. Из истории математики	374
4.4.2. Из истории логики	387
Послесловие	408
Литература	409

ПРЕДИСЛОВИЕ

Трудно, на наш взгляд, оспорить утверждение, что *значительная часть математики XX века базировалась на теоретико-множественном фундаменте*. И в начале XXI века, 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.

XX век был периодом бурного развития математической логики, в рамках которой аксиоматический метод изложения математических теорий, ведущий свое начало от древнегреческих математиков, был доведен до своего логического завершения — были формализованы, выражены на подходящем формальном языке, не только основные положения ряда математических теорий, но и логические средства доказательства теорем в этих теориях. *Была установлена возможность формализации самой логики математических рассуждений, что позволило сделать процесс доказательства математических теорем объектом математического изучения*. В этот же период установилась тесная связь математической логики с исследованиями в области оснований математики, с ее философскими вопросами. В рамках математической логики была разработана теория формальных языков, что сыграло, в частности, важнейшую роль при разработке языков программирования. *Именно в математической логике было выработано математическое уточнение интуитивного понятия алгоритма*, которым к тому времени математики пользовались уже более двух тысяч лет. Это позволило установить *существование неразрешимых алгоритмических проблем* во многих разделах математики. *В настоящее время математическая логика имеет свой предмет и методы исследования*, играет важную роль как в различных разделах математики, так и в ее приложениях,

в частности в информатике.

К середине XX века математическая логика достигла немалых успехов в постановке и решении принципиально новых математических проблем. Она действительно стала, как говорил П. С. Порецкий, *логикой по предмету, математикой по методу*. В рамках математической логики было предложено точное математическое определение понятия “доказательство”, что позволило *поставить вопросы о доказуемости и недоказуемости* тех или иных математических утверждений. Были разработаны и методы установления недоказуемости. Это позволило, в частности, К. Геделю и П. Дж. Коэну доказать, что знаменитая *континуум-гипотеза Г. Кантора не зависит от остальных аксиом* общепринятых на сегодняшний день вариантов *аксиоматической теории множеств*.

Приведем мнения ряда авторитетных математиков о роли математической логики в конце XX века.

Дж. Шенфильд: “...математическая логика является не собранием разрозненных результатов, а действенным методом изучения некоторых наиболее интересных проблем, стоящих перед математиками.” (“Математическая логика”. М.: Наука, 1975.)

Э. Мендельсон: “Глубокие и опустошительные результаты Геделя, Тарского, Черча, Россера, Клини и многих других были богатой наградой за вложенный труд и завоевали для математической логики положение независимой ветви математики.” (“Введение в математическую логику”. М.: Наука, 1971.)

При работе над пособием автором преследовалась цель — попытаться изложить с единых позиций основную, по его мнению, материал по теории множеств и математической логике, необходимый и в то же время в идейном отношении доступный студентам I–III 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 — доказательства некоторых теорем, конечно, можно сократить, однако при этом, по мнению автора, может пострадать ясность и несколько затрудниться понимание смысла проводимых построений. А ведь понимание доказательства включает в себя, прежде всего, понимание общей идеи доказательства, которая реализуется через этапы доказательства. Начинаяшему изучать предмет часто бывает проще понять длинное доказательство, в котором легко просматривается мотивировка каждого шага, чем краткое доказательство, основанное на оригинальной идее. В последнем случае возникает вопрос “Почему так?”. Конечно, после неоднократного использования оригинальная когда-то идея становится рабочим инструментом, и вопрос отпадает сам собой — эта идея становится частью нашего общего образования. Но, по нашему мнению, надо стремиться

ся максимально облегчить труд начинающего читателя, а не ошеломлять его "фейерверками мысли". Насколько это нам удалось — судить читателю. Автор сделал, что мог, пусть другие сделают больше.

При написании пособия в той или иной мере 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. Включенный в пособие материал можно считать, в основном, уже достаточно устоявшимся, ставшим общематематическим достоянием. Хотя время от времени и появляются оригинальные доказательства известных в этой области теорем.

О содержании пособия можно понять по его достаточно подробному оглавлению. Приведем краткий обзор глав пособия.

Первая глава "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. То есть мы как бы пытаемся повозможности полно сформулировать "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, вовремя 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 отно-

шения 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 замечательной 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.

Вторая глава ”Логика и Исчисление Высказываний” посвящена рассмотрению Логике и Исчисления Высказываний. Она 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 Логике 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 Логике Предикатов*. Эта теорема, особенно ее доказательство, конечно, трудна для студентов младших курсов. Однако в случае Логике 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 Высказы-

ваний 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.

В третьей главе "Логика и Исчисление Предикатов" рассматриваются основные вопросы Логики и Исчисления Предикатов. Вводится понятие языка первого порядка, его синтаксиса и семантики. Основными изучаемыми понятиями являются *понятие интерпретации, истинностного значения замкнутой формулы в интерпретации, понятие логического следствия, вывода и вывода из множества гипотез*. Изложение достаточно целенаправленное — оно ориентировано на доказательство основной теоремы третьей главы пособия — *теоремы К. Геделя о полноте*. Это и определило отбор соответствующего материала.

Заканчивается глава доказательством *алгоритмической неразрешимости проблем тождественной истинности и выполнимости для Логики двуместных предикатов*.

В "Дополнении" приведены некоторые основные сведения о булевых алгебрах и фильтрах. Заканчивается пособие некоторыми, на наш взгляд, полезными сведениями из истории развития теории множеств и математической логики, сведениями о некоторых их создателях, чтобы у читателя не складывалось впечатление, что "теория множеств и математическая логика существовала вечно" и была создана не известно кем. Чтобы студент понимал, что изучаемое им было создано конкретными людьми, которым мы должны отдать дань уважения за их вклад в развитие общечеловеческой культуры.

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

ГЛАВА 1.

ЭЛЕМЕНТЫ ТЕОРИИ МНОЖЕСТВ

*”Я считаю, что она (теория множеств) представляет собой
высочайшее проявление математического гения,
а также одно из самых высоких достижений
чисто духовной деятельности человека.”*

*”Никто не изгонит нас из рая,
созданного для нас Кантором”*
Д. Гильберт

1.1. Множества и операции над ними

Начало канторовской, или, как иногда говорят, ”наивной”, теории множеств было положено открытиями, содержащимися в публикациях Г. Кантора 1871–1883 г.г. 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 заинтересовал 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 и даже встретили сопротивление со стороны некоторых весьма авторитетных математиков. Особенно яростной критике они были подвергнуты Л. Кронекером. Однако позже теоретико-множественные идеи 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. В настоящее время теория множеств служит фундаментом таких разделов современной математики, как теория функций действительного переменного, общая алгебра, топология, функциональный анализ, геометрия, теория 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*", "*отношение*", "*отображение*", "*функция*" 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, в той или иной мере 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 приходим 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, обозна-*

ченный 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 "А или В" или "дизъюнкция А, В";

каждый из знаков \wedge и $\&$ является сокращением (обозначением) для союза "и" и называется "конъюнкцией", формула $(A \wedge B)$ читается "А и В" или "конъюнкция А, В";

знак \Rightarrow служит сокращением для "если ..., то..." и называется "импликацией", формула $(A \Rightarrow B)$ читается "если А, то В", или "из А следует В", или "А имплицирует В";

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

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

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

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

З а м е ч а н и е. 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. рефлексивность: $(\forall x)(x = x)$;
2. симметричность: $(\forall x)(\forall y)(x = y \Rightarrow y = x)$;
3. транзитивность: $(\forall x)(\forall y)(\forall z)(x = y \wedge y = z \Rightarrow x = z)$;
4. правило замены: $(\forall x)(\forall y)(x = y \Rightarrow (\forall z)(x \in z \Leftrightarrow y \in z))$;
5. правило замены: $(\forall x)(\forall y)(x = y \Rightarrow (\forall z)(z \in x \Leftrightarrow z \in y))$.

Первые три формулы выражают обычные свойства равенства – *рефлексивность, симметричность и транзитивность*, 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 или постулатами***

теории множеств или ее **нелогическими аксиомами**. Эти принципы мы будем вводить постепенно, ориентируясь на систему аксиом Цермело – Френкеля **ZF**. Однако введем мы не все традиционно включаемые в эту систему аксиомы, 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

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

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 удается 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 1.1.1. Если каждый элемент множества X является элементом множества Y , т. е. если

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

то множество X называется **подмножеством** множества 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 1.1.2. Если X – произвольное множество, то через $P(X)$ будем обозначать множество, элементами которого являются всевозможные подмножества множества X и только они, т. е.

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

Множество $P(X)$ часто называется **множеством-степенью** множества X и обозначается через 2^X .

В силу принципа объемности для каждого множества X множество $P(X)$ единственно, если вообще оно существует.

В дальнейшем мы считаем, что верен

Принцип существования множества-степени. Для любого множества X существует множество $P(X)$ всех его подмножеств (множество-степень).

Определение 1.1.3. 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 верен

Принцип существования пустого множества. Пустое множество существует.

Введем следующее соглашение:

знак \Rightarrow в формуле $A \Rightarrow B$ означает, что " A есть по определению B ", знак \Rightarrow 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 1.1.4. *Объединением* множеств A и B называется множество

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

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

Определение 1.1.5. 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 1.1.6. *Объединением* семейства $(A_i)_{i \in I}$ множеств, называется следующее множество:

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

Мы приходим к следующему принципу (соглашению).

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

Ясно, что объединение двух множеств A и B можно рассматривать как объединение семейства

$$(A_i)_{i \in I}, \text{ где } I = \{1, 2\}, A_1 = A, A_2 = B.$$

Определение 1.1.7. *Пересечением* семейства $(A_i)_{i \in I}$ множеств называется множество

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

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

Определение 1.1.8. *Пересечением* множеств A и B называется множество

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

Ясно, что $A \cap B$ – это пересечение семейства

$$(A_i)_{i \in I}, \text{ где } I = \{1, 2\}, A_1 = A, A_2 = B.$$

Определение 1.1.9. *Разностью* множеств A и B называется множество

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

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.

Принцип выделения подмножества.

Для произвольного множества X и условия $P(x)$ существует множество

$$\{x \mid x \in X \wedge P(x)\}.$$

Принцип выделения подмножества гарантирует для произвольного множества X существование в нем подмножества, состоящего из всех элементов x , для которых выполнено условие $P(x)$. При этом мы пока не уточняем, какие условия $P(x)$ допустимо рассматривать.

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) $A \cup (B \cup C) = (A \cup B) \cup C$,
 $A \cap (B \cap C) = (A \cap B) \cap C$;
- 4) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
- 5) $(A \cup B) \cap A = A$, $A \cup (B \cap A) = A$,

доказательства 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 1.1.1. *Имеют место следующие равенства, носящие название **формул двойственности** (законы де Моргана):*

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

Д о к а з а т е л ь с т в о. 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 $x \in \bigcup_{i \in I} A_i$, 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,

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

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

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

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

1.2. 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.

Для произвольных объектов a и b через $\{a, b\}$ обозначается множество, элементами которого являются a и b и только они. Это множество называется **неупорядоченной парой** элементов a и b .

Если неупорядоченная пара объектов существует, то в силу **принципа объемности** она единственна.

Принцип существования неупорядоченной пары элементов.

Для произвольных объектов a и b существует их **неупорядоченная пара** $\{a, b\}$.

Определение 1.2.1. 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, показывает следующая теорема.

Теорема 1.2.1. Для любых a, b, c, d

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

До к а з а т е л ь с т в о. 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

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

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

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 $a = c$. \square

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

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

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

Индукцией по n доказывается следующая теорема, являющаяся обобщением теоремы 1.2.1.

Теорема 1.2.2. *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 1.2.2. *Прямое (декартовое) произведение множеств A_1, \dots, A_n называется следующее множество:*

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

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 1.2.3. *Любое подмножество R прямого произведения $A_1 \times \dots \times A_n$ множеств A_1, \dots, A_n ($R \subseteq A_1 \times \dots \times A_n$) называется n -местным **отношением на множествах A_1, \dots, A_n** .*

Если $\langle a_1, \dots, a_n \rangle \in R$, то говорят, что элементы a_1, \dots, a_n *находятся в отношении* R и пишут $R(a_1, \dots, a_n)$.

В случае, когда $A_1 = \dots = A_n = A$ и $R \subseteq A^n = A \times \dots \times A$, R называется n -местным **отношением на множестве** A .

В этом пособии основное внимание будет уделено двуместным или бинарным отношениям, т. е. случаю $n = 2$. В этой ситуации несколько расширим понятие двуместного отношения, не определяя заранее множества, на которых оно определено.

Определение 1.2.4. Любое множество R упорядоченных пар называется **двуместным или бинарным отношением или соответствием**.

Таким образом, R – **бинарное отношение (соответствие)**, если для любого $x \in R$ найдутся такие u и v , что $x = \langle u, v \rangle$.

Если для **бинарного отношения (соответствия)** 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** или **соответствием из A в A** .

Если $\langle u, v \rangle \in R$, то говорят, что элементы u и v **находятся в отношении** R или элементу u **соответствует** элемент v (при соответствии R), и пишут $u R v$.

С каждым соответствием (бинарным отношением) R естественным образом связаны два множества, называемые **областью определения** и соответственно **областью значений** (областью изменения) соответствия (бинарного отношения) R .

Определение 1.2.5. **Областью определения** соответствия (бинарного отношения) R называется следующее множество:

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

обозначаемое через $D(R)$, а в некоторых случаях – через $\delta(R)$.

Определение 1.2.6. **Областью значений** соответствия (бинарного отношения) R называется следующее множество:

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

обозначаемое через $E(R)$, а в некоторых случаях – через $\rho(R)$.

Ясно, что для любого соответствия (бинарного отношения) R :

$$R \subseteq D(R) \times E(R)$$

и множества $D(R)$ и $E(R)$ минимальны в том смысле, что если

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

то $D(R) \subseteq A$ и $E(R) \subseteq B$.

Определение 1.2.7. С каждым соответствием R естественным образом связывается соответствие R^c , называемое **обращением соответствия** R (или **обратным соответствием** для соответствия R)

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

Ясно, что

$$D(R^c) = E(R), \quad E(R^c) = D(R), \quad (R^c)^c = R.$$

Над соответствиями (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 соответствиями (бинарными отношениями), называемую **умножением соответствий (отношений)**, а именно по соответствиям (отношениям) R и S можно следующим образом определить новое отношение, называемое **произведением (композицией) соответствий (отношений) R и S** .

Определение 1.2.8. *Произведением (композицией) соответствий (отношений) R и S называется следующее соответствие (отношение)*

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

Ясно, что

$$D(R \circ S) \subseteq D(S), \quad E(R \circ S) \subseteq E(R).$$

Определение 1.2.9. *Соответствие (бинарное отношение) R называется **отображением** или **функцией**, если для любых x, y и 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** соответствия (отношения) R .

Если R – отображение, $A = D(R)$, $B \supseteq E(R)$, 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 $x \in A = D(R)$ найдется единственный элемент $y \in B$ такой, что $\langle x, y \rangle \in R$ (или в других обозначениях xRy), 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 1.2.10. Отображение (функция) R называется **1-1-отображением (1-1-функцией)**, если для любых x_1 и x_2 из $D(R)$ равенство

$$R(x_1) = R(x_2)$$

влечет равенство $x_1 = x_2$.

З а м е ч е н и е. 1-1-отображение называется еще **инъективным отображением** или **инъекцией**.

Теорема 1.2.3. Для того чтобы обращение R^c отображения (функции) само было отображением (функцией), необходимо и достаточно, чтобы отображение (функция) R было 1-1-функцией.

Д о к а з а т е л ь с т в о. Пусть R^c – функция. Покажем, что R – 1-1-отображение. Если $x_1, x_2 \in D(R)$ 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 и 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 1.2.4. Если R и S – отображения (функции), то $R \circ S$ – отображение (функция).

Д о к а з а т е л ь с т в о. Если x, y и z – такие элементы, что

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

то найдутся такие элементы u и v , что

$$\begin{aligned} x S u, & \quad u R y, \\ x S v, & \quad v R z. \end{aligned}$$

Так как S – отображение, то из $x S u$ и $x S v$ следует, что $u = v$.

Тогда, так как R – отображение, то из $u R y$ и $u R z$ следует, что $y = z$. \square

З а м е ч а н и е 1. Если $E(S) \subseteq D(R)$, то $D(R \circ S) = D(S)$. Если же $E(S) = D(R)$, то $E(R \circ S) = E(R)$.

З а м е ч а н и е 2. Если R и S – отображения, то, как только что доказано, $R \circ S$ тоже является отображением. Пусть $x \in D(R \circ S)$, 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

$$\langle x, v \rangle \in S \text{ и } \langle v, (R \circ S)(x) \rangle \in R,$$

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 1.2.5. Если R и S – инъективные отображения, то $R \circ S$ – инъективное отображение.

Д о к а з а т е л ь с т в о. По теореме 1.2.3 $R \circ S$ – отображение, значит, остается доказать его инъективность. Если u и v – такие элементы из $D(R \circ S)$, 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

$$u = v.$$

□

Рассмотрим наиболее важные для дальнейшего виды отображений.

Определение 1.2.11. Отображение f множества A во множество B называется **инъективным отображением (инъекцией, вложением)**, если для любых u и v из A из того, что $u \neq v$, следует, что $f(u) \neq f(v)$.

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

Определение 1.2.12. *Образование 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 $f : A \rightarrow B$ будет служить для сокращенного обозначения утверждения " f – **инъективное отображение множества A во множество B** ".

Определение 1.2.13. *Образование f множества A во множество B называется **сюръективным отображением (сюръекцией, отображением на)**, если $E(f) = B$, 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 1.2.6. *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 .*

Д о 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 1.2.14. *Образование 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** .

З а м е ч а н и е. Если R – биективное отображение множества A на множество B , то будем говорить, что R осуществляет **взаимнооднозначное соответствие** между множествами A и B .

Теорема 1.2.7. *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 .*

Д о к а з а т е л ь с т в о. сразу следует из теоремы 1.2.4 и теоремы 1.2.5. \square

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

Определение 1.2.15. Для произвольного множества X обозначим через id_X следующее отображение

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

Легко понять, что id_X — биективное отображение множества X на себя.

id_X называется **тождественным отображением множества X на себя**.

Определение 1.2.16. 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

$$S \circ R = id_A, \quad R \circ S = id_B.$$

З а м е ч а н и е. 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

$$S \circ R = id_A, \quad R \circ S = id_B,$$

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

Теорема 1.2.8. 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. $R^{-1} = R^c$.

Д о к а з а т е л ь с т в о. 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

$$S \circ R = id_A, \quad R \circ S = id_B.$$

Покажем, что R — биекция.

Прежде всего убедимся в инъективности R .

Если u и 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

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

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

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

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

Для доказательства обратного утверждения предположим, что

$$R : A \rightarrow B \text{ — биективное отображение}$$

множества A на множество B .

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

По теореме 1.2.2 R^c – отображение, а так как

$$D(R^c) = E(R) = B,$$

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

$$R \circ S = id_B, \quad S \circ R = id_A$$

предоставляется читателю в качестве простого упражнения. □

В качестве некоторого дополнения к только что доказанной теореме 1.2.7 может рассматриваться следующая теорема.

Теорема 1.2.9. *Для того, чтобы отношение R между элементами множеств A и B осуществляло **взаимнооднозначное соответствие** между A и B необходимо и достаточно, чтобы выполнялись равенства*

$$R \circ R^c = id_B, \quad R^c \circ R = id_A.$$

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

$$R \circ R^c = id_B, \quad R^c \circ R = id_A.$$

Чтобы доказать обратное утверждение, предположим, что выполняются равенства

$$R \circ R^c = id_B, \quad R^c \circ R = id_A.$$

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 $D(R_c \circ R) \subseteq D(R)$, то $D(id_A) \subseteq D(R)$. Но $D(id_A) = A$, значит, $A \subseteq D(R)$, что вместе с $D(R) \subseteq A$ дает равенство $D(R) = A$.

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

$$R \circ R^c = id_B, \quad R^c \circ R = id_A,$$

то R – **обратимое отображение** множества A во множество B , поэтому по теореме 1.2.7 R – **биекция**. \square

Теорема 1.2.10. Для любых бинарных отношений R, S и U выполняются следующие равенства

- (1) $(R \circ S) \circ U = R \circ (S \circ U)$,
- (2) $(R \circ S)^c = S^c \circ R^c$.

Д о к а з а т е л ь с т в о. Докажем равенство (1).

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

Докажем равенство (2).

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

\square

Определение 1.2.17. Пусть R – соответствие (бинарное отношение), а X – произвольное множество. **Образом** множества X относительно R называется следующее множество

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

Прообразом множества X относительно R называется следующее множество

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

З а м е ч а н и е. 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 1.2.11. Для любого отношения R имеют место следующие равенства и включения:

$$(1) R\left(\bigcup_{i \in I} A_i\right) = \bigcup_{i \in I} R(A_i);$$

$$(2) R\left(\bigcap_{i \in I} A_i\right) \subseteq \bigcap_{i \in I} R(A_i);$$

$$(3) R^{-1}\left(\bigcup_{i \in I} A_i\right) = \bigcup_{i \in I} R^{-1}(A_i);$$

$$(4) \text{ если } R \text{ — функция, то } R^{-1}\left(\bigcap_{i \in I} A_i\right) = \bigcap_{i \in I} R^{-1}(A_i);$$

$$(5) \text{ если } A \subseteq B, \text{ то } R(A) \subseteq R(B);$$

$$(6) \text{ если } A \subseteq B, \text{ то } R^{-1}(A) \subseteq R^{-1}(B).$$

Д о к а з а т е л ь с т в о. (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

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

Пусть $x \in \bigcup_{i \in I} R(A_i)$, тогда при некотором 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

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

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

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

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

Напомним, что n -местное отношение на множестве A – это 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 $\langle a_1, \dots, a_n \rangle$.

Одним из основных понятий математической логики является понятие n -местного предиката.

Определение 1.2.20. n -местным предикатом, определенным на множестве A , называется любая n -местная функция из множества A во множество $\{\mathbf{И}, \mathbf{Л}\}$, состоящее из двух элементов $\mathbf{И}$ – "истина", $\mathbf{Л}$ – "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

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

1.3. Некоторые специальные отношения

Одним из важнейших двуместных отношений является **отношение эквивалентности**.

Определение 1.3.1. Отношением эквивалентности или просто эквивалентностью на множестве A называется каждое двуместное отношение R на множестве A , т. е. $R \subseteq A \times A$, 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 Δ_A так называемую диагональ множества A , положив

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

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

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

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

Определение 1.3.3. *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 1.3.1. (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) $A = \bigcup_{a \in A} [a]$.

До к а з а т е л ь с т в о. (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 1.3.2. *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 $b \in B$.

Д о к а з а т е л ь с т в о. 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, $[a] = B$. \square

Определение 1.3.4. *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 1.3.3. *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 1.3.4. *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 $xR_{\mathcal{U}}u$, значит, и xR_Yu . 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 1.3.5. *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 $R_{\mathcal{U}} = R$. \square

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: для произвольных $\alpha, \beta \in \mathbb{R}$ 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: для произвольных $\alpha, \beta \in \mathbb{R}$ 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

$$\mathbb{N} \equiv \{1, 2, \dots, n, \dots\} -$$

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 .

$$[\langle a, b \rangle] + [\langle c, d \rangle] \equiv [\langle a + c, b + d \rangle],$$

$$[\langle a, b \rangle] \cdot [\langle c, d \rangle] \equiv [\langle ac + bd, bc + ad \rangle].$$

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 :

$$[\langle a, b \rangle] + [\langle c, d \rangle] \equiv [\langle ad + cb, bd \rangle],$$

$$[\langle a, b \rangle] \cdot [\langle c, d \rangle] \equiv [\langle ac, bd \rangle].$$

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 *сходящейся к нулю последовательности*.

Определение 1.3.5. Последовательность $(r_n)_{n \in \mathbb{N}}$ рациональных чисел называется *фундаментальной*, если для любого положительного рационального числа ε 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 1.3.6. Последовательность $(r_n)_{n \in \mathbb{N}}$ рациональных чисел называется *сходящейся к нулю*, если для любого положительного рационального числа ε 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

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

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

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

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

Система $\langle \mathbb{R}, +, \cdot \rangle$ называется *полем действительных чисел*. Кроме того, это поле можно упорядочить, т. е. определить двуместное отношение \leq порядка таким образом, что \mathbb{R} станет *непрерывно архимедовски упорядоченным полем*. Архимедовость означает, что множество натуральных чисел неограничено в \mathbb{R} , а непрерывность – любая фундаментальная последовательность действительных чисел, т. е. элементов из \mathbb{R} , имеет в \mathbb{R} предел. Детали можно найти в книгах по математическому анализу.

Построение по полю действительных чисел \mathbb{R} поля комплексных чисел \mathbb{C} осуществляется еще проще.

Обозначим через \mathbb{C} множество $\mathbb{R} \times \mathbb{R}$ упорядоченных пар действительных чисел.

Определим на множестве \mathbb{C} операции сложения $+$ и умножения \cdot :

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

Читателю предоставляется в качестве упражнения проверить, что множество \mathbb{C} вместе с так определенными операциями сложения $+$ и умножения \cdot является *полем*, причем отображение $f : a \mapsto \langle a, 0 \rangle$ задает изоморфное вложение поля действительных чисел \mathbb{R} в это поле.

Система $\langle \mathbb{C}, +, \cdot \rangle$ называется *полем комплексных чисел*.

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

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

Наряду с традиционным обозначением $a \equiv b \pmod{m}$ будем использовать и обозначение $a \equiv_m b$.

Легко проверить, что это отношение \equiv_m является отношением эквивалентности. Оно называется *отношением сравнимости* или *равноостаточности по модулю m* . Для произвольного целого числа a через $\text{rem}(a, m)$ обозначим *остаток* при делении a на m , т. е. это такое неотрицательное число r , что $0 \leq r < m$ и для некоторого целого числа q выполняется равенство $a = mq + r$.

Для произвольных целых чисел a и b выполняется эквивалентность

$$a \equiv b \pmod{m} \iff \text{rem}(a, m) = \text{rem}(b, m).$$

Фактормножество \mathbb{Z}/\equiv_m множества целых чисел \mathbb{Z} по отношению эквивалентности \equiv_m обычно обозначается через \mathbb{Z}_m или $\mathbb{Z}(m)$ и называется множеством классов вычетов по модулю m .

На множестве \mathbb{Z}_m классов вычетов по модулю m естественным образом определяются операции сложения $+$ и умножения \cdot .

$$[a] + [b] \Rightarrow [a + b], \quad [a] \cdot [b] \Rightarrow [ab].$$

Читателю предоставляется в качестве упражнения проверить, что множество \mathbb{Z}_m классов вычетов вместе с так определенными операциями сложения $+$ и умножения \cdot является *кольцом*, причем отображение $f : a \mapsto [a]$ задает гомоморфизм кольца целых чисел на это кольцо.

По каждому бинарному отношению R на множестве A , т. е. $R \subseteq A \times A$, естественным образом строится его **рефлексивное замыкание** $RefCl(R)$

$$RefCl(R) \Rightarrow R \cup \{ \langle a, a \rangle \mid a \in A \}$$

и его **симметричное замыкание** $SimCl(R)$

$$SimCl(R) \Rightarrow R \cup R^c.$$

Ясно, что $RefCl(R)$ – минимальное относительно включения бинарное рефлексивное отношение на множестве A , содержащее R .

$SimCl(R)$ – минимальное относительно включения бинарное симметричное отношение на множестве A , содержащее R .

Несколько сложнее определяется **транзитивное замыкание**

$$TrCl(R)$$

отношения R .

Для произвольного натурального числа n определим n -ую степень отношения R , полагая

$$R^1 \Rightarrow R, \quad R^2 \Rightarrow R \circ R, \quad R^{n+1} \Rightarrow R^n \circ R.$$

Тогда

$$TrCl(R) \Rightarrow \bigcup_{n=1}^{\infty} R^n.$$

Ясно, что $TrCl(R)$ – минимальное относительно включения бинарное транзитивное отношение на множестве A , содержащее R . Поэтому $TrCl(R)$ – это пересечение всех бинарных транзитивных отношений на множестве A , содержащих R .

В некоторых ситуациях **транзитивное замыкание** $TrCl(R)$ отношения R определяется следующим образом:

для произвольных элементов a и b множества A полагают

$a \operatorname{TrCl}(R) b$ тогда и только тогда, когда

существует такое неотрицательное целое число n

и такие элементы $a_1, a_2, \dots, a_{n-1}, a_n$ множества A , что

$$aRa_1, a_1Ra_2, \dots, a_{n-1}Ra_n, a_nRb.$$

Тогда $\operatorname{TrCl}(\operatorname{SimCl}(R))$ – **симметричное, транзитивное замыкание** отношения R , т. е. минимальное относительно включения бинарное симметричное, транзитивное отношение на множестве A , содержащее R ,

$\operatorname{TrCl}(\operatorname{RefCl}(R))$ – **рефлексивное, транзитивное замыкание** отношения R , т. е. – минимальное относительно включения бинарное рефлексивное, транзитивное отношение на множестве A , содержащее R .

Тогда $\operatorname{TrCl}(\operatorname{SimCl}(\operatorname{RefCl}(R)))$ – **рефлексивное, симметричное, транзитивное замыкание** отношения R , т. е. – минимальное относительно включения бинарное рефлексивное, симметричное, транзитивное отношение на множестве A , содержащее R .

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

Определение 1.3.7. *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 тоже обозначается 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 **нестромого частичного порядка**, так как оно обладает свойством рефлексивности. Полагая

$$a < b \iff a \leq b \text{ \& } a \neq b,$$

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 рассуждения с отношения строгого частичного порядка $<$ как произвольного двуместного отношения, обладающего свойством транзитивности и антирефлексивности, и получить отношение \leq нестромого 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

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

Определение 1.3.8. 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 1.3.9. 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 1.3.10. 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 1.3.11. 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 1.3.12. 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. В этом случае для любых a и b из $P(A)$, т. е. подмножеств множества A , $a \cup b$ – это обычное объединение множеств, а $a \cap b$ – их пересечение.

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 1.3.13. 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 1.3.14. 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.

1.4. 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 1.4.1. 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 равномощны". 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 N – множество всех натуральных чисел, а B – множество всех четных натуральных чисел. Тогда функция $f(x) = 2x$ устанавливает равномощность множеств N и B . Из этого примера видно, что бесконечное множество может быть равномощно своему собственному подмножеству. Что невозможно для конечных множеств.

Теорема 1.4.1. Для любых множеств A и B выполняются следующие утверждения:

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

Доказательство. (1) Равномощность множества A самому себе устанавливает функция id_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 понятия 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 $\overline{\overline{A}}$ для обозначения мощности множества. Конечно, приведенное только что пояснение 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 принципиальных 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 о соотношениях между ними, справедливость же этих соотношений можно доказать при помощи понятия равномощности. Однако формулировки многих теорем 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 $\overline{\overline{A}}$, называемый *кардинальным числом* или *мощностью* множества A , причем множества A и B равномощны тогда и только тогда, когда $\overline{\overline{A}} = \overline{\overline{B}}$.

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

Определение 1.4.2. *Мощность множества A не больше мощности множества B , если существует инъективное отображение множества A во множество B .*

Запись $\overline{\overline{A}} \leq \overline{\overline{B}}$ 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 $\overline{\overline{A}} = \overline{\overline{B}}$.*

Д о к а з а т е л ь с т в о. 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

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

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

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

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 $\overline{A} = \overline{B}$. \square

Рассмотрим еще одно доказательство этой важной теоремы следуя пособию Е. И. Гордона и Г. М. Полотовского [7]. Предварительно докажем интересное и важное утверждение, носящее название **Лемма А. Тарского**.

Определение 1.4.3. *Отображение φ 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 1.4.4. *Если φ – отображение в себя произвольного множества W , а A^* – такой элемент этого множества, что $\varphi(A^*) = A^*$, то A^* называется **неподвижной точкой** отображения φ .*

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

Д о 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 φ 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 φ . Если B – произвольное множество из M , то $A^* \subseteq B$, откуда в силу монотонности отображения φ 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 A , что

$$A^* = A \setminus g(B \setminus f(A^*)).$$

Рассмотрим отображение φ в себя множества $P(A)$ всех подмножеств множества A , заданное равенством

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

Нетрудно проверить, что φ – 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 1.4.5. *Мощность $\overline{\overline{A}}$ множества A меньше мощности $\overline{\overline{B}}$ множества B , если $\overline{\overline{A}} \leq \overline{\overline{B}}$ и $\overline{\overline{A}} \neq \overline{\overline{B}}$.*

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 : $\overline{\overline{A}} \not< \overline{\overline{A}}$ (антифлексивность $<$);
- (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 $<$).

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 $\overline{\overline{A}} < \overline{\overline{P(A)}}$.*

Д о к а з а т е л ь с т в о. 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 φ – произвольное отображение множества A во множество $P(A)$. Рассмотрим следующее подмножество D_φ 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_φ 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_φ 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 φ не является сюръективным.

Это завершает доказательство теоремы Г. Кантора. \square

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

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

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. Лишь заметим, 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, доказательство которой, однако, использует **Аксиому выбора**.

Теорема 1.4.2. *Если существует сюръективное отображение множества A на множество B , то мощность B не превосходит мощности A .*

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

$$A_b \triangleq \{a \mid f(a) = b\}.$$

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 (аксиома выбора гарантирует возможность такого выбора). Тогда легко понять, что отображение φ , заданное равенством $\varphi(b) \triangleq a_b$, является вложением множества B во множество A . Это завершает доказательство теоремы. \square

1.5. 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 1.5.1. *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 1.5.1. *Подмножество конечного множества само является конечным множеством.*

Теорема 1.5.2. *Объединение конечного числа конечных множеств само является конечным множеством.*

Теорема 1.5.3. *Если A – конечное множество из n элементов, а B – конечное множество из m элементов, то $A \times B$ – конечное множество из nm элементов.*

Теорема 1.5.4. *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 1.5.2. Множество A , не являющееся конечным, называется **бесконечным**.

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

Определение 1.5.3. Множество A , равномощное множеству \mathbb{N} натуральных чисел, называется **счетным**. Его мощность обозначается через \aleph_0 .

Теорема 1.5.5. 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

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

□

Следствие 1.5.5.1. Прямое произведение конечного числа счетных множеств само является счетным множеством.

Теорема 1.5.6. 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 1.5.7. 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

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

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

□

Следствие 1.5.7.1. *Подмножество счетного множества является конечным или счетным множеством.*

Теорема 1.5.8. *Если A – бесконечное множество, а B – конечное или счетное множество, то $\overline{A \cup B} = \overline{A}$.*

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 $\overline{C \cup B} = \overline{C}$. Пусть f – биекция \mathbb{N} на C . Если B – конечное множество, состоящее из элементов b_1, \dots, b_n , то функция h , определенная равенствами $h(t) = b_t$ при $1 \leq t \leq n$, $h(n+k) = f(k)$, задает биекцию \mathbb{N} на $C \cup B$, значит, $\overline{C \cup B} = \overline{\mathbb{N}} = \overline{C}$.

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, $\overline{C \cup B} = \overline{\mathbb{N}} = \overline{C}$. Поэтому для завершения доказательства достаточно воспользоваться равенствами

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

□

Следствие 1.5.8.1. *Объединение конечного числа счетных множеств само является счетным множеством.*

Теорема 1.5.9. *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 $A \setminus \{a\}$. □

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

Теорема 1.5.10. *Если существует сюръективное отображение множества натуральных чисел на множество A , то A – конечное или счетное множество.*

Д о к а з а т е л ь с т в о. 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

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

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 $\varphi(a) \doteq n_a$. Нетрудно проверить, что φ – инъективное отображение множества A во множество \mathbb{N} . И остается воспользоваться одной из предыдущих теорем. \square

Теорема 1.5.11. *Объединение счетного множества счетных множеств само является счетным множеством.*

Д о к а з а т е л ь с т в о. 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 $f(n, k) \doteq f_n(k)$. 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 fc_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 1.5.12. *Множество всех конечных последовательностей, составленных из элементов счетного множества, само является счетным множеством.*

Д о к а з а т е л ь с т в о. Достаточно доказать счетность множества

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

А это сразу следует из теорем 1.5.5 и 1.5.11. \square

Следствие 1.5.12.1. *Множество всех конечных подмножеств счетного множества само является счетным множеством.*

Закончим параграф доказательством одной интересной теоремы из теории чисел.

Определение 1.5.4. *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 \mathcal{A} алгебраических чисел по своим алгебраическим свойствам не отличается от множества \mathbb{C} комплексных чисел: \mathcal{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. Линдеманом в 1882 г. трансцендентности числа π , откуда следовала невозможность построения с помощью циркуля и линейки квадрата, равного по площади данному кругу (задача о квадратуре круга).

Теорема 1.5.13. *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 $-\mathbb{N} = \{-n | n \in \mathbb{N}\}$. 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 1.5.14. *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 1.5.7 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 α , 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 1.5.15. 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 1.5.13, 1.5.8 и 1.5.14, поэтому нужное равенство следует из теорем 1.5.13 и 1.5.8. \square

1.6. Множества мощности континуум

Определение 1.6.1. Множество A , равномощное множеству \mathbb{R} всех действительных чисел, называется **континуальным** множеством. Его мощность обозначается через \mathfrak{c} и называется **мощностью континуума**.

Теорема 1.6.1. $\overline{(0, 1)} = \mathfrak{c}$. Для любых действительных чисел a и b , если $a < b$, то $\overline{(a, b)} = \mathfrak{c}$ и $\overline{[a, b]} = \mathfrak{c}$.

Доказательство. Функция $f(x) = tg(\pi x - \pi/2)$ 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 1.5.8. \square

Теорема 1.6.2. 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 квадрата $(0, 1)^2$ в интервал $(0, 1)$. 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 φ 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 1.6.2.1. 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 1.6.3. Множество $P(\mathbb{N})$ всех подмножеств множества натуральных чисел \mathbb{N} имеет мощность \mathfrak{c} , т. е. выполняется равенство $\mathfrak{c} = 2^{\aleph_0}$.

Доказательство. Пусть χ_A – характеристическая функция подмножества A множества \mathbb{N} натуральных чисел, т. е.

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

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

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

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 α из интервала $(0, 1)$ представимо в виде бесконечной двоичной дроби

$$(0, a_1 a_2 \dots a_n \dots)_2, \text{ где } a_n \in \{0, 1\},$$

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

$$\{1 \cdot a_1, 2 \cdot a_2, 3 \cdot a_3, \dots, n \cdot a_n, \dots\}.$$

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 о мощности множества всех подмножеств данного множества сразу получаем

Следствие 1.6.3.1. $\aleph_0 < \mathfrak{c}$.

Теорема 1.6.4. *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} .

Д о к а з а т е л ь с т в о. 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

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

где χ_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,

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

Для завершения доказательства первой части теоремы остается воспользоваться теоремой 1.6.3. Для доказательства второй части теоремы достаточно воспользоваться теоремами 1.6.2 и 1.6.6. \square

Теорема 1.6.5. *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, ..., 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

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

А так как обратное неравенство очевидно, то получаем равенство

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

Для завершения доказательства остается воспользоваться теоремой 1.6.4. □

Теорема 1.6.6. *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 φ_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

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

Это вместе с неравенством

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

дает нужное равенство

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

□

Теорема 1.6.7. *Объединение континуального 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 $\alpha \in (0, 1)$ множество A_α имеет мощность \mathfrak{c} . Обозначим через φ_α некоторое биективное отображение интервала $(0, 1)$ на множество A_α , имеющее по условию мощность \mathfrak{c} . Полагаем $\varphi(\alpha, t) \equiv \varphi_\alpha(t)$. Тогда φ — 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 1.6.8. *Множество всех бесконечных последовательностей действительных чисел имеет мощность \mathfrak{c} .*

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

Д о к а з а т е л ь с т в о. Покажем, что множество $\mathbb{R}^{\mathbb{N}}$ всех бесконечных последовательностей действительных чисел имеет мощность \mathfrak{c} . Используя теоремы 1.6.4 и 1.5.5, получаем равенства

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

□

Рассматривая бесконечные подмножества множества действительных чисел, мы познакомились со счетными множествами, т. е. множествами, равномощными множеству натуральных чисел, и множествами мощности континуум, т. е. множествами, равномощными множеству всех действительных чисел. Попытки построить множество мощности промежуточной между счетной и континуальной привели в конце XIX века Г. Кантора к формулировке предположения, получившего название

Континуум-гипотеза Г. Кантора:

”Если множество A таково, что $\mathbb{N} \subseteq A \subseteq \mathbb{R}$, то либо $\overline{A} = \overline{\mathbb{N}}$, либо $\overline{A} = \overline{\mathbb{R}}$.”

Континуум-гипотеза Г. Кантора включена Д. Гильбертом под номером 1 в его знаменитый список из 23 проблем, представленный им II Международному математическому конгрессу, проходившему в августе 1900 года в Париже. Попытки доказательства **Континуум-гипотезы Г. Кантора** в XX веке привели к постановке и исследованию достаточно тонких вопросов теории множеств и математики в целом, однако у нас нет возможности уделить этому достаточное внимание.

1.7. Операции над кардинальными числами

Как уже было сказано выше, мы считаем, что каждому множеству A сопоставлено **кардинальное число** 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 1.7.1. *Суммой кардинальных чисел n_1 и n_2 называется кардинальное число $n = \overline{A_1 \cup A_2}$, где A_1 и A_2 – такие непересекающиеся множества, что $n_i = \overline{A_i}$ ($i = 1, 2$).*

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 1.7.2. *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 1.7.3. *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 \mathfrak{n}_1 и \mathfrak{n}_2 обозначается через $\mathfrak{n}_1 \cdot \mathfrak{n}_2$.

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

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

Произведение семейства кардинальных чисел $(\mathfrak{n}_i)_{i \in I}$ обозначается через

$$\prod_{i \in I} \mathfrak{n}_i.$$

Введем обозначения $0 \rightleftharpoons \emptyset$, $1 \rightleftharpoons \{\emptyset\}$.

Хотя для кардинальных чисел выполняются равенства

$$1.1) \mathfrak{n}_1 + \mathfrak{n}_2 = \mathfrak{n}_2 + \mathfrak{n}_1,$$

$$1.2) (\mathfrak{n}_1 + \mathfrak{n}_2) + \mathfrak{n}_3 = \mathfrak{n}_1 + (\mathfrak{n}_2 + \mathfrak{n}_3),$$

$$1.3) \mathfrak{n}_1 + 0 = \mathfrak{n}_1,$$

$$2.1) \mathfrak{n}_1 \cdot \mathfrak{n}_2 = \mathfrak{n}_2 \cdot \mathfrak{n}_1,$$

$$2.2) (\mathfrak{n}_1 \cdot \mathfrak{n}_2) \cdot \mathfrak{n}_3 = \mathfrak{n}_1 \cdot (\mathfrak{n}_2 \cdot \mathfrak{n}_3),$$

$$2.3) \mathfrak{n}_1 \cdot 1 = \mathfrak{n}_1,$$

$$3.1) (\mathfrak{n}_1 + \mathfrak{n}_2) \cdot \mathfrak{n}_3 = \mathfrak{n}_1 \cdot \mathfrak{n}_3 + \mathfrak{n}_2 \cdot \mathfrak{n}_3,$$

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

Из теоремы 1.5.8 следует, что для любого бесконечного кардинального числа \mathfrak{n} выполняется равенство $\aleph_0 + \mathfrak{n} = \mathfrak{n}$, в частности, $\aleph_0 + \aleph_0 = \aleph_0$ и $\aleph_0 + \mathfrak{c} = \mathfrak{c}$.

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

Из теоремы 1.5.5 следует, что выполняется равенство $\aleph_0 \cdot \aleph_0 = \aleph_0$, а из теоремы 1.6.6 – равенство $\aleph_0 \cdot \mathfrak{c} = \mathfrak{c}$.

По теореме 1.6.7 $\mathfrak{c} \cdot \mathfrak{c} = \mathfrak{c}$.

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

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

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:

$$\begin{aligned} m^n \cdot m^k &= m^{n+k}, \\ (m \cdot n)^k &= m^k \cdot n^k, \\ (m^n)^k &= m^{n \cdot k}, \\ m^1 &= m, \\ 1^n &= 1. \end{aligned}$$

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 1.8.1. *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 1.8.2. *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 $x, y \in A$:*

если $x \leq_A y$, 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 1.8.3. *Начальным отрезком, отсекаемым элементом a множества A , называется множество*

$$A_a \doteq \{x \mid x \in A \& x < a\}.$$

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

Теорема 1.8.1. *Для любого линейно упорядоченного множества A множество $W(A)$, упорядоченное отношением включения \subseteq , подобно самому множеству A .*

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

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

Ясно, что φ – биекция множества A на множество $W(A)$.

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

Определение 1.8.5. 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 1.8.2. 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 $B = A_a$.

Д о к а з а т е л ь с т в о. 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. $a < b \iff a \leq b \text{ и } a \neq b$. В частности, $a \not< a$.

Определение 1.8.6. 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 1.8.3. Пусть $f : A \rightarrow A$ – монотонное отображение вполне упорядоченного множества A в себя. Не существует элемента $a \in A$ такого, что $f(a) < a$.

Д о к а з а т е л ь с т в о. 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

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

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

Д о к а з а т е л ь с т в о. 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 1.8.3.2. *Два различных отрезка вполне упорядоченного множества не могут быть подобны.*

Д о к а з а т е л ь с т в о. 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 1.8.3.3. *Существует не более одного изоморфизма двух вполне упорядоченных множеств.*

Д о к а з а т е л ь с т в о. 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 1.8.7. *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 ω – 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 1.8.8. *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 1.8.4. *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.

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_b , g – изоморфизм B на C_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

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

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 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 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_i, b_i} – изоморфизм отрезка A_{a_i} на отрезок B_{b_i} . 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 $b \equiv f_{a_2, b_2}(a_1)$. 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 1.8.3, $b_1 = b = f_{a_2, b_2}(a_1)$. 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 $f_{a_2, b_2} |_{A_{a_1}}$ на A_{a_1} изоморфизма f_{a_2, b_2} совпадает с f_{a_1, b_1} .

Из выше сказанного 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 $f_{a, b} |_{A_c}$ – изоморфизм отрезка A_c на отрезок B_d .

Заметим, что $f_{a, b} |_{A_c}$ – монотонное отображение отрезка A_c в отрезок B_b . При этом если $m \in A_c$, то $m < c$, значит,

$$f_{a, b} |_{A_c}(m) = f_{a, b}(m) < f_{a, b}(c) = d.$$

Следовательно, $f_{a, b} |_{A_c}(A_c) \subseteq B_d$. 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, $f_{a, b} |_{A_c}(A_c) = B_d$, 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 из B . Пусть f – изоморфизм отрезка A_y на отрезок B_b . Покажем, что ограничение $f |_{A_x}$ 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 $\varphi \equiv f |_{A_x}$. Если $z \in A_x$, то $z < x$, значит, $\varphi(z) = f(z) < f(x)$. Поэтому φ – монотонное отображение отрезка A_x в отрезок $B_{f(x)}$. Остается убедиться в сюръективности отображения φ . 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 φ – 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 1.8.2 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 $\overline{A} \leq \overline{B}$, то $\overline{\overline{A}} \leq \overline{\overline{B}}$.

Поэтому получаем следующее важное следствие.

Следствие 1.8.4.1. *Если A и B – вполне упорядоченные множества, то либо $\overline{\overline{A}} \leq \overline{\overline{B}}$, либо $\overline{\overline{B}} \leq \overline{\overline{A}}$, 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 1.8.9. *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 $f \circ g = id_B$.

Заметим, что функция g будет инъекцией.

8. Аксиома мультипликативности. Декартово произведение непустого семейства непустых множеств непусто.

Теорема 1.8.5. Сформулированные выше восемь утверждений эквивалентны.

Доказательство. Доказательство проведем по следующей схеме

$$\begin{array}{ccccc}
 (3) & \implies & (2) & \iff & (6) \\
 \uparrow & & \downarrow & & \\
 (5) & \implies & (1) & \iff & (8) \\
 & & \updownarrow & & \\
 & & (4) & & \\
 & & \updownarrow & & \\
 & & (7) & &
 \end{array}$$

$$(2) \implies (1).$$

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

$$\left\{ \varphi \mid \varphi \subseteq X \times \bigcup_{x \in X} f(x) \text{ \& } \varphi \text{ — функционально \& } \right. \\
 \left. \text{для любого } x \text{ из } \delta(\varphi) \quad \varphi(x) \in f(x) \right\},$$

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 φ .

Покажем, что φ можно взять в качестве функции выбора (заметим, что функция φ определена, конечно, неоднозначно, так как T может содержать более одного максимального элемента).

Так как $\varphi \in T$, то φ – 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 φ следует, что $y = z$.

В случае (2) получаем $y = b = z$.

Если $x \in \delta(\varphi)$, то найдется элемент $y = \varphi(x)$ такой, что

$$\langle x, y \rangle \in \varphi \cup \{\langle a, b \rangle\}.$$

Если $\langle x, y \rangle \in \varphi$, то $g(x) = y = \varphi(x) \in f(x)$. Если же $\langle x, y \rangle \in \{\langle a, b \rangle\}$, то $x = a$ и $y = b$. Поэтому $g(x) = y = b \in f(a) = f(x)$. Значит, $g \in T$. Однако это вместе с условиями $\varphi \subset g$ и $\varphi \neq g$ противоречит максимальнойности φ . 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

$$\langle x, y \rangle \in B \cap (\{x\} \times f(x)) \text{ и } \langle x, z \rangle \in B \cap (\{x\} \times f(x)).$$

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 1.8.2 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. $C = A_a$, $C = B_b$, 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, $a \in C$, 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 \prec : если $x, y \in L$, то $x \prec y \iff x < y$ 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 \prec 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 \mathcal{X} множества E , имеющее конечный характер, обладает максимальным элементом.

Пусть семейство подмножеств \mathcal{X} множества E имеет конечный характер. Множество \mathcal{X} частично упорядочено отношением \subseteq . Покажем, что для него выполнено условие **Леммы Цорна**. Пусть L – любая цепь в \mathcal{X} . Покажем, что множество $A = \bigcup_{y \in L} y$ является верхней гранью для L в \mathcal{X} .

Во-первых, если $y \in L$, то $y \subseteq A$.

Во-вторых, покажем, что $A \in \mathcal{X}$. 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 $y_n \in \mathcal{X}$, а C – конечное подмножество y_n , то $C \in \mathcal{X}$. Значит, каждое конечное подмножество множества A принадлежит \mathcal{X} , поэтому и $A \in \mathcal{X}$.

Итак, A – верхняя грань цепи L в \mathcal{X} . По **Лемме Цорна** в \mathcal{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 $\{y\} \times \{x \mid x \in A \text{ и } f(x) = y\}$. 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

$$g = D = \left(\bigcup_{y \in B} W_y \right) \cap D.$$

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

$$\overline{\overline{f(A)}} \leq \overline{A}.$$

$$(7) \implies (4).$$

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 1.8.6. Для произвольных мощностей α и β выполняется одно и только одно из условий

$$(1) \alpha = \beta, \quad (2) \alpha < \beta, \quad (3) \beta < \alpha.$$

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 $\alpha = \overline{\overline{X}}$, $\beta = \overline{\overline{Y}}$. 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 1.8.4 имеет место один из следующих двух случаев:

$$(1) \overline{X} \leq \overline{Y}, \quad (2) \overline{Y} \leq \overline{X}.$$

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

$$(1) \alpha = \beta, \quad (2) \alpha < \beta, \quad (3) \beta < \alpha.$$

□

Следствие 1.8.6.1. Кардинальные числа линейно упорядочены отношением $<$ (и отношением \leq).

Для произвольного порядкового числа α через $W(\alpha)$ обозначим множество всех порядковых чисел, меньших α .

Теорема 1.8.7. Для любого порядкового числа α множество $W(\alpha)$ – вполне упорядоченное множество порядкового типа α .

Д о к а з а т е л ь с т в о. Пусть A – вполне упорядоченное множество порядкового типа α . Тогда A изоморфно множеству $W(A) = \{A_a \mid a \in A\}$, упорядоченному отношением включения \subseteq . В свою очередь множество $\{A_a \mid a \in A\}$, 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 β . Тогда найдется отрезок A_a подобный B , значит, $\beta = \overline{B} = \overline{A_a}$. $\beta \in \{\overline{A_a} \mid a \in A\}$. Поэтому $\overline{W(\alpha)} = \alpha$. □

Следствие 1.8.7.1. Всякое множество ординальных чисел вполне упорядоченно.

Д о к а з а т е л ь с т в о. Пусть A – произвольное множество ординальных чисел, B – его непустое подмножество. Пусть $\alpha \in B$. Если $W(\alpha) \cap B = \emptyset$, то α – наименьший элемент в B . Если же $W(\alpha) \cap B \neq \emptyset$, то пусть β – наименьший элемент подмножества $W(\alpha) \cap B$ множества $W(\alpha)$. Тогда β будет и наименьшим элементом подмножества B множества A . □

Следствие 1.8.7.2. Для любого множества A порядковых чисел существует порядковое число, большее всех чисел из A .

Д о к а з а т е л ь с т в о. 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_α , то $\beta = \overline{B} > \overline{B_\alpha} = \overline{W(\alpha)} = \alpha$. □

Следствие 1.8.7.3. *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 1.8.7.4. *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 α – порядковое число больше всех чисел из A , а β – наименьшее в $W(\alpha) \cup \{\alpha\}$ число из $(W(\alpha) \cup \{\alpha\}) \setminus A$, тогда β – искомое число. \square

Определение 1.8.10. *Для порядкового числа α наименьшее порядковое число β , не принадлежащее $W(\alpha) \cup \{\alpha\}$, называется **непосредственно следующим** за α и обозначается через α' .*

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 1.8.7.5. *Всякое множество кардинальных чисел вполне упорядоченно.*

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 α_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 1.8.6 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 упорядоченно, то и множество V ординальных чисел вполне упорядоченно, значит, вполне упорядоченно и X . \square

Следствие 1.8.7.6. *Для любого кардинального числа n существует непосредственно следующее за ним кардинальное число n^+ , т. е. такое кардинальное число n^+ , что (1) $n < n^+$, (2) если m – кардинальное число и $n < m$, 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 α 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 α из того, что все ординальные числа $\beta < \alpha$ обладают свойством Q , следует что и α обладает свойством Q . Тогда все ординальные числа обладают свойством Q .

Д о к а з а т е л ь с т в о. Предположим противное, и пусть β – одно из ординальных, не обладающих свойством Q . Пусть α – 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 α . Что противоречит выбору α . \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 1.8.8. Для произвольного бесконечного кардинального числа n выполняются равенства

- 1) $n + n = n$,
- 2) $n \cdot k = n$, где k – конечное ненулевое кардинальное число,
- 3) $n \cdot \aleph_0 = n$.

Д о к а з а т е л ь с т в о. 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 1.8.3 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

$$\overline{\overline{A}} = \overline{\overline{\mathbb{N} \times A}}.$$

Значит, $\mathfrak{n} \cdot \aleph_0 = \mathfrak{n}$. Во втором случае

$$\overline{\overline{A}} = \overline{(\mathbb{N} \times A)_{\langle n_0, a_0 \rangle}}.$$

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 $\mathfrak{n} = \aleph_0 \cdot \mathfrak{n}_0$, где $\mathfrak{n} = \overline{\overline{A_{a_0}}}$.

Равенство 1) следует из следующих равенств

$$\mathfrak{n} + \mathfrak{n} = \aleph_0 \cdot \mathfrak{n}_0 + \aleph_0 \cdot \mathfrak{n}_0 = (\aleph_0 + \aleph_0) \cdot \mathfrak{n}_0 = \aleph_0 \cdot \mathfrak{n}_0 = \mathfrak{n}.$$

Равенство 2) следует из следующих равенств

$$\mathfrak{n} \cdot k = (\aleph_0 \cdot \mathfrak{n}_0) \cdot k = (\aleph_0 \cdot k) \cdot \mathfrak{n}_0 = \aleph_0 \cdot \mathfrak{n}_0 = \mathfrak{n}.$$

Равенство 3) $\mathfrak{n} \cdot \aleph_0 = \mathfrak{n}$ получаем из следующих равенств

$$\aleph_0 \cdot \mathfrak{n} = \aleph_0 \cdot \aleph_0 \cdot \mathfrak{n}_0 = \aleph_0 \cdot \mathfrak{n}_0 = \mathfrak{n}.$$

□

Следующая теорема следует из **Леммы Цорна** и даже на самом деле ей эквивалентна.

Теорема 1.8.9. Для произвольного бесконечного кардинального числа \mathfrak{n} выполняется равенство $\mathfrak{n} \cdot \mathfrak{n} = \mathfrak{n}$.

Д о к а з а т е л ь с т в о. Для произвольного множества A такого, что $\overline{\overline{A}} = \mathfrak{n}$, 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 $\overline{\overline{B \times B}} = \overline{\overline{B}}$, то множество $M(A)$ непусто. Множество $M(A)$ частично упорядочено отношением включения \subseteq и нетрудно проверить выполнимость условия **Леммы Цорна**. Значит, по **Лемме Цорна**, во множестве $M(A)$ есть максимальный элемент $g : C \times C \rightarrow C$.

Пусть $\mathfrak{m} = \overline{\overline{C}}$. Заметим, что $\overline{\overline{C \times C}} = \overline{\overline{C}}$, поэтому $\mathfrak{m} \cdot \mathfrak{m} = \mathfrak{m}$, т. е. $\mathfrak{m}^2 = \mathfrak{m}$.

Ясно, что $m \leq n$. Если $m = n$, то теорема доказана.

Предположим $m < n$.

Покажем, что выполнено неравенство $\overline{\overline{A \setminus C}} > m$.

Предположим противное $\overline{\overline{A \setminus C}} \leq m$.

Тогда в силу предыдущей теоремы

$$n = \overline{\overline{A}} = \overline{\overline{C \cup (A \setminus C)}} = \overline{\overline{C}} + \overline{\overline{A \setminus C}} \leq m + m = m,$$

что противоречит сделанному выше предположению $m < n$.

Пусть C_1 – подмножество мощности m множества $A \setminus C$.

Для получения противоречия рассмотрим множество $D \Leftarrow C \cup C_1$. Тогда

$$D \times D = (C \times C) \cup (C \times C_1) \cup (C_1 \times C) \cup (C_1 \times C_1).$$

Пусть

$$E \Leftarrow (C \times C_1) \cup (C_1 \times C) \cup (C_1 \times C_1).$$

Тогда $\overline{\overline{E}} = m^2 + m^2 + m^2 = m + m + m = m$. Поэтому существует биективное отображение h множества E на множество C_1 .

Полагаем $f \Leftarrow g \cup h$. 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 1.8.9.1. 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 1.8.6 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 Цермело** и **Теоремы Цермело**, а значит, и эквивалентных им утверждений, рассмотрим вопрос о существовании базисов в векторных пространствах.

Определение 1.8.11. 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 1.8.10. *В любом векторном пространстве V над произвольным полем K существует базис.*

Доказательство. 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 равносильны*.

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 выше сказанного 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 α и β 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 α 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 α и любого вектора v из L выполняется равенство $p(\alpha v) = \alpha p(v)$.

Теорема 1.8.11. 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, а v — произвольный вектор из U . 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 выполнено по условию. 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 U выполняется неравенство

$$f(v') - p(v' - w) \leq p(v'' + w) - f(v'').$$

Последнее неравенство доказывается следующим образом: при любых v' и v'' из U

$$\begin{aligned} f(v') + f(v'') &= f(v' + v'') \leq p(v' + v'') = \\ &= p(v' - w + v'' + w) \leq p(v' - w) + p(v'' + w). \end{aligned}$$

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 Φ , 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 Σ множества Φ 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 Φ и является верхней гранью для Σ . По лемме Цорна в Φ 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 Φ и $\langle \bar{W}, F_{\bar{W}} \rangle < \langle \bar{W}(w), F_{\bar{W}(w)} \rangle$, что противоречит максимальной $\langle \bar{W}, F_{\bar{W}} \rangle$. \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 μ , определенной на множестве $P(\mathcal{X})$ всех его подмножеств и принимающей лишь два значения 0 и 1, такой, что значение функции μ 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 μ на каждом одноэлементном подмножестве, то пример такой функции легко привести: для произвольного множества \mathcal{X} и фиксированного в нем элемента a полагаем

$$\text{если } A \subseteq X, \text{ то } \mu(A) = 1 \iff a \in A.$$

Такие функции называются δ -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.

1.9. 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 с соответствием 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.

1.9.1. Системы Пеано

Определение 1.9.1. *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 1.9.2. 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 1.9.1. 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.

$$B = \{a \mid a \in P \ \& \ (\exists b)(b \in P' \ \& \ \langle a, b \rangle \in f)\}$$

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 $U \Rightarrow f \setminus \{\langle c, e \rangle\}$.

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 $U \Rightarrow f \setminus \{\langle s(a), e \rangle\}$.

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) $f_i(s(a)) = s'(f_i(a))$ $i = 1, 2$.

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 1.9.3. Для произвольного множества U полагаем

$$U' \triangleq U \cup \{U\}.$$

Множество U' называется **последователем** множества U .

Определение 1.9.4. Множество S назовем индуктивным, если его элементом является пустое множество \emptyset и вместе с каждым элементом a a' тоже является элементом этого множества.

Следующее утверждение принимаем в качестве еще одной из аксиом теории множеств.

Аксиома бесконечности. Существует индуктивное множество S .

Определение 1.9.5. 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. 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. Рассмотренный способ определения понятия натурального числа через понятие множества принадлежит Джону фон Нейману:

$$0 \doteq \emptyset, \quad n' \doteq n \cup \{n\}.$$

Готтлоб Фреге в 1884 году 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.

1.9.2. Рекурсивные определения в системах Пеано

Теорема 1.9.2. 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 $\delta(f) = \mathbb{N}^{n+1}$, $\rho(h) \subseteq \mathbb{N}$ 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) если $\langle \langle a_1, \dots, a_n, b \rangle, c \rangle \in U$, 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

$$f \rightleftharpoons \cap_{U \in W} U.$$

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 $1 \in P_{\bar{a}}$. Условия 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 $e \neq g(a_1, \dots, a_n)$.

Рассмотрим множество $U \rightleftharpoons f \setminus \{\langle \langle a_1, \dots, a_n, 1 \rangle, e \rangle\}$.

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

$$\langle \langle a_1, \dots, a_n, b \rangle, c \rangle \in f \text{ и } e = h(a_1, \dots, a_n, b, c).$$

Рассмотрим множество $U \Rightarrow f \setminus \{\langle \langle a_1, \dots, a_n, s(b) \rangle, e \rangle\}$.

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

$$\langle \langle a_1, \dots, a_n, s(b) \rangle, e_1 \rangle \in f \text{ \& } \langle \langle a_1, \dots, a_n, s(b) \rangle, e_2 \rangle \in f.$$

Тогда найдутся такие элементы c_i ($i = 1, 2$), что

$$\langle \langle a_1, \dots, a_n, b \rangle, c_i \rangle \in f \text{ и } e_i = h(a_1, \dots, a_n, b, c_i).$$

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 $Q_{\bar{a}} = \mathbb{N}$.

Следовательно, f – функция.

Тем самым доказано существование функции f такой, что

$$\delta(f) = \mathbb{N}^{n+1}, \quad \rho(f) \subseteq \mathbb{N}$$

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) $f_i(a_1, \dots, a_n, s(b)) = h(a_1, \dots, a_n, b, f_i(a_1, \dots, a_n, b))$ $i = 1, 2$.

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,

$$\begin{aligned} f_1(a_1, \dots, a_n, s(b)) &= h(a_1, \dots, a_n, b, f_1(a_1, \dots, a_n, b)) = \\ &= h(a_1, \dots, a_n, b, f_2(a_1, \dots, a_n, b)) = \\ &= f_2(a_1, \dots, a_n, s(b)). \end{aligned}$$

Следовательно, $s(b) \in R_{\bar{a}}$.

Значит, $R_{\bar{a}}$ – индуктивное множество, поэтому по третьей аксиоме Пеано $R_{\bar{a}} = \mathbb{N}$. Поэтому $f_1 = f_2$. □

1.9.3. Определения сложения и умножения натуральных чисел

Из доказанной теоремы 1.9.2 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" [36], устанавливается, что для введенной операции сложения натуральных чисел выполняются хорошо известные из школьного курса математики свойства.

Сложение натуральных чисел удовлетворяет ассоциативному закону.

Теорема 1.9.3. *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 1.9.4. *Для любых натуральных чисел a и b выполняется равенство $a + b = b + a$.*

Для операции сложения натуральных чисел выполняется закон сокращения.

Теорема 1.9.5. *Для любых натуральных чисел a, b и c из равенства $a + c = b + c$ следует равенство $a = b$.*

Теорема 1.9.6. *Для любых натуральных чисел a и b выполняется неравенство $b \neq a + b$.*

Следующая теорема устанавливает закон трихотомии для операции сложения натуральных чисел.

Теорема 1.9.7. *Для любых натуральных чисел a и b выполняется одно из трех условий*

- I) $a = b$;*
- 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 1.9.2 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 1.9.8. *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 1.9.9. 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 1.9.10. Для любых натуральных чисел a и b выполняется равенство $a \cdot b = b \cdot a$.

Ассоциативность операции умножения натуральных чисел.

Теорема 1.9.11. 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 1.9.12. Для любых натуральных чисел a, b и c из равенства $a \cdot c = b \cdot c$ следует равенство $a = b$.

Из теоремы 1.9.2 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 1.9.13. 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) $(a \cdot b)^c = a^c \cdot b^c$.

1.10. Некоторые приложения аксиомы выбора

Чтобы продемонстрировать применения аксиомы выбора, рассмотрим некоторые задачи из теории измерения площадей и объемов.

Определение 1.10.1. 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) $f_a(x) \rightleftharpoons x + a$, где a – фиксированное действительное число; такие движения f_a называются **сдвигами**;
- 2) $f(x) \rightleftharpoons -x$ – симметрия относительно начала координат;
- 3) $f_a^{(-)}(x) \rightleftharpoons -x + a$, где a – фиксированное действительное число.

Оказывается, что других движений числовой прямой нет.

Теорема 1.10.1. 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 $a \equiv g(0)$. 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 α и β – два различных действительных числа, причем α 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 ρ 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 α , а при $\rho = 0$ получаем, что $\alpha = \beta$, а это противоречит выбору α и β .

Следовательно, $\alpha - (-1)^\rho\beta = \alpha - \beta$, а значит, $\rho = 0$.

Тем самым доказано, что для любых двух различных действительных чисел α и β , 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 1.10.2. 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} .

Следуя И. П. Натансону [29] 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:

$$1) \mu([0, 1]^n) = 1,$$

$$2) \text{ Если множества } A \text{ и } B \text{ конгруэнтны, то } \mu(A) = \mu(B);$$

3) Если $(A_i)_{i \in I}$ – конечное или счетное семейство ограниченных попарно не пересекающихся множеств и их объединение $\cup_{i \in I} A_i$ ограничено, то

$$\mu(\cup_{i \in I} A_i) = \sum_{i \in I} \mu(A_i).$$

Теорема 1.10.2. Трудная задача теории измерения неразрешима даже для числовой прямой \mathbb{R} .

Доказательство. Предположим противное и пусть μ – 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 α и β 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 $A_n \Leftarrow f_{r_n}(A)$, 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. \square

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 $(A_i)_{i \in N_m}$ – конечное семейство ограниченных попарно не пересекающихся множеств, то

$$\mu(\cup_{i \in N_m} A_i) = \sum_{i \in N_m} \mu(A_i).$$

Теорема 1.10.3 (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. 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 непересекающиеся 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, \dots, A_m конгруэнтно B_m .

Запись $A \approx B$ будет обозначать, что множества A и B 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, необходимо и достаточно, чтобы они были конгруэнтны при некоторых 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 [41] 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_φ и a_ψ , расположенные в плоскости XOY , причем a_ψ — это ось OX , а ось a_φ составляет с ней угол θ . Через ψ обозначим поворот на угол 120° относительно оси a_ψ , а через φ — поворот на угол 180° относительно оси a_φ . 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 ψ и φ . 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 θ , для которого никакое нетривиальное приведенное слово не дает тождественное преобразование*. Пусть θ — один из таких углов, тогда любым двум различным приведенным словам соответствуют различные преобразования. Обозначим через \mathbb{G} группу, порожденную преобразованиями ψ и φ . 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

$$\langle\langle \psi \mid \psi^3 = 1 \rangle\rangle \quad \text{и} \quad \langle\langle \varphi \mid \varphi^2 = 1 \rangle\rangle$$

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 φ предшествует ψ , 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 φu , 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 φ , 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:

$$1) (gh) \cdot v = g \cdot (h \cdot v), \quad 2) 1 \cdot v = v.$$

На сфере \mathbb{S} пространства \mathbb{R}^3 введем отношение эквивалентности

$$v \equiv_S u \iff (\exists g \in \mathbb{G})(u = g \cdot v).$$

Нетрудно проверить, что введенное отношение \equiv_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

$$A = \mathcal{A} \cdot M, B = \mathcal{B} \cdot M, C = \mathcal{C} \cdot M.$$

Тогда $\mathbb{S} = A \cup B \cup C \cup Q$ и $\psi^2(A) = C$, $\psi^2(B) = A$, $\psi^2(C) = B$ и $\varphi(A) = B \cup C$.

Обозначим через \mathbb{D} *шар* пространства \mathbb{R}^3 с центром в начале координат. Для произвольного подмножества E сферы \mathbb{S} , ограничивающей шар \mathbb{D} , через \mathbb{E} обозначим подмножество этого шара, состоящее из всех отличных от начала координат точек всех отрезков, соединяющих начало координат O с точками множества E .

Тогда

$$\mathbb{D} = \mathbb{A} \cup \mathbb{B} \cup \mathbb{C} \cup \mathbb{Q}_1 \cup \{O\}$$

и $\psi^2(\mathbb{A}) = \mathbb{C}$, $\psi^2(\mathbb{B}) = \mathbb{A}$, $\psi^2(\mathbb{C}) = \mathbb{B}$ и $\varphi(\mathbb{A}) = \mathbb{B} \cup \mathbb{C}$. Пусть \mathbb{Q} — это $\mathbb{Q}_1 \cup \{O\}$.

Допустим, что легкая задача теории измерения разрешима для пространства \mathbb{R}^3 и пусть μ — соответствующая мера. Тогда

$$\mu(\mathbb{D}) = \mu(\mathbb{A}) + \mu(\mathbb{B}) + \mu(\mathbb{C}) + \mu(\mathbb{Q}),$$

$$\mu(\mathbb{A}) = \mu(\mathbb{C}), \mu(\mathbb{B}) = \mu(\mathbb{A}), \mu(\mathbb{C}) = \mu(\mathbb{B}) \text{ и } \mu(\mathbb{A}) = \mu(\mathbb{B}) + \mu(\mathbb{C}).$$

Значит,

$$\mu(\mathbb{A}) = \mu(\mathbb{B}) = \mu(\mathbb{C}) = 0.$$

Поэтому $\mu(\mathbb{D}) = \mu(\mathbb{Q})$.

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 $f(\mathbb{Q}) \cap \mathbb{Q} = \emptyset$. Тогда $\mathbb{D} = \mathbb{Q} \cup f(\mathbb{Q}) \cup U$ и эти три множества попарно не пересекаются, поэтому $\mu(\mathbb{D}) \geq 2\mu(\mathbb{Q})$, что вместе с равенством $\mu(\mathbb{D}) = \mu(\mathbb{Q})$ дает равенство $\mu(\mathbb{D}) = 0$. Значит, мера любого подмножества шара \mathbb{D} равна 0, поэтому мера любого ограниченного множества равна 0, т. е. μ — 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 в начале напомним основные, необходимые для дальнейшего, определения из топологии.

Определение 1.10.3. Топологическое пространство — это пара $\langle U, \tau \rangle$, где U — множество, а τ — 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 τ

$$\bigcup_{i \in I} A_i \in \tau.$$

Множества из τ называются открытыми множествами, а сама система τ — 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 τ_1 слабее топологии τ_2 , если $\tau_1 \subseteq \tau_2$, при этом топология τ_2 сильнее топологии τ_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 τ_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* τ , в которой непрерывны все функции проектирования pr_t . Множество $\prod_{i \in I} U_i$ вместе с этой топологией τ называется *произведением* семейства $(\langle U_i, \tau_i \rangle)_{i \in I}$ топологических пространств и обозначается через $\prod_{i \in I} \langle U_i, \tau_i \rangle$. Ради некоторой краткости будем обозначать его через U , если это не приведет к недоразумениям.

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 Γ 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 Γ 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 Γ 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 Γ указанного вида образуют *базу* топологии на U . Эта база носит название база А. Н. Тихонова.

Определение 1.10.4. *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 1.10.4 (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 1.10.1. *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 Φ 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

$$\Phi(\mathcal{R}_0) \equiv \{Y \mid (\exists X_1, \dots, X_n \in \mathcal{R}_0) (\cap_{i=1}^n X_i \subseteq Y)\}.$$

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 Φ – *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 Φ содержит \mathcal{R} , то так как Φ – 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 Φ имеет место эквивалентность

$$(A \in \Phi \wedge B \in \Phi) \longleftrightarrow A \cap B \in \Phi.$$

Покажем, что для любого максимального фильтра Φ 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

$$A \cup B \in \Phi, \text{ но } A \notin \Phi \text{ и } B \notin \Phi.$$

Тогда в силу максимальной центрированного семейства Φ семейства $\Phi \cup \{A\}$ и $\Phi \cup \{B\}$ не являются центрированными, поэтому в Φ 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 Φ 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 максимальной фильтра Φ 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 Φ – максимальный фильтр.*

Пусть фильтр Φ' содержит фильтр Φ . 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 Φ – максимальный фильтр, а A – такое подмножество множества U , что для любого X из Φ $A \cap X \neq \emptyset$, то $A \in \Phi$.

Рассмотрим семейство $\Phi' = \Phi \cup \{A\}$. Нетрудно показать, что семейство Φ' является центрированным, поэтому из максимальной Φ следует равенство $\Phi' = \Phi$. Поэтому $A \in \Phi' = \Phi$.

Доказательство 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

$$\emptyset \neq \bigcap_{1 \leq j \leq n} Y_j \subseteq \bigcap_{1 \leq j \leq n} \prod_{t \in I} Y_j^t = \prod_{t \in I} \left(\bigcap_{1 \leq j \leq n} Y_j^t \right),$$

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

$$f \in \prod_{t \in I} \left(\bigcap_{X \in \mathcal{R}^t} X \right) = \prod_{t \in I} \left(\bigcap_{Y \in \mathcal{R}} \overline{Y^t} \right).$$

Тогда при любом $t \in I$

$$f(t) \in \bigcap_{Y \in \mathcal{R}} \overline{Y^t}.$$

Пусть $Y \in \mathcal{R}$. Покажем, что $f \in \overline{Y}$. 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 Γ 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 Γ указанного вида образуют *базу* топологии на U). Поэтому найдется такое открытое множество Γ 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 $t \in I$: $f(t) \in \overline{Z^t}$, в частности, при $s \in S$: $f(s) \in \overline{Z^s}$. 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, $f \in \overline{Y}$, поэтому

$$\prod_{t \in I} \left(\bigcap_{X \in \mathcal{R}^t} X \right) = \prod_{t \in I} \left(\bigcap_{Y \in \mathcal{R}} \overline{Y^t} \right) \subseteq \bigcap_{Y \in \mathcal{R}} \overline{Y}.$$

Значит, $\bigcap_{Y \in \mathcal{R}} \overline{Y} \neq \emptyset$. Выше уже отмечалось, что из последнего следует

$$\bigcap_{X \in \mathcal{R}_0} X \neq \emptyset.$$

Теорема А. Н. Тихонова доказана. □

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) $\notin \mathcal{R}$.

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 максимальнойности семейства \mathcal{R} получаем равенство $\mathcal{R} \cup \{B\} = \mathcal{R}' = \mathcal{R}$, значит, $B \in \mathcal{R}$.

3) Докажем, что имеет место эквивалентность

$$(A \in \mathcal{R} \wedge B \in \mathcal{R}) \longleftrightarrow (A \cap B) \in \mathcal{R}.$$

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 максимальнойности семейства \mathcal{R} получаем равенство $\mathcal{R} \cup \{(A \cap B)\} = \mathcal{R}' = \mathcal{R}$, значит, $(A \cap B) \in \mathcal{R}$.

4) Докажем, 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 максимальнойности 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 $A \cap \bigcap_{1 \leq i \leq n} X_i = \emptyset$ и $B \cap \bigcap_{1 \leq j \leq m} Y_j = \emptyset$. Но тогда

$$\begin{aligned} (A \cup B) \cap \bigcap_{1 \leq i \leq n} X_i \cap \bigcap_{1 \leq j \leq m} Y_j = \\ (A \cap \bigcap_{1 \leq i \leq n} X_i \cap \bigcap_{1 \leq j \leq m} Y_j) \cup (B \cap \bigcap_{1 \leq i \leq n} X_i \cap \bigcap_{1 \leq j \leq m} Y_j) = \emptyset, \end{aligned}$$

что противоречит предположению $(A \cup B) \in \mathcal{R}$ и центрированности \mathcal{R} .

5) Докажем, 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 $V_s = t \in I \setminus \{s\} \prod U_t \times G_s$, 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

$$\mathcal{R}^t = \{ (CV)^t \mid CV \in \mathcal{R} \wedge V - \text{из базы топологии Тихонова} \}.$$

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 U_t . В силу компактности U_t получаем

$$\bigcap_{\{CV \in \mathcal{R} \wedge V - \text{из базы топологии Тихонова}\}} (CV)^t \neq \emptyset.$$

Пусть

$$f \in \prod_{t \in I} \left(\bigcap_{\{CV \in \mathcal{R} \wedge V - \text{из базы топологии Тихонова}\}} (CV)^t \right).$$

Тогда при любом t из I :

$$f(t) \in \left(\bigcap_{\{CV \in \mathcal{R} \wedge V - \text{из базы топологии Тихонова}\}} (CV)^t \right).$$

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

$$f(s) \in \bigcap_{\{CV \in \mathcal{R} \wedge V - \text{из базы топологии Тихонова}\}} (CV)^t \subseteq (CV_s)^t = CG_s.$$

Значит,

$$\emptyset \neq \prod_{t \in I} \left(\bigcap_{\{CV \in \mathcal{R} \wedge V - \text{из базы топологии Тихонова}\}} (CV)^t \right) \subseteq \bigcap_{\{CV \in \mathcal{R} \wedge V - \text{из базы топологии Тихонова}\}} CV = \bigcap_{Y \in \mathcal{R}} Y \subseteq \bigcap_{X \in \mathcal{R}_0} X.$$

ГЛАВА 2.

ЛОГИКА И ИСЧИСЛЕНИЕ ВЫСКАЗЫВАНИЙ

*”...математическая логика является
не собранием разрозненных результатов,
а действенным методом изучения
некоторых наиболее интересных проблем,
стоящих перед математиками.”*

(Дж. Шенфильд. ”Математическая логика.” М.: Наука, 1975.)

*” Глубокие и опустошительные результаты
Геделя, Тарского, Черча, Россера, Клини и многих других
были богатой наградой за вложенный труд
и завоевали для математической логики
положение независимой ветви математики.”*

(Э. Мендельсон. ”Введение в математическую логику.”
М.: Наука, 1971.)

2.1. Алфавиты. Слова

Определение 2.1.1. *Алфавитом* называется любое непустое множество Σ символов. Элементы множества Σ называются **символами** или **буквами** данного алфавита.

Никаких ограничений на природу элементов множества Σ (символов алфавита) мы не накладываем, единственное предположение относительно Σ состоит в том, что мы должны *уметь распознавать каждый символ из Σ как тот же самый при каждом из его вхождений и отличать его от всех других символов из Σ* , т. е. предполагается, что *различия неодинаковых символов значительно превосходят мелкие различия одинаковых символов*. Символы из Σ рассматриваются как простые знаки, а не как символы, которые что-либо означают. Символы алфавита Σ

считаются *элементарными знаками*, далее неделимыми. Например, если W и V входят в Σ , то мы считаем, что W – это элементарный объект, далее неделимый, в частности, не считаем, что W – это два раза повторенное V .

Определение 2.1.2. *Словом или выражением в алфавите Σ называется произвольная конечная (возможно пустая) последовательность $w_1w_2\dots w_n$ символов из Σ , т. е. $n \geq 0$ и при любом i ($1 \leq i \leq n$) $w_i \in \Sigma$. Число n называется **длиной** слова $w_1w_2\dots w_n$.*

Длину произвольного слова X будем обозначать через $|X|$. Пустое слово – это слово длины 0, будем его обозначать через Λ или через 1, если это не приведет к путанице.

Пусть X – это слово $w_1w_2\dots w_n$ ($w_i \in \Sigma$, $i = 1, \dots, n$), а Y – это слово $v_1v_2\dots v_m$ ($v_i \in \Sigma$, $i = 1, \dots, m$).

Определение 2.1.3. *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 Σ .*

Утверждение “слова X и Y равны графически” будем записывать в виде

$$X = Y.$$

Определение 2.1.4. *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

$$XZ = YZ \text{ и } ZX = ZY,$$

и обратно, если

$$XZ = YZ \text{ или } ZX = ZY,$$

то $X = Y$.

Определение 2.1.5. *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 2.1.1. *Если X, Y, Z, V – слова в алфавите Σ и $XY = ZV$, то для некоторого слова P либо $X = ZP$ и $V = PY$, либо $Z = XP$ и $Y = PV$.*

Д о к а з а т е л ь с т в о. 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

$$Z = XP \text{ и } Y = PV.$$

□

Определение 2.1.6. 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 2.1.7. **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 α ($\alpha \in \Sigma$), то вхождение V слова Y в слово X называется **вхождением символа (буквы) α в слово X** .

Если α – символ алфавита Σ , а X и Z – слова в алфавите Σ , то **результат одновременной замены каждого вхождения символа α в слово X на слово Z** обозначается через

$$X_\alpha [Z].$$

Аналогично, если $\alpha_1, \dots, \alpha_n$ – попарно различные символы из Σ , а X, Z_1, \dots, Z_n – слова в алфавите Σ , 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 $X_{\alpha_1, \dots, \alpha_n} [Z_1, \dots, Z_n]$.

2.2. Логика Высказываний

В этом параграфе будет рассмотрен один из простейших языков математической логики – **язык Логики Высказываний**.

Произвольный **логический язык L считается заданным**, если выполнены следующие условия:

(1) задан **алфавит Σ языка**, т. е. некоторое множество символов – символов языка L . Слова в алфавите Σ , т. е. конечные последовательности символов из Σ , 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 $\Sigma_{ЛВ}$ языка $L_{ЛВ}$ Логики 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 Σ_1 называется **пропозициональной переменной** или переменным высказыванием. Смысл этого названия будет ясен из дальнейшего употребления элементов множества Σ_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 Σ_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 \mathcal{A} и \mathcal{B} обладают свойством \mathcal{D} , то и формулы

$$(\neg \mathcal{A}), (\mathcal{A} \vee \mathcal{B}), (\mathcal{A} \& \mathcal{B}), (\mathcal{A} \rightarrow \mathcal{B})$$

обладают свойством \mathcal{D} .

Определим теперь одно из основных понятий математической логики – понятие **интерпретации**.

Определение 2.2.1. *Интерпретацией языка $L_{ЛВ}$ называется любое отображение φ множества пропозициональных переменных*

$$\Sigma_1 = \{A_1, A_2, \dots\}$$

этого языка $L_{ЛВ}$ во множество истинностных значений $\{И, Л\}$.

Будем говорить, что интерпретация φ **задает истинностные значения для пропозициональных переменных** языка $L_{ЛВ}$.

Пусть φ – произвольная интерпретация языка $L_{ЛВ}$. Распространим φ 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 α ($n = 1, 2$) сопоставим некоторую n -местную функцию H_α , определенную на множестве истинностных значений $\{И, Л\}$ и принимающую значения в том же множестве.

Традиционно функции H_α задаются с помощью таблиц, которые называются **истинностными таблицами**.

		A_1		$H_{\neg}(A_1)$	
		\mathcal{I}		\mathcal{L}	
		\mathcal{L}		\mathcal{I}	

	A_1		A_2		$H_{\vee}(A_1, A_2)$	
	\mathcal{I}		\mathcal{I}		\mathcal{I}	
	\mathcal{I}		\mathcal{L}		\mathcal{I}	
	\mathcal{L}		\mathcal{I}		\mathcal{I}	
	\mathcal{L}		\mathcal{L}		\mathcal{L}	

	A_1		A_2		$H_{\&}(A_1, A_2)$	
	\mathcal{I}		\mathcal{I}		\mathcal{I}	
	\mathcal{I}		\mathcal{L}		\mathcal{L}	
	\mathcal{L}		\mathcal{I}		\mathcal{L}	
	\mathcal{L}		\mathcal{L}		\mathcal{L}	

\parallel	A_1	$ $	A_2	\parallel	$H_{\rightarrow}(A_1, A_2)$	\parallel
\parallel	I	$ $	I	\parallel	I	\parallel
\parallel	I	$ $	L	\parallel	L	\parallel
\parallel	L	$ $	I	\parallel	I	\parallel
\parallel	L	$ $	L	\parallel	I	\parallel

Определим значение φ для произвольной формулы из множества F_{LV} языка L_{LV} индукцией по построению формул.

Заметим, что $\Sigma_1 \subset F_{LV}$.

(i) **Атомная** или **элементарная формула** Φ языка L_{LV} – это просто любая пропозициональная переменная A_i , поэтому для любой элементарной формулы Φ истинностное значение $\varphi(\Phi)$ уже определено.

(ii) Если формула Φ языка L_{LV} 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_{LV} , то истинностное значение $\varphi(\Phi)$ определяем следующими равенствами

$$\begin{aligned}\varphi(\neg \mathcal{A}) &\equiv H_{\neg}(\varphi(\mathcal{A})), \\ \varphi(\mathcal{A} \vee \mathcal{B}) &\equiv H_{\vee}(\varphi(\mathcal{A}), \varphi(\mathcal{B})), \\ \varphi(\mathcal{A} \& \mathcal{B}) &\equiv H_{\&}(\varphi(\mathcal{A}), \varphi(\mathcal{B})), \\ \varphi(\mathcal{A} \rightarrow \mathcal{B}) &\equiv H_{\rightarrow}(\varphi(\mathcal{A}), \varphi(\mathcal{B})).\end{aligned}$$

Итак, любую интерпретацию φ языка L_{LV} , т. е. любое отображение

$$\varphi : \Sigma_1 \rightarrow \{I, L\},$$

множества пропозициональных переменных языка L_{LV} во множество истинностных значений, можно естественным образом продолжить до отображения

$$\varphi : F_{LV} \rightarrow \{I, L\}$$

множества F_{LV} всех формул языка L_{LV} во множество $\{I, L\}$ истинностных значений.

Определение 2.2.2. Для произвольной интерпретации φ и любой формулы \mathcal{A} языка L_{LV} истинностное значение $\varphi(\mathcal{A})$ будем называть **истинностным значением** формулы \mathcal{A} в интерпретации φ . Если при этом $\varphi(\mathcal{A}) = I$, то будем говорить, что формула \mathcal{A} **истинна в интерпретации** φ , а если $\varphi(\mathcal{A}) = L$, то будем говорить, что формула \mathcal{A} **ложна в интерпретации** φ .

Определение 2.2.3. Формула \mathcal{A} языка L_{LV} называется **выполнимой**, если существует интерпретация, в которой эта формула истинна.

Определение 2.2.4. Множество формул Γ языка $L_{ЛВ}$ называется **совместным**, если существует интерпретация, в которой все формулы из этого множества истинны.

Замечание. Для произвольного множества формул Γ языка $L_{ЛВ}$ и для любой интерпретации φ запись

$$\varphi(\Gamma) = И$$

будет служить сокращением для утверждения "все формулы множества Γ истинны в интерпретации φ ."

Определение 2.2.5. 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.**"

Для произвольных формул A, B и C **Логике Высказываний** любая формула указанного ниже вида является тождественно истинной

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. $((\neg(\neg A)) \rightarrow A).$

IV.3. $(A \vee (\neg A)).$

Определение 2.2.6. Формулы A и B языка $L_{ЛВ}$ называются **равносильными** или **эквивалентными**, если для любой интерпретации φ этого языка выполняется равенство

$$\varphi(A) = \varphi(B).$$

Замечание. Запись $A \equiv B$ будет служить сокращением для утверждения "**формула A и B эквивалентны.**"

Следующие эквивалентности играют важную роль в **Логике Высказываний**.

$$1a) \quad \mathcal{A} \& (\mathcal{B} \& \mathcal{C}) \equiv (\mathcal{A} \& \mathcal{B}) \& \mathcal{C}, \quad 1b) \quad (\mathcal{A} \& \mathcal{B}) \equiv (\mathcal{B} \& \mathcal{A});$$

$$2a) \quad \mathcal{A} \vee (\mathcal{B} \vee \mathcal{C}) \equiv (\mathcal{A} \vee \mathcal{B}) \vee \mathcal{C}, \quad 2b) \quad (\mathcal{A} \vee \mathcal{B}) \equiv (\mathcal{B} \vee \mathcal{A}).$$

$$3a) \quad \mathcal{A} \vee (\mathcal{B} \& \mathcal{C}) \equiv (\mathcal{A} \vee \mathcal{B}) \& (\mathcal{A} \vee \mathcal{C}), \quad 3b) \quad (\mathcal{A} \vee \mathcal{A}) \equiv \mathcal{A};$$

$$4a) \quad \mathcal{A} \& (\mathcal{B} \vee \mathcal{C}) \equiv (\mathcal{A} \& \mathcal{B}) \vee (\mathcal{A} \& \mathcal{C}), \quad 4b) \quad (\mathcal{A} \& \mathcal{A}) \equiv \mathcal{A}.$$

$$5a) \quad (\neg(\mathcal{A} \vee \mathcal{B})) \equiv ((\neg \mathcal{A}) \& (\neg \mathcal{B})),$$

$$5b) \quad (\neg(\mathcal{A} \& \mathcal{B})) \equiv ((\neg \mathcal{A}) \vee (\neg \mathcal{B}));$$

$$6a) \quad (\mathcal{A} \vee \mathcal{B}) \equiv (\neg((\neg \mathcal{A}) \& (\neg \mathcal{B}))),$$

$$6b) \quad (\mathcal{A} \& \mathcal{B}) \equiv (\neg((\neg \mathcal{A}) \vee (\neg \mathcal{B})));$$

$$7a) \quad (\mathcal{A} \rightarrow \mathcal{B}) \equiv ((\neg \mathcal{A}) \vee \mathcal{B}),$$

$$7b) \quad (\mathcal{A} \rightarrow \mathcal{B}) \equiv (\neg(\mathcal{A} \& (\neg \mathcal{B}))).$$

Введем одно из основных понятий *Логике Высказываний* – понятие **логического следствия**.

Определение 2.2.7. Формула \mathcal{A} языка $L_{ЛВ}$ называется **логическим следствием** множества формул Γ этого языка $L_{ЛВ}$, если для любой интерпретации φ , в которой все формулы из этого множества Γ истинны, истинна и формула \mathcal{A} .

Замечание. Запись $\Gamma \models \mathcal{A}$ будет служить сокращением для утверждения “формула \mathcal{A} является логическим следствием множества формул Γ .”

Отметим одно полезное в дальнейшем свойство логического следствия:

если $\Gamma \models \mathcal{A}$ и $\Gamma \models (\mathcal{A} \rightarrow \mathcal{B})$, то $\Gamma \models \mathcal{B}$.

Кроме того, справедлива эквивалентность

$\models \mathcal{A}$ тогда и только тогда, когда $\emptyset \models \mathcal{A}$.

Следующее понятие играет особо важную роль в приложениях математической логики, например, к алгебре.

Определение 2.2.8. Множество формул Γ языка $L_{ЛВ}$ назовем **локально совместным**, если любое его конечное подмножество совместно.

Введем в определенной мере технические два понятия, необходимые нам прежде всего для доказательства теоремы компактности.

Определение 2.2.9. Формула \mathcal{A} языка $L_{ЛВ}$ называется **локальным логическим следствием** множества формул Γ этого языка $L_{ЛВ}$, если она является логическим следствием некоторого конечного подмножества Γ_0 множества Γ .

Замечание. Запись $\Gamma \models_{fin} \mathcal{A}$ будет служить сокращением для утверждения "формула \mathcal{A} является **локальным логическим следствием** множества формул Γ ."

Определение 2.2.10. Множество формул Γ языка $L_{ЛВ}$ назовем **локально полным**, если оно локально совместно и для любой формулы \mathcal{A} языка $L_{ЛВ}$ либо $\Gamma \models_{fin} \mathcal{A}$, либо $\Gamma \models_{fin} (\neg \mathcal{A})$.

Замечание. Если Γ – локально совместное множество формул, то не существует такой формулы \mathcal{A} , что $\Gamma \models_{fin} \mathcal{A}$ и $\Gamma \models_{fin} (\neg \mathcal{A})$. В самом деле, предположим, что существует такая формула \mathcal{A} , что $\Gamma \models_{fin} \mathcal{A}$ и $\Gamma \models_{fin} (\neg \mathcal{A})$. В соответствии с определением найдутся такие конечные подмножества Γ_1 и Γ_2 множества Γ , что $\Gamma_1 \models \mathcal{A}$ и $\Gamma_2 \models (\neg \mathcal{A})$. Тогда $\Gamma_1 \cup \Gamma_2 \models (\mathcal{A} \& (\neg \mathcal{A}))$. Значит, множество $\Gamma_1 \cup \Gamma_2$ не является совместным, что противоречит предположению о локальной совместности множества Γ .

Теорема о локальном пополнении. Для любого локально совместного множества формул Γ языка $L_{ЛВ}$ **Логики Высказываний** существует такое локально полное множество формул Γ^* 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

$$\Gamma_1 \Leftarrow \Gamma.$$

Если множество Γ_n уже определено, то полагаем

$$\Gamma_{n+1} \Leftarrow \begin{cases} \Gamma_n \cup \{\Phi_n\}, & \text{если } \Gamma_n \models_{fin} \Phi_n \\ \Gamma_n \cup \{(\neg \Phi_n)\}, & \text{если } \Gamma_n \not\models_{fin} \Phi_n. \end{cases}$$

Индукцией по n докажем, что каждое из множеств формул Γ_n является *локально совместным*.

Так как $\Gamma_1 \Leftarrow \Gamma$, то множество формул Γ_1 является локально совместным по условию теоремы.

Предположим, что уже доказана локальная совместность множества формул Γ_n . Докажем локальную совместность множества формул Γ_{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 Γ' – конечное подмножество множества Γ_n . Пусть Γ'' – такое конечное подмножество множества Γ_n , что $\Gamma'' \models \Phi_n$. Для конечного подмножества $\Gamma' \cup \Gamma''$ локально совместного множества формул Γ_n существует интерпретация φ такая, что $\varphi(\Gamma' \cup \Gamma'') = И$. Тогда $\varphi(\Phi_n) = И$ и $\varphi(\Gamma' \cup \{\Phi_n\}) = И$.

Значит, множество $\Gamma' \cup \{\Phi_n\}$ *совместно*, поэтому в рассматриваемом случае множество Γ_{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 Γ_{n+1} не является локально совместным, то найдется такое конечное подмножество Γ' множества Γ_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 Γ_{n+1} является *локально совместным*.

Тем самым доказано, что *при любом n множество формул Γ_n является локально совместным*.

Полагаем

$$\Gamma^* = \bigcup_{n=1}^{\infty} \Gamma_n.$$

Покажем, что Γ^* – *локально полное множество формул* и

$$\Gamma \subseteq \Gamma^*.$$

Последнее очевидно, так как

$$\Gamma = \Gamma_1 \subseteq \Gamma^*.$$

Если бы множество формул Γ^* 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 Γ_n .

Значит, Γ^* – *локально совместное* множество формул.

Пусть \mathcal{A} – произвольная формула. Тогда найдется такое число n , что $\mathcal{A} = \Phi_n$.

Если $\Gamma_n \models_{fin} \Phi_n$, то $\Gamma^* \models_{fin} \Phi_n$, а значит, $\Gamma^* \models_{fin} \mathcal{A}$.

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. $\Gamma^* \models_{fin} \neg\mathcal{A}$.

Итак, доказано, что Γ^* – *локально полное* множество формул языка L_{IV} такое, что $\Gamma \subseteq \Gamma^*$. \square

Теорема Компактности. *Множество формул Γ языка $L_{ЛВ}$ является совместным тогда и только тогда, когда оно является локально совместным, т. е. совместно любое его конечное подмножество.*

Д о к а з а т е л ь с т в о. Если множество формул Γ языка $L_{ЛВ}$ является совместным, то, очевидно, является совместным и любое его подмножество. В частности, является совместным и любое конечное подмножество множества формул Γ . Значит, Γ *локально совместно*.

Обратно, предположим, что множество Γ *локально совместно*, т. е. любое его конечное подмножество является совместным. Докажем, что тогда *совместно и все множество* Γ . 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 Γ^* такое, что $\Gamma \subseteq \Gamma^*$.

Покажем, что множество формул Γ^* является *совместным*. Отсюда, конечно, сразу будет следовать совместность и множества формул Γ .

Построим интерпретацию φ 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 Γ^* – **локально полное множество** формул, поэтому для любой формулы \mathcal{A}

$$\Gamma^* \models_{fin} \mathcal{A} \quad \text{или} \quad \Gamma^* \models_{fin} (\neg \mathcal{A}),$$

но не то и другое одновременно, в частности, это верно и для произвольной пропозициональной переменной A_n . Поэтому интерпретация φ определена корректно.

Обычным образом продолжаем отображение φ , заданное на множестве Σ_1 пропозициональных переменных, до отображения, заданного на множестве $F_{ЛВ}$ всех формул языка $L_{ЛВ}$ Логики Высказываний.

Индукцией по построению формул докажем, что для произвольной формулы \mathcal{A} имеет место эквивалентность:

$$\Gamma^* \models_{fin} \mathcal{A} \iff \varphi(\mathcal{A}) = И.$$

(i) Для элементарных формул \mathcal{A} указанная эквивалентность имеет место по определению интерпретации φ .

(ii) Предположим, что указанная эквивалентность имеет место для формул \mathcal{A} и \mathcal{B} и докажем, что тогда она выполняется и для формул

$$(\neg \mathcal{A}), \quad (\mathcal{A} \& \mathcal{B}),$$

$$(\mathcal{A} \vee \mathcal{B}), \quad (\mathcal{A} \rightarrow \mathcal{B}).$$

Так как

$$\Gamma^* \models_{fin} (\neg \mathcal{A}) \iff \Gamma^* \not\models_{fin} \mathcal{A}$$

и

$$\varphi(\mathcal{A}) = Л \iff \varphi((\neg \mathcal{A})) = И,$$

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 φ

$$\varphi(\mathcal{A}) = \text{И} \text{ и } \varphi(\mathcal{B}) = \text{И} \iff \varphi(\mathcal{A} \& \mathcal{B}) = \text{И}.$$

Значит,

$$\Gamma^* \models_{fin} (\mathcal{A} \& \mathcal{B}) \iff \varphi(\mathcal{A} \& \mathcal{B}) = \text{И}.$$

Покажем, что для локально полного множества формул Γ^* 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 Γ^* – **локально полное** множество формул, то тогда

$$\Gamma^* \models_{fin} (\neg \mathcal{A}) \text{ и } \Gamma^* \models_{fin} (\neg \mathcal{B}),$$

а значит,

$$\Gamma^* \models_{fin} (\neg \mathcal{A}) \& (\neg \mathcal{B}),$$

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 Γ^* .

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 Γ^* .

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 Γ^* , то, очевидно, $\Gamma^* \models_{fin} \mathcal{A}$, поэтому $\varphi(\mathcal{A}) = \text{И}$.

Значит, $\varphi(\Gamma^*) = \text{И}$, поэтому множество формул Γ^* 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 $L_{ЛВ}$ является **счетным** множеством, то счетным является и множество $F_{ЛВ}$ всех формул языка $L_{ЛВ}$, поэтому счетно и любое множество формул Γ .

Счетным будет множество всех **конечных** подмножеств множества формул Γ .

Пусть $(\Gamma_i)_{i \in N}$ – семейство всех **конечных** подмножеств множества формул Γ .

Так как каждое множество формул Γ_i по предположению является совместным, то найдется такая интерпретация φ_i , что $\varphi_i(\Gamma_i) = \text{И}$.

Зададим следующим образом счетное семейство подмножеств множества N натуральных чисел

$$I_k \Leftarrow \{i \mid i \in N, \varphi_i(\Gamma_k) = \text{И}\}.$$

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 Γ_s является конечным, то найдется интерпретация φ_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 $(I_k)_{k \in N}$.

Определим интерпретацию φ , полагая для произвольной пропозициональной переменной A_j

$$\varphi(A_j) = \text{И} \iff \{i | \varphi_i(A_j) = \text{И}\} \in D.$$

Покажем, что для произвольной формулы \mathcal{A} имеет место эквивалентность

$$\varphi(\mathcal{A}) = \text{И} \iff \{i | \varphi_i(\mathcal{A}) = \text{И}\} \in D.$$

Доказательство проведем **индукцией по построению формул**.

(i) Для элементарных формул (пропозициональных переменных) указанная эквивалентность имеет место по определению интерпретации φ .

(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 – **ультрафильтр**, а значит, для любых подмножеств A и B множества натуральных чисел N выполняются эквивалентности

- 1) $A \in D \iff (N \setminus A) \notin D$,
- 2) $(A \cup B) \in D \iff A \in D \text{ или } B \in D$,
- 3) $(A \cap B) \in D \iff A \in D \text{ и } B \in D$.

Заметим, что последнее верно и для любого фильтра.

Отметим, что

$$\varphi((\neg \mathcal{A})) = \text{И} \iff \varphi(\mathcal{A}) = \text{Л}.$$

Предположим, что

$$\varphi(\mathcal{A}) = \text{И} \iff \{i | \varphi_i(\mathcal{A}) = \text{И}\} \in D.$$

Значит,

$$\varphi(\mathcal{A}) = \text{Л} \iff \{i | \varphi_i(\mathcal{A}) = \text{И}\} \notin D.$$

Так как D – **ультрафильтр**, то

$$\{i | \varphi_i(\mathcal{A}) = \text{И}\} \notin D \iff N \setminus \{i | \varphi_i(\mathcal{A}) = \text{И}\} \in D.$$

Но

$$N \setminus \{i|\varphi_i(\mathcal{A}) = \text{И}\} = \{i|\varphi_i(\mathcal{A}) = \text{Л}\} = \{i|\varphi_i(\neg\mathcal{A}) = \text{И}\}.$$

Окончательно получаем

$$\varphi((\neg\mathcal{A})) = \text{И} \iff \{i|\varphi_i((\neg\mathcal{A})) = \text{И}\} \in D.$$

Предположим, что

$$\varphi(\mathcal{A}) = \text{И} \iff \{i|\varphi_i(\mathcal{A}) = \text{И}\} \in D$$

и

$$\varphi(\mathcal{B}) = \text{И} \iff \{i|\varphi_i(\mathcal{B}) = \text{И}\} \in D.$$

Покажем, что тогда

$$\begin{aligned} \varphi(\mathcal{A} \vee \mathcal{B}) = \text{И} &\iff \{i|\varphi_i(\mathcal{A} \vee \mathcal{B}) = \text{И}\} \in D, \\ \varphi(\mathcal{A} \&\mathcal{B}) = \text{И} &\iff \{i|\varphi_i(\mathcal{A} \&\mathcal{B}) = \text{И}\} \in D, \\ \varphi(\mathcal{A} \rightarrow \mathcal{B}) = \text{И} &\iff \{i|\varphi_i(\mathcal{A} \rightarrow \mathcal{B}) = \text{И}\} \in D. \end{aligned}$$

Напомним, что

$$\varphi(\mathcal{A} \vee \mathcal{B}) = \text{И} \iff \varphi(\mathcal{A}) = \text{И} \quad \text{или} \quad \varphi(\mathcal{B}) = \text{И}.$$

По предположению

$$\varphi(\mathcal{A}) = \text{И} \iff \{i|\varphi_i(\mathcal{A}) = \text{И}\} \in D$$

и

$$\varphi(\mathcal{B}) = \text{И} \iff \{i|\varphi_i(\mathcal{B}) = \text{И}\} \in D.$$

Так как D – **ультрафильтр**, то

$$\begin{aligned} \{i|\varphi_i(\mathcal{A}) = \text{И}\} \in D \quad \text{или} \quad \{i|\varphi_i(\mathcal{B}) = \text{И}\} \in D &\iff \\ \{i|\varphi_i(\mathcal{A}) = \text{И}\} \cup \{i|\varphi_i(\mathcal{B}) = \text{И}\} &\in D. \end{aligned}$$

Окончательно получаем

$$\begin{aligned} \varphi(\mathcal{A} \vee \mathcal{B}) = \text{И} &\iff \varphi(\mathcal{A}) = \text{И} \quad \text{или} \quad \varphi(\mathcal{B}) = \text{И} \iff \\ \{i|\varphi_i(\mathcal{A}) = \text{И}\} \in D \quad \text{или} \quad \{i|\varphi_i(\mathcal{B}) = \text{И}\} \in D &\iff \\ \{i|\varphi_i(\mathcal{A}) = \text{И}\} \cup \{i|\varphi_i(\mathcal{B}) = \text{И}\} &\in D. \end{aligned}$$

Остается заметить, что

$$\{i|\varphi_i(\mathcal{A}) = \text{И}\} \cup \{i|\varphi_i(\mathcal{B}) = \text{И}\} = \{i|\varphi_i(\mathcal{A} \vee \mathcal{B}) = \text{И}\}.$$

Полученная цепочка эквивалентностей дает эквивалентность

$$\varphi(\mathcal{A} \vee \mathcal{B}) = \text{И} \iff \{i|\varphi_i(\mathcal{A} \vee \mathcal{B}) = \text{И}\} \in D.$$

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

$$\varphi(\mathcal{A} \& \mathcal{B}) = \text{И} \iff \varphi(\mathcal{A}) = \text{И} \quad \text{и} \quad \varphi(\mathcal{B}) = \text{И}.$$

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

$$\begin{aligned} \varphi(\mathcal{A} \& \mathcal{B}) = \text{И} &\iff \varphi(\mathcal{A}) = \text{И} \quad \text{и} \quad \varphi(\mathcal{B}) = \text{И} \iff \\ \{i \mid \varphi_i(\mathcal{A}) = \text{И}\} \in D \quad \text{и} \quad \{i \mid \varphi_i(\mathcal{B}) = \text{И}\} \in D &\iff \\ \{i \mid \varphi_i(\mathcal{A}) = \text{И}\} \cap \{i \mid \varphi_i(\mathcal{B}) = \text{И}\} \in D. \end{aligned}$$

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 φ истинна любая формула из множества формул Γ .

В самом деле, пусть \mathcal{A} — произвольная формула из множества формул Γ .

Рассмотрим конечное множество $\Gamma_k \Leftarrow \{\mathcal{A}\}$.

Напомним, что

$$I_k = \{i \mid i \in N, \varphi_i(\mathcal{A}) = \text{И}\}.$$

Так как $I_k \in D$, то $\{i \mid i \in N, \varphi_i(\mathcal{A}) = \text{И}\} \in D$.

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 Γ является **совместным**.

Это завершает второе доказательство **Теоремы компактности**. \square

Следствие 2.2.0.1. Для любой формулы \mathcal{A} языка $L_{\text{ЛВ}}$ и для любого множества формул Γ этого языка имеет место следующая эквивалентность:

формула \mathcal{A} является логическим следствием множества формул Γ тогда и только тогда, когда она является логическим следствием некоторого конечного подмножества Γ_0 множества формул Γ , 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 Γ_0 множества формул Γ , то, очевидно, формула \mathcal{A} является логическим следствием и множества формул Γ .

Предположим теперь, что формула \mathcal{A} является логическим следствием множества формул Γ .

Тогда множество формул $\Gamma \cup \{(\neg \mathcal{A})\}$ не является совместным, значит, по **Теореме компактности** найдется такое конечное подмножество Γ_0 множества формул Γ , что множество формул $\Gamma_0 \cup \{(\neg \mathcal{A})\}$ не является совместным. Значит, для любой интерпретации φ 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 Γ_0 множества формул Γ . \square

Сделаем некоторые пояснения по поводу использования термина "**компактность**."

Напомним некоторые топологические понятия и определения, частично уже рассматривавшиеся в первой главе.

Определение 2.2.11. 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 2.2.12. Семейство \mathcal{R} подмножеств множества X называется **центрированным**, если непусто пересечение любого конечного числа множеств из семейства \mathcal{R} .

Определение 2.2.13. 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 Γ формул этого языка запись $\varphi(\Gamma) = И$ означает, что для любой формулы Φ из множества Γ выполняется равенство $\varphi(\Phi) = И$.

Определение 2.2.14. Подмножество X множества U назовем **замкнутым**, если найдется такое подмножество Γ множества формул $F_{ЛВ}$ языка $L_{ЛВ}$, что

$$X = \{ \varphi \mid \varphi(\Gamma) = И \}.$$

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.

$$\emptyset = \{ \varphi \mid \varphi(\{(A_1 \& (\neg A_1))\}) = И \},$$

$$U = \{ \varphi \mid \varphi(\{(A_1 \vee (\neg A_1))\}) = И \}.$$

2. Если $(X_i)_{i \in I}$ – произвольное семейство замкнутых множеств и

$$X_i = \{ \varphi \mid \varphi(\Gamma_i) = И \},$$

то

$$\bigcap_{i \in I} X_i = \{ \varphi \mid \varphi(\bigcup_{i \in I} \Gamma_i) = И \}.$$

3. Пусть X_i ($i = 1, 2$) – два произвольных замкнутых множества и

$$X_i = \{ \varphi \mid \varphi(\Gamma_i) = И \}.$$

Обозначим через $\Gamma_1 \vee \Gamma_2$ следующее множество формул языка $L_{ЛВ}$

$$\{ (\Phi_1 \vee \Phi_2) \mid \Phi_1 \in \Gamma_1, \Phi_2 \in \Gamma_2 \}.$$

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 $L_{ЛВ}$ 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 Γ_i формул языка $L_{ЛВ}$ 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 Γ – 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

$$\bigcap_{i \in I_0} X_i = \{ \varphi \mid \varphi(\bigcup_{i \in I_0} \Gamma_i) = \text{И} \}.$$

Поэтому

$$\{ \varphi \mid \varphi(\bigcup_{i \in I_0} \Gamma_i) = \text{И} \} \neq \emptyset,$$

т. е. множество формул

$$\bigcup_{i \in I_0} \Gamma_i$$

совместно.

Поэтому совместно и множество формул Γ .

Так как мы установили совместность любого конечного подмножества Γ 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 φ_1, φ_2 – две различные интерпретации, тогда найдется число i такое, что

$$\varphi_1(A_i) \neq \varphi_2(A_i).$$

Предположим, что

$$\varphi_1(A_i) = \mathbb{I}, \quad \varphi_2(A_i) = \mathbb{L}.$$

Рассмотрим замкнутые множества

$$F_1 \Leftarrow \{\varphi \mid \varphi((\neg A_i)) = \mathbb{I}\}, \quad F_2 \Leftarrow \{\varphi \mid \varphi(A_i) = \mathbb{I}\}.$$

Полагаем

$$U_1 \Leftarrow U \setminus F_1, \quad U_2 \Leftarrow U \setminus F_2.$$

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_{LB} .

Заметим, что для любой формулы \mathcal{A} выполняется равенство

$$\{\varphi \mid \varphi(\mathcal{A}) = \mathbb{I}\} = U \setminus \{\varphi \mid \varphi((\neg \mathcal{A})) = \mathbb{I}\},$$

поэтому множество

$$\{\varphi | \varphi(\mathcal{A}) = \text{И}\}$$

является одновременно замкнутым и открытым.

Из последнего, очевидно, следует, что пространство интерпретаций U не является связным.

2.3. Исчисление Высказываний

Алфавит Исчисления Высказываний $\Sigma_{ИВ}$ совпадает с **Алфавитом Логики Высказываний** $\Sigma_{ЛВ}$.

Понятие **формулы Исчисления Высказываний** совпадает с понятием **формулы Логики Высказываний**, т. е. язык $L_{ИВ}$ **Исчисления Высказываний** совпадает с языком $L_{ЛВ}$ **Логики Высказываний**.

Теперь мы приступаем к определению двух важнейших понятий **Исчисления Высказываний** – понятия **ВЫВОДА** и понятия **ВЫВОДИМОЙ ФОРМУЛЫ**.

Аксиомы Исчисления Высказываний

Для произвольных формул $\mathcal{A}, \mathcal{B}, \mathcal{C}$ **Исчисления Высказываний** любая формула любого указанного ниже вида является **Логической Аксиомой Исчисления Высказываний**.

I $_{\rightarrow}$.

I.1. $(\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{A}))$.

I.2. $((\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})) \rightarrow ((\mathcal{A} \rightarrow \mathcal{B}) \rightarrow (\mathcal{A} \rightarrow \mathcal{C})))$.

II $_{\&}$.

II.1. $((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{A})$.

II.2. $((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{B})$.

II.3. $((\mathcal{C} \rightarrow \mathcal{A}) \rightarrow ((\mathcal{C} \rightarrow \mathcal{B}) \rightarrow (\mathcal{C} \rightarrow (\mathcal{A} \& \mathcal{B}))))$.

III $_{\vee}$.

III.1. $(\mathcal{A} \rightarrow (\mathcal{A} \vee \mathcal{B}))$.

III.2. $(\mathcal{B} \rightarrow (\mathcal{A} \vee \mathcal{B}))$.

III.3. $((\mathcal{A} \rightarrow \mathcal{C}) \rightarrow ((\mathcal{B} \rightarrow \mathcal{C}) \rightarrow ((\mathcal{A} \vee \mathcal{B}) \rightarrow \mathcal{C})))$.

IV $_{\neg}$.

IV.1. $((\mathcal{A} \rightarrow (\neg \mathcal{B})) \rightarrow (\mathcal{B} \rightarrow (\neg \mathcal{A})))$.

IV.2. $((\neg(\neg \mathcal{A})) \rightarrow \mathcal{A})$.

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 2.3.1. *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 2.3.2. Формула B называется *выводимой в Исчислении Высказываний*, если существует *Вывод в Исчислении Высказываний*

$$B_1, \dots, B_n,$$

оканчивающийся формулой B .

Выражение $\vdash_{ИВ} A$ служит сокращенной записью утверждения "*формула A выводима в Исчислении Высказываний*". В дальнейшем для сокращения индекс *ИВ* будем опускать, т. е. вместо $\vdash_{ИВ} A$ будем писать просто $\vdash A$.

Теорема 2.3.1. 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) $((\mathcal{A} \rightarrow ((\mathcal{A} \rightarrow \mathcal{A}) \rightarrow \mathcal{A})) \rightarrow ((\mathcal{A} \rightarrow (\mathcal{A} \rightarrow \mathcal{A})) \rightarrow (\mathcal{A} \rightarrow \mathcal{A})))$ – логическая аксиома I.2,
- 2) $(\mathcal{A} \rightarrow ((\mathcal{A} \rightarrow \mathcal{A}) \rightarrow \mathcal{A}))$ – логическая аксиома I.1,
- 3) $((\mathcal{A} \rightarrow (\mathcal{A} \rightarrow \mathcal{A})) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}))$ – получается из 2) и 1) по правилу **MP**,
- 4) $(\mathcal{A} \rightarrow (\mathcal{A} \rightarrow \mathcal{A}))$ — логическая аксиома I.1,
- 5) $(\mathcal{A} \rightarrow \mathcal{A})$ – получается из 4) и 3) по правилу **MP**. □

Приведенное доказательство показывает, что установление выводимости даже достаточно простых формул – процесс весьма трудоемкий. С целью облегчения изучения отношения $\vdash \mathcal{A}$ введем и изучим более общее понятие, чем понятие **Вывода в Исчислении Высказываний** – понятие **Вывода в Исчислении Высказываний из множества гипотез**.

Пусть Γ – произвольное множество формул. Формулы из множества Γ будем называть **гипотезами**. Смысл этого названия проявится позже.

Определение 2.3.3. *Выводом в Исчислении Высказываний из множества формул Γ называется любая конечная последовательность*

$$\mathcal{B}_1, \dots, \mathcal{B}_n$$

формул Исчисления Высказываний, удовлетворяющая следующему условию:

- для любого i ($i = 1, \dots, n$)*
- либо*
- 0) $\mathcal{B}_i \in \Gamma$,*
- либо*
- 1) формула \mathcal{B}_i является Логической Аксиомой Исчисления Высказываний,*
- либо*
- 2) найдутся числа j и k меньшие, чем i , такие, что формула \mathcal{B}_i получается из формул \mathcal{B}_j и \mathcal{B}_k по правилу **MP**.*

Определение 2.3.4. *Формула \mathcal{B} называется выводимой в Исчислении Высказываний из множества формул Γ , если существует Вывод в Исчислении Высказываний из множества формул Γ*

$$\mathcal{B}_1, \dots, \mathcal{B}_n,$$

оканчивающийся формулой \mathcal{B} .

Выражение $\Gamma \vdash_{\text{ИВ}} \mathcal{A}$ служит сокращенной записью утверждения ”**формула \mathcal{A} выводима в Исчислении Высказываний из множества формул Γ** ”. И вновь индекс **ИВ** не будем писать.

Если Γ и Δ – два произвольных множества формул, то запись $\Gamma \vdash \Delta$ означает, что *любая формула из множества Δ выводима в Исчислении Высказываний из множества формул Γ .*

Теорема 2.3.2. Если $\Gamma \vdash \mathcal{A}$ и $\Gamma \subset \Gamma_1$, то $\Gamma_1 \vdash \mathcal{A}$.

Если $\Gamma_1 \vdash \mathcal{A}$, то найдется **конечное** подмножество Γ множества Γ_1 такое, что $\Gamma \vdash \mathcal{A}$.

Доказательство. Если $\Gamma \subset \Gamma_1$, то любой вывод из множества формул Γ будет выводом и из множества формул Γ_1 .

Если $\Gamma_1 \vdash \mathcal{A}$ и $\mathcal{B}_1, \dots, \mathcal{B}_n$ – вывод формулы \mathcal{A} из множества формул Γ_1 , то в качестве Γ можно взять $\Gamma_1 \cap \{\mathcal{B}_1, \dots, \mathcal{B}_n\}$. \square

Лемма 2.3.1. Если $\Gamma_1 \vdash \mathcal{B}$ и $\Gamma_2 \cup \{\mathcal{B}\} \vdash \mathcal{A}$, то $\Gamma_1 \cup \Gamma_2 \vdash \mathcal{A}$.

Доказательство. Пусть $\mathcal{D}_0: \mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_n \vdash \mathcal{B}$ – вывод формулы \mathcal{B} из множества формул Γ_1 .

По произвольному выводу $\mathcal{D}: \mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_m \vdash \mathcal{A}$ формулы \mathcal{A} из множества формул $\Gamma_2 \cup \{\mathcal{B}\}$ построим вывод $\mathcal{D}^*: \mathcal{A}_1^*, \mathcal{A}_2^*, \dots, \mathcal{A}_p^* \vdash \mathcal{A}$ формулы \mathcal{A} из множества формул $\Gamma_1 \cup \Gamma_2$.

Для произвольного i ($i = 1, \dots, p$) заменим в выводе \mathcal{D} вхождение формулы \mathcal{A}_i некоторой последовательностью формул с соответствующими комментариями по следующему правилу

если

0) $\mathcal{A}_i \in \Gamma_2 \cup \{\mathcal{B}\}$, то в случае $\mathcal{A}_i \in \Gamma_2$ вхождение формулы \mathcal{A}_i не меняется, а в случае $\mathcal{A}_i \in \{\mathcal{B}\}$, т. е. $\mathcal{A}_i \equiv \mathcal{B}$, заменяем вхождение формулы \mathcal{A}_i на последовательность формул $\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_n \vdash \mathcal{B} \equiv \mathcal{A}_i$, являющуюся выводом формулы $\mathcal{B} \equiv \mathcal{A}_i$ из множества формул Γ_1 , с соответствующим комментарием,

если

1) формула \mathcal{A}_i является **Логической Аксиомой Исчисления Высказываний**, то вхождение формулы \mathcal{A}_i и соответствующий ей комментарий не меняются,

если

2) найдутся числа j и k меньшие, чем i , такие, что формула \mathcal{A}_i получается из формул \mathcal{A}_j и \mathcal{A}_k по правилу **МР**, то вхождение формулы \mathcal{A}_i не меняется, а в соответствующем ей комментарии меняются лишь номера формул, из которых получается формула \mathcal{A}_i . \square

Теорема 2.3.3. Если $\Gamma_1 \vdash \Delta$ и $\Gamma_2 \cup \Delta \vdash \mathcal{A}$, то $\Gamma_1 \cup \Gamma_2 \vdash \mathcal{A}$.

Доказательство. В силу предыдущей теоремы можно считать, что множество Δ конечное, поэтому доказательство легко получается из предыдущей леммы индукцией по числу формул в множестве Δ . \square

Замечание. В дальнейшем по сложившейся традиции вместо записи

$$\Gamma_1 \cup \Gamma_2 \vdash \mathcal{A}$$

будем использовать запись

$$\Gamma_1, \Gamma_2 \vdash \mathcal{A},$$

а вместо записи

$$\Gamma_1, \{\mathcal{B}\} \vdash \mathcal{A} -$$

запись

$$\Gamma_1, \mathcal{B} \vdash \mathcal{A}.$$

Теперь мы докажем теорему, которая значительно облегчает изучение отношения $\Gamma \vdash \mathcal{A}$. Эта теорема носит специальное название **Теорема Дедукции**.

Теорема Дедукции. Если $\Gamma, \mathcal{A} \vdash \mathcal{B}$, то $\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B})$.

Обратно, если $\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B})$, то $\Gamma, \mathcal{A} \vdash \mathcal{B}$.

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 теореме 2.3.3 получаем

$$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B}_i).$$

Если же $\mathcal{B}_i \in \{\mathcal{A}\}$, то $\mathcal{B}_i = \mathcal{A}$.

Тогда по теореме 2.3.1

$$\vdash (\mathcal{A} \rightarrow \mathcal{B}_i),$$

значит,

$$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B}_i).$$

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 теореме 2.3.3 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 **MP**.

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

$$\vdash ((\mathcal{A} \rightarrow (\mathcal{B}_j \rightarrow \mathcal{B}_i)) \rightarrow ((\mathcal{A} \rightarrow \mathcal{B}_j)) \rightarrow (\mathcal{A} \rightarrow \mathcal{B}_i))$$

и

$$(\mathcal{A} \rightarrow (\mathcal{B}_j \rightarrow \mathcal{B}_i)), (\mathcal{A} \rightarrow \mathcal{B}_j) \vdash (\mathcal{A} \rightarrow \mathcal{B}_i)),$$

то по теореме 2.3.3 получаем

$$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B}_i).$$

При $i = n$ получаем

$$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B}).$$

Для доказательства второй части теоремы предположим, что

$$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B}).$$

Так как

$$\mathcal{A} \vdash \mathcal{A}$$

и

$$\mathcal{A}, (\mathcal{A} \rightarrow \mathcal{B}) \vdash \mathcal{B},$$

то по теореме 2.3.3 получаем

$$\Gamma, \mathcal{A} \vdash \mathcal{B}.$$

Это завершает доказательство теоремы. □

Теорема 2.3.4. *Для любых формул \mathcal{A} и \mathcal{B}*

$$\mathcal{A}, \mathcal{B} \vdash (\mathcal{A} \& \mathcal{B}).$$

Д о к а з а т е л ь с т в о. Используя аксиому II.3.

$$((C \rightarrow A) \rightarrow ((C \rightarrow B) \rightarrow (C \rightarrow (A \& B))))$$

и вторую часть **Теоремы Дедукции**, получаем

$$C, (C \rightarrow A), (C \rightarrow B) \vdash (A \& B).$$

Так как

$$A \vdash (C \rightarrow A), \quad B \vdash (C \rightarrow B),$$

то, воспользовавшись теоремой 2.3.3, получим

$$C, A, B \vdash (A \& B).$$

Взяв в качестве формулы C любую выводимую в **Исчислении Высказываний** формулу и воспользовавшись теоремой 2.3.3, получим

$$A, B \vdash (A \& B).$$

□

Применив два раза **Теорему Дедукции**, получим

Следствие 2.3.4.1. Для любых формул A и B

$$\vdash (A \rightarrow (B \rightarrow (A \& B))).$$

Теорема 2.3.5. Для любых формул A и B и любого множества формул Γ 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. Если

$$\Gamma \vdash A \quad \text{и} \quad \Gamma \vdash B,$$

то, применив теоремы 2.3.3 и 2.3.4, 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

$$(A \& B) \vdash A \quad \text{и} \quad (A \& B) \vdash B,$$

поэтому применив теорему 2.3.3, получим

$$\Gamma \vdash A \quad \text{и} \quad \Gamma \vdash B.$$

□

Теорема 2.3.6. *Для любой формулы \mathcal{A}*

$$\vdash (\mathcal{A} \rightarrow (\neg(\neg\mathcal{A}))).$$

Д о к а з а т е л ь с т в о. Логическая аксиома IV.1 дает

$$\vdash (((\neg\mathcal{A}) \rightarrow (\neg\mathcal{A})) \rightarrow (\mathcal{A} \rightarrow (\neg(\neg\mathcal{A}))))).$$

Откуда по **Теореме Дедукции** получаем

$$((\neg\mathcal{A}) \rightarrow (\neg\mathcal{A})) \vdash (\mathcal{A} \rightarrow (\neg(\neg\mathcal{A}))).$$

По теореме 2.3.1

$$\vdash ((\neg\mathcal{A}) \rightarrow (\neg\mathcal{A})).$$

Применив Теорему 2.3.3, получим

$$\vdash (\mathcal{A} \rightarrow (\neg(\neg\mathcal{A}))).$$

□

Для любых двух формул \mathcal{A} и \mathcal{B} запись $\mathcal{A} \leftrightarrow \mathcal{B}$ будет служить сокращенным обозначением формулы

$$((\mathcal{A} \rightarrow \mathcal{B}) \& (\mathcal{B} \rightarrow \mathcal{A})).$$

Следствие 2.3.6.1. *Для любой формулы \mathcal{A} и любого множества формул Γ имеем*

- 1) $\mathcal{A} \vdash (\neg(\neg\mathcal{A})),$
- 2) $(\neg(\neg\mathcal{A})) \vdash \mathcal{A},$
- 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 2.3.6

$$\vdash (\mathcal{A} \rightarrow (\neg(\neg\mathcal{A}))),$$

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 2.3.3 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 2.3.2 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 2.3.7. 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 2.3.3, получаем

$$(\neg\mathcal{A}) \vdash (\mathcal{A} \rightarrow (\neg(\neg\mathcal{B}))).$$

По **Теореме Дедукции** получаем

$$\mathcal{A}, (\neg\mathcal{A}) \vdash (\neg(\neg\mathcal{B})).$$

В силу пункта 3) предыдущего следствия получаем

$$\mathcal{A}, (\neg\mathcal{A}) \vdash \mathcal{B}.$$

□

Определение 2.3.5. Множество формул Γ называется **противоречивым**, если найдется такая формула \mathcal{A} , что

$$\Gamma \vdash \mathcal{A} \quad \text{и} \quad \Gamma \vdash (\neg \mathcal{A}),$$

в противном случае множество формул Γ называется **непротиворечивым**.

Следствие 2.3.7.1. Если Γ – противоречивое множество формул, то для любой формулы \mathcal{B}

$$\Gamma \vdash \mathcal{B}.$$

Д о к а з а т е л ь с т в о. Если Γ – противоречивое множество формул, то найдется такая формула \mathcal{A} , что

$$\Gamma \vdash \mathcal{A} \quad \text{и} \quad \Gamma \vdash (\neg \mathcal{A}).$$

Пусть \mathcal{B} – произвольная формула. По предыдущей теореме 2.3.7

$$\mathcal{A}, (\neg \mathcal{A}) \vdash \mathcal{B}.$$

Поэтому по теореме 2.3.3

$$\Gamma \vdash \mathcal{B}.$$

□

Следствие 2.3.7.2. Для любых формул \mathcal{A} и \mathcal{B}

$$\begin{aligned} 1) \vdash (\mathcal{A} \rightarrow ((\neg \mathcal{A}) \rightarrow \mathcal{B})), \quad 2) \vdash ((\neg \mathcal{A}) \rightarrow (\mathcal{A} \rightarrow \mathcal{B})), \\ 3) (\mathcal{A} \& (\neg \mathcal{A})) \vdash \mathcal{B}, \quad 4) \vdash ((\mathcal{A} \& (\neg \mathcal{A})) \rightarrow \mathcal{B}). \end{aligned}$$

Д о к а з а т е л ь с т в о. 1) Так как

$$\mathcal{A}, (\neg \mathcal{A}) \vdash \mathcal{B},$$

то, применяя два раза **Теорему Дедукции**, получаем

$$\vdash (\mathcal{A} \rightarrow ((\neg \mathcal{A}) \rightarrow \mathcal{B})).$$

2) Аналогичным образом устанавливается, что

$$\vdash ((\neg \mathcal{A}) \rightarrow (\mathcal{A} \rightarrow \mathcal{B})).$$

3) Так как

$$(\mathcal{A} \& (\neg \mathcal{A})) \vdash \mathcal{A}, \quad (\mathcal{A} \& (\neg \mathcal{A})) \vdash (\neg \mathcal{A}),$$

то из предыдущей теоремы 2.3.7 и теоремы 2.3.3 получаем

$$(\mathcal{A} \& (\neg \mathcal{A})) \vdash \mathcal{B}.$$

4) Применяя **Теорему Дедукции**, из предыдущего утверждения получаем

$$\vdash ((\mathcal{A} \& (\neg \mathcal{A})) \rightarrow \mathcal{B}).$$

□

Следующая теорема аналогична **Теореме компактности** для **Исчисления Высказываний**.

Теорема 2.3.8. *Множество формул Γ 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 Γ_1 множества формул Γ языка $L_{ЛВ}$ является противоречивым, то возьмем такую формулу \mathcal{A} , что

$$\Gamma_1 \vdash \mathcal{A} \quad \text{и} \quad \Gamma_1 \vdash (\neg \mathcal{A}),$$

но тогда

$$\Gamma \vdash \mathcal{A} \quad \text{и} \quad \Gamma \vdash (\neg \mathcal{A}),$$

т. е. и само множество формул Γ является противоречивым.

Если противоречивым является само множество формул Γ языка $L_{ЛВ}$, то возьмем такую формулу \mathcal{A} , что

$$\Gamma \vdash \mathcal{A} \quad \text{и} \quad \Gamma \vdash (\neg \mathcal{A}).$$

Пусть \mathcal{D} – вывод из множества формул Γ формулы \mathcal{A} , а \mathcal{D}_1 – вывод из множества формул Γ формулы $(\neg \mathcal{A})$.

Если Γ_1 – это множество всех формул из множества Γ , входящих в \mathcal{D} или в \mathcal{D}_1 , то, очевидно,

$$\Gamma_1 \vdash \mathcal{A} \quad \text{и} \quad \Gamma_1 \vdash (\neg \mathcal{A}).$$

Остается заметить, что Γ_1 – конечное множество формул. □

Теорема 2.3.9. *Для любых формул \mathcal{A} , \mathcal{B} и \mathcal{C}*

$$(\mathcal{A} \rightarrow \mathcal{B}), (\mathcal{B} \rightarrow \mathcal{C}) \vdash (\mathcal{A} \rightarrow \mathcal{C}).$$

Д о к а з а т е л ь с т в о. Покажем, что

$$\mathcal{A}, (\mathcal{A} \rightarrow \mathcal{B}), (\mathcal{B} \rightarrow \mathcal{C}) \vdash \mathcal{C},$$

а затем применим **Теорему Дедукции**.

Обозначим через Γ множество формул

$$\{\mathcal{A}, (\mathcal{A} \rightarrow \mathcal{B}), (\mathcal{B} \rightarrow \mathcal{C})\}.$$

Так как

$$\Gamma \vdash \mathcal{A} \quad \text{и} \quad \Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B}),$$

то

$$\Gamma \vdash \mathcal{C}.$$

А так как, кроме того,

$$\Gamma \vdash (\mathcal{B} \rightarrow \mathcal{C}),$$

то

$$\Gamma \vdash \mathcal{C}.$$

Как уже отмечалось выше, для завершения доказательства остается воспользоваться **Теоремой Дедукции**. \square

Следствие 2.3.9.1. Для любых формул \mathcal{A} , \mathcal{B} , \mathcal{C} и любого множества формул Γ : если

$$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B}) \quad \text{и} \quad \Gamma \vdash (\mathcal{B} \rightarrow \mathcal{C}),$$

то

$$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{C}).$$

Доказательство. Для доказательства достаточно воспользоваться только что доказанной теоремой 2.3.9 и теоремой 2.3.3. \square

Следующая теорема позволяет переставлять посылки.

Теорема 2.3.10. Для любых формул \mathcal{A} , \mathcal{B} и \mathcal{C}

$$(\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})) \vdash (\mathcal{B} \rightarrow (\mathcal{A} \rightarrow \mathcal{C})).$$

Доказательство. Покажем, что

$$\mathcal{A}, \mathcal{B}, (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})) \vdash \mathcal{C},$$

а затем два раза применим **Теорему Дедукции**.

Обозначим через Δ множество формул

$$\{\mathcal{A}, \mathcal{B}, (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C}))\}.$$

Тогда

$$\Delta \vdash \mathcal{A} \quad \text{и} \quad \Delta \vdash (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})),$$

поэтому

$$\Delta \vdash (\mathcal{B} \rightarrow \mathcal{C}).$$

Так как, кроме того,

$$\Delta \vdash \mathcal{B},$$

то

$$\Delta \vdash \mathcal{C}.$$

Итак, доказано, что

$$\mathcal{A}, \mathcal{B}, (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})) \vdash \mathcal{C},$$

поэтому по **Теореме Дедукции**

$$\mathcal{B}, (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})) \vdash (\mathcal{A} \rightarrow \mathcal{C}).$$

Еще раз применяя **Теорему Дедукции**, получаем

$$(\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})) \vdash (\mathcal{B} \rightarrow (\mathcal{A} \rightarrow \mathcal{C})).$$

□

Следствие 2.3.10.1. Для любых формул \mathcal{A} , \mathcal{B} и \mathcal{C} и любого множества формул Γ : если

$$\Gamma \vdash (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})),$$

то

$$\Gamma \vdash (\mathcal{B} \rightarrow (\mathcal{A} \rightarrow \mathcal{C})).$$

Д о к а з а т е л ь с т в о. следует из предыдущей теоремы 2.3.10 и теоремы 2.3.3. □

Следующее следствие позволяет объединять посылки.

Следствие 2.3.10.2. Для любых формул \mathcal{A} , \mathcal{B} , \mathcal{C} и любого множества формул Γ : если

$$\Gamma \vdash (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})),$$

то

$$\Gamma \vdash ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{C}).$$

Д о к а з а т е л ь с т в о. Если

$$\Gamma \vdash (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})),$$

то по **Теореме Дедукции**

$$\Gamma, \mathcal{A}, \mathcal{B} \vdash \mathcal{C}.$$

Так как, кроме того,

$$\mathcal{A} \& \mathcal{B} \vdash \mathcal{A} \quad \text{и} \quad \mathcal{A} \& \mathcal{B} \vdash \mathcal{B},$$

то, применяя теорему 2.3.3, получаем

$$\Gamma, (\mathcal{A} \& \mathcal{B}) \vdash \mathcal{C}.$$

Применив **Теорему Дедукции**, получим

$$\Gamma \vdash ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{C}).$$

□

Следующее следствие позволяет разъединять посылки.

Следствие 2.3.10.3. Для любых формул \mathcal{A} , \mathcal{B} , \mathcal{C} и любого множества формул Γ : если

$$\Gamma \vdash ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{C}),$$

то

$$\Gamma \vdash (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})).$$

Д о к а з а т е л ь с т в о. Если

$$\Gamma \vdash ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{C}),$$

то по **Теореме Дедукции**

$$\Gamma, (\mathcal{A} \& \mathcal{B}) \vdash \mathcal{C}.$$

Так как, кроме того,

$$\mathcal{A}, \mathcal{B} \vdash (\mathcal{A} \& \mathcal{B}),$$

то, применяя теорему 2.3.3, получаем

$$\Gamma, \mathcal{A}, \mathcal{B} \vdash \mathcal{C}.$$

Применив **Теорему Дедукции**, получим

$$\Gamma \vdash (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})).$$

□

Теорема 2.3.11. Для любых формул \mathcal{A} и \mathcal{B}

1. $((\neg \mathcal{B}) \rightarrow (\neg \mathcal{A})) \vdash (\mathcal{A} \rightarrow \mathcal{B})$,
2. $(\mathcal{A} \rightarrow \mathcal{B}) \vdash ((\neg \mathcal{B}) \rightarrow (\neg \mathcal{A}))$.

Д о к а з а т е л ь с т в о. 1. Используя логическую аксиому IV.1, получаем

$$\vdash (((\neg \mathcal{B}) \rightarrow (\neg \mathcal{A})) \rightarrow (\mathcal{A} \rightarrow (\neg(\neg \mathcal{B}))))).$$

Применив два раза **Теорему Дедукции**, получим

$$((\neg \mathcal{B}) \rightarrow (\neg \mathcal{A})), \mathcal{A} \vdash (\neg(\neg \mathcal{B})).$$

Тогда в силу следствия теоремы 2.3.6 получаем

$$((\neg \mathcal{B}) \rightarrow (\neg \mathcal{A})), \mathcal{A} \vdash \mathcal{B}.$$

Используя **Теорему Дедукции**, получаем

$$((\neg \mathcal{B}) \rightarrow (\neg \mathcal{A})) \vdash (\mathcal{A} \rightarrow \mathcal{B}).$$

2. Так как, очевидно, что

$$(\mathcal{A} \rightarrow \mathcal{B}), \mathcal{A} \vdash \mathcal{B},$$

то в силу следствия теоремы 2.3.6, получаем

$$(\mathcal{A} \rightarrow \mathcal{B}), \mathcal{A} \vdash (\neg(\neg\mathcal{B})).$$

По **Теореме Дедукции** получаем

$$(\mathcal{A} \rightarrow \mathcal{B}) \vdash (\mathcal{A} \rightarrow (\neg(\neg\mathcal{B}))).$$

Используя логическую аксиому II.1, получаем

$$\vdash ((\mathcal{A} \rightarrow (\neg(\neg\mathcal{B}))) \rightarrow ((\neg\mathcal{B}) \rightarrow (\neg\mathcal{A}))).$$

По **Теореме Дедукции**

$$(\mathcal{A} \rightarrow (\neg(\neg\mathcal{B}))) \vdash ((\neg\mathcal{B}) \rightarrow (\neg\mathcal{A})).$$

Значит, по теореме 2.3.3

$$(\mathcal{A} \rightarrow \mathcal{B}) \vdash ((\neg\mathcal{B}) \rightarrow (\neg\mathcal{A})).$$

□

Следствие 2.3.11.1. Для любых формул \mathcal{A} и \mathcal{B}

1. $\vdash (((\neg\mathcal{B}) \rightarrow (\neg\mathcal{A})) \rightarrow (\mathcal{A} \rightarrow \mathcal{B})),$
2. $\vdash ((\mathcal{A} \rightarrow \mathcal{B}) \rightarrow ((\neg\mathcal{B}) \rightarrow (\neg\mathcal{A}))).$

Д о к а з а т е л ь с т в о. Получается применением **Теоремы Дедукции**.

□

Следствие 2.3.11.2. Для любых формул \mathcal{A} , \mathcal{B} и любого множества формул Γ имеют место эквивалентности

1. $\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B})$ тогда и только тогда, когда $\Gamma \vdash ((\neg\mathcal{B}) \rightarrow (\neg\mathcal{A})).$
2. $\Gamma, \mathcal{A} \vdash \mathcal{B}$ тогда и только тогда, когда $\Gamma, (\neg\mathcal{B}) \vdash (\neg\mathcal{A}).$

Теорема 2.3.12. Для любых формул \mathcal{A} и \mathcal{B}

$$\mathcal{A}, (\neg\mathcal{B}) \vdash (\neg(\mathcal{A} \rightarrow \mathcal{B})).$$

Д о к а з а т е л ь с т в о. Так как

$$\mathcal{A}, (\mathcal{A} \rightarrow \mathcal{B}) \vdash \mathcal{B},$$

то по второму следствию предыдущей теоремы 2.3.11

$$\mathcal{A}, (\neg\mathcal{B}) \vdash (\neg(\mathcal{A} \rightarrow \mathcal{B})).$$

□

Следствие 2.3.12.1. Для любых формул \mathcal{A} и \mathcal{B}

$$\vdash (\mathcal{A} \rightarrow ((\neg \mathcal{B}) \rightarrow (\neg(\mathcal{A} \rightarrow \mathcal{B}))))).$$

Д о к а з а т е л ь с т в о. Достаточно два раза применить **Теорему Дедукции**. \square

Теорема 2.3.13. Для любых формул \mathcal{A} и \mathcal{B}

$$(\mathcal{A} \rightarrow \mathcal{B}), ((\neg \mathcal{A}) \rightarrow \mathcal{B}) \vdash \mathcal{B}.$$

Д о к а з а т е л ь с т в о. По теореме 2.3.11 получаем

$$((\neg \mathcal{A}) \rightarrow \mathcal{B}) \vdash ((\neg \mathcal{B}) \rightarrow (\neg(\neg \mathcal{A}))).$$

По **Теореме Дедукции** из этого следует, что

$$((\neg \mathcal{A}) \rightarrow \mathcal{B}), (\neg \mathcal{B}) \vdash (\neg(\neg \mathcal{A})).$$

Применяя следствие теоремы 2.3.6, получаем

$$((\neg \mathcal{A}) \rightarrow \mathcal{B}), (\neg \mathcal{B}) \vdash \mathcal{A}.$$

Применив теорему 2.3.12 и теорему 2.3.3, получим

$$((\neg \mathcal{A}) \rightarrow \mathcal{B}), (\neg \mathcal{B}) \vdash (\neg(\mathcal{A} \rightarrow \mathcal{B})).$$

Применив второе следствие теоремы 2.3.11, получим

$$((\neg \mathcal{A}) \rightarrow \mathcal{B}), (\mathcal{A} \rightarrow \mathcal{B}) \vdash \mathcal{B}.$$

\square

Следствие 2.3.13.1. Для любых формул \mathcal{A} и \mathcal{B}

$$\vdash ((\mathcal{A} \rightarrow \mathcal{B}) \rightarrow (((\neg \mathcal{A}) \rightarrow \mathcal{B}) \rightarrow \mathcal{B})).$$

Д о к а з а т е л ь с т в о. Достаточно два раза применить **Теорему Дедукции**. \square

Формула $(\mathcal{A} \vee (\neg \mathcal{A}))$ носит название **Закон исключенного третьего**.

Следствие 2.3.13.2. Для любой формулы \mathcal{A}

$$\vdash (\mathcal{A} \vee (\neg \mathcal{A})).$$

Д о к а з а т е л ь с т в о. Если в качестве формулы \mathcal{B} взять формулу $(\mathcal{A} \vee (\neg \mathcal{A}))$, то получим

$$(\mathcal{A} \rightarrow (\mathcal{A} \vee (\neg \mathcal{A}))), ((\neg \mathcal{A}) \rightarrow (\mathcal{A} \vee (\neg \mathcal{A}))) \vdash (\mathcal{A} \vee (\neg \mathcal{A})).$$

Заметим, что

$$\vdash (\mathcal{A} \rightarrow (\mathcal{A} \vee (\neg \mathcal{A}))), \quad \vdash ((\neg \mathcal{A}) \rightarrow (\mathcal{A} \vee (\neg \mathcal{A}))).$$

Поэтому по теореме 2.3.3 получаем

$$\vdash (\mathcal{A} \vee (\neg \mathcal{A})).$$

□

Следствие 2.3.13.3. Если $\Gamma, \mathcal{B} \vdash \mathcal{A}$ и $\Gamma, (\neg \mathcal{B}) \vdash \mathcal{A}$, то $\Gamma \vdash \mathcal{A}$.

Д о к а з а т е л ь с т в о. Если $\Gamma, \mathcal{B} \vdash \mathcal{A}$ и $\Gamma, (\neg \mathcal{B}) \vdash \mathcal{A}$, то по **Теореме Дедукции** $\Gamma \vdash (\mathcal{B} \rightarrow \mathcal{A})$ и $\Gamma \vdash ((\neg \mathcal{B}) \rightarrow \mathcal{A})$. И остается воспользоваться теоремой 2.3.4. □

Для произвольной интерпретации φ языка $L_{ЛВ}$ и для произвольной формулы \mathcal{A} этого языка полагаем

$$\mathcal{A}' \equiv \begin{cases} \mathcal{A}, & \text{если } \varphi(\mathcal{A}) = \text{И}, \\ (\neg \mathcal{A}), & \text{если } \varphi(\mathcal{A}) = \text{Л}. \end{cases}$$

Теорема Кальмара. Если все пропозициональные переменные, входящие в формулу \mathcal{A} , содержатся в списке A_1, \dots, A_n , то

$$A'_1, \dots, A'_n \vdash \mathcal{A}'.$$

Д о к а з а т е л ь с т в о. Проведем индукцию по числу k логических связок, входящих в формулу \mathcal{A} .

Если $k = 0$, то \mathcal{A} – это некоторая пропозициональная переменная A_i .

Но тогда $\mathcal{A}' \equiv A'_i$ и доказываемое утверждение следует из того, что

$$\mathcal{A}' \vdash \mathcal{A}'.$$

Сделаем индуктивное предположение, что доказываемое утверждение выполняется для формул, содержащих менее чем k логических связок.

Пусть теперь формула \mathcal{A} содержит k логических связок, причем $k > 0$.

Тогда формула \mathcal{A} имеет один из следующих видов:

1. $(\neg \mathcal{B})$, 2. $(\mathcal{B} \vee \mathcal{C})$,
3. $(\mathcal{B} \& \mathcal{C})$, 4. $(\mathcal{B} \rightarrow \mathcal{C})$.

Для сокращения обозначений полагаем

$$\Gamma \equiv \{A'_1, \dots, A'_n\}.$$

1. Пусть формула \mathcal{A} имеет вид $(\neg \mathcal{B})$.

Если $\varphi(\mathcal{A}) = \text{И}$, то $\mathcal{A}' = \mathcal{A}$.

Тогда $\varphi(\mathcal{B}) = \text{Л}$, поэтому $\mathcal{B}' = (\neg \mathcal{B}) = \mathcal{A}$.

По индуктивному предположению

$$\Gamma \vdash \mathcal{B}',$$

т. е.

$$\Gamma \vdash \mathcal{A}, \quad \Gamma \vdash \mathcal{A}'.$$

Если $\varphi(\mathcal{A}) = \text{Л}$, то $\mathcal{A}' = (\neg \mathcal{A})$.

Тогда $\varphi(\mathcal{B}) = \text{И}$, поэтому $\mathcal{B}' = \mathcal{B}$.

По индуктивному предположению

$$\Gamma \vdash \mathcal{B}',$$

т. е.

$$\Gamma \vdash \mathcal{B}.$$

Тогда по следствию теоремы 2.3.6

$$\Gamma \vdash (\neg(\neg \mathcal{B})).$$

Но $\mathcal{A}' = (\neg(\neg \mathcal{B}))$, значит,

$$\Gamma \vdash \mathcal{A}'.$$

2. $\mathcal{A} = (\mathcal{B} \rightarrow \mathcal{C})$.

Для большей наглядности построим следующую таблицу, в которой для сокращения вместо $(\neg \mathcal{D})$ пишем $\overline{\mathcal{D}}$.

\mathcal{B}	\mathcal{C}	\mathcal{A}	\mathcal{B}'	\mathcal{C}'	\mathcal{A}'	Индуктивное предположение	Доказать
И	И	И	\mathcal{B}	\mathcal{C}	\mathcal{A}	$\Gamma \vdash \mathcal{B}, \Gamma \vdash \mathcal{C},$	$\Gamma \vdash (\mathcal{B} \rightarrow \mathcal{C})$
Л	И	И	$\overline{\mathcal{B}}$	\mathcal{C}	\mathcal{A}	$\Gamma \vdash \overline{\mathcal{B}}, \Gamma \vdash \mathcal{C},$	$\Gamma \vdash (\mathcal{B} \rightarrow \mathcal{C})$
И	Л	Л	\mathcal{B}	$\overline{\mathcal{C}}$	$\overline{\mathcal{A}}$	$\Gamma \vdash \mathcal{B}, \Gamma \vdash \overline{\mathcal{C}},$	$\Gamma \vdash \overline{(\mathcal{B} \rightarrow \mathcal{C})}$
Л	Л	И	$\overline{\mathcal{B}}$	$\overline{\mathcal{C}}$	\mathcal{A}	$\Gamma \vdash \overline{\mathcal{B}}, \Gamma \vdash \overline{\mathcal{C}},$	$\Gamma \vdash (\mathcal{B} \rightarrow \mathcal{C})$

В случаях 2.1 и 2.2 по индуктивному предположению $\Gamma \vdash \mathcal{C}$. Так как

$$\vdash (\mathcal{C} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})),$$

то $\mathcal{C} \vdash (\mathcal{B} \rightarrow \mathcal{C})$.

Поэтому по теореме 2.3.3 получаем,

$$\Gamma \vdash (\mathcal{B} \rightarrow \mathcal{C}).$$

В случае 2.3, воспользовавшись теоремой 2.3.12

$$\mathcal{B}, (\neg\mathcal{C}) \vdash (\neg(\mathcal{B} \rightarrow \mathcal{C})),$$

индуктивным предположением

$$\Gamma \vdash \mathcal{B}, \quad \Gamma \vdash (\neg\mathcal{C})$$

и теоремой 2.3.3 получим

$$\Gamma \vdash (\neg(\mathcal{B} \rightarrow \mathcal{C})).$$

В случае 2.4 по индуктивному предположению $\Gamma \vdash (\neg\mathcal{B})$, что вместе с

$$\vdash ((\neg\mathcal{B}) \rightarrow ((\neg\mathcal{C}) \rightarrow (\neg\mathcal{B})))$$

дает

$$\Gamma \vdash ((\neg\mathcal{C}) \rightarrow (\neg\mathcal{B})).$$

Отсюда по следствию 2 теоремы 2.3.11 получаем

$$\Gamma \vdash (\mathcal{B} \rightarrow \mathcal{C}).$$

3. $\mathcal{A} = (\mathcal{B} \& \mathcal{C})$.

Вновь рассмотрим вспомогательную таблицу

\mathcal{B}	\mathcal{C}	\mathcal{A}	\mathcal{B}'	\mathcal{C}'	\mathcal{A}'	Индуктивное предположение	Доказать
И	И	И	\mathcal{B}	\mathcal{C}	\mathcal{A}	$\Gamma \vdash \mathcal{B}, \Gamma \vdash \mathcal{C},$	$\Gamma \vdash (\mathcal{B} \& \mathcal{C})$
Л	И	Л	$\overline{\mathcal{B}}$	\mathcal{C}	$\overline{\mathcal{A}}$	$\Gamma \vdash \overline{\mathcal{B}}, \Gamma \vdash \mathcal{C},$	$\Gamma \vdash \overline{(\mathcal{B} \& \mathcal{C})}$
И	Л	Л	\mathcal{B}	$\overline{\mathcal{C}}$	$\overline{\mathcal{A}}$	$\Gamma \vdash \mathcal{B}, \Gamma \vdash \overline{\mathcal{C}},$	$\Gamma \vdash \overline{(\mathcal{B} \& \mathcal{C})}$
Л	Л	Л	$\overline{\mathcal{B}}$	$\overline{\mathcal{C}}$	$\overline{\mathcal{A}}$	$\Gamma \vdash \overline{\mathcal{B}}, \Gamma \vdash \overline{\mathcal{C}},$	$\Gamma \vdash \overline{(\mathcal{B} \& \mathcal{C})}$

В случае 3.1 по индуктивному предположению

$$\Gamma \vdash \mathcal{B}, \quad \Gamma \vdash \mathcal{C},$$

по теореме 2.3.5 получаем

$$\Gamma \vdash (\mathcal{B} \& \mathcal{C}).$$

В случае 3.2 из того, что

$$\vdash ((\mathcal{B} \& \mathcal{C}) \rightarrow \mathcal{B})$$

по следствию 1 теоремы 2.3.11 получаем

$$\vdash ((\neg\mathcal{B}) \rightarrow (\neg(\mathcal{B} \& \mathcal{C}))),$$

что вместе с индуктивным предположением $\Gamma \vdash (\neg \mathcal{B})$ дает

$$\Gamma \vdash (\neg(\mathcal{B} \& \mathcal{C})).$$

В случаях 3.3 и 3.4 из того, что

$$\vdash ((\mathcal{B} \& \mathcal{C}) \rightarrow \mathcal{C})$$

по следствию 1 теоремы 2.3.11 получаем

$$\vdash ((\neg \mathcal{C}) \rightarrow (\neg(\mathcal{B} \& \mathcal{C}))),$$

что вместе с индуктивным предположением $\Gamma \vdash (\neg \mathcal{C})$ дает

$$\Gamma \vdash (\neg(\mathcal{B} \& \mathcal{C})).$$

4. $\mathcal{A} \equiv (\mathcal{B} \vee \mathcal{C})$.

Построим вспомогательную таблицу

\mathcal{B}	\mathcal{C}	\mathcal{A}	\mathcal{B}'	\mathcal{C}'	\mathcal{A}'	Индуктивное предположение	Доказать
И	И	И	\mathcal{B}	\mathcal{C}	\mathcal{A}	$\Gamma \vdash \mathcal{B}, \Gamma \vdash \mathcal{C},$	$\Gamma \vdash (\mathcal{B} \vee \mathcal{C})$
Л	И	И	$\overline{\mathcal{B}}$	\mathcal{C}	\mathcal{A}	$\Gamma \vdash \overline{\mathcal{B}}, \Gamma \vdash \mathcal{C},$	$\Gamma \vdash (\mathcal{B} \vee \mathcal{C})$
И	Л	И	\mathcal{B}	$\overline{\mathcal{C}}$	\mathcal{A}	$\Gamma \vdash \mathcal{B}, \Gamma \vdash \overline{\mathcal{C}},$	$\Gamma \vdash (\mathcal{B} \vee \mathcal{C})$
Л	Л	Л	$\overline{\mathcal{B}}$	$\overline{\mathcal{C}}$	$\overline{\mathcal{A}}$	$\Gamma \vdash \overline{\mathcal{B}}, \Gamma \vdash \overline{\mathcal{C}},$	$\Gamma \vdash \overline{(\mathcal{B} \vee \mathcal{C})}$

В случаях 4.1 и 4.2 из

$$\vdash (\mathcal{C} \rightarrow (\mathcal{B} \vee \mathcal{C}))$$

по **Теореме Дедукции** получаем

$$\mathcal{C} \vdash (\mathcal{B} \vee \mathcal{C}).$$

Отсюда по индуктивному предположению $\Gamma \vdash \mathcal{C}$ с использованием теоремы 2.3.3 получаем

$$\Gamma \vdash (\mathcal{B} \vee \mathcal{C}).$$

В случае 4.3 из

$$\vdash (\mathcal{B} \rightarrow (\mathcal{B} \vee \mathcal{C}))$$

и индуктивного предположения $\Gamma \vdash \mathcal{B}$ аналогичным образом получаем

$$\Gamma \vdash (\mathcal{B} \vee \mathcal{C}).$$

Рассмотрим случай 4.4. Воспользовавшись логической аксиомой III.3, получим

$$\vdash ((\mathcal{B} \rightarrow \mathcal{D}) \rightarrow ((\mathcal{C} \rightarrow \mathcal{D}) \rightarrow ((\mathcal{B} \vee \mathcal{C}) \rightarrow \mathcal{D}))).$$

По **Теореме Дедукции** получаем

$$(\mathcal{B} \rightarrow \mathcal{D}), (\mathcal{C} \rightarrow \mathcal{D}) \vdash ((\mathcal{B} \vee \mathcal{C}) \rightarrow \mathcal{D}).$$

По теореме 2.3.7 $(\neg \mathcal{B}), \mathcal{B} \vdash \mathcal{D}$, что вместе с индуктивным предположением $\Gamma \vdash (\neg \mathcal{B})$ по теореме 2.3.3 дает

$$\Gamma, \mathcal{B} \vdash \mathcal{D}.$$

По **Теореме Дедукции** получаем

$$\Gamma \vdash (\mathcal{B} \rightarrow \mathcal{D}).$$

Аналогично показывается, что

$$\Gamma \vdash (\mathcal{C} \rightarrow \mathcal{D}).$$

Поэтому по теореме 2.3.3 получаем

$$\Gamma \vdash ((\mathcal{B} \vee \mathcal{C}) \rightarrow \mathcal{D}).$$

Отсюда по следствию 2 теоремы 2.3.11 получаем

$$\Gamma \vdash ((\neg \mathcal{D}) \rightarrow (\neg(\mathcal{B} \vee \mathcal{C}))).$$

Взяв в качестве формулы \mathcal{D} формулу \mathcal{B} , получим

$$\Gamma \vdash ((\neg \mathcal{B}) \rightarrow (\neg(\mathcal{B} \vee \mathcal{C}))),$$

$$\Gamma, (\neg \mathcal{B}) \vdash (\neg(\mathcal{B} \vee \mathcal{C})).$$

По индуктивному предположению $\Gamma \vdash (\neg \mathcal{B})$, поэтому в силу теоремы 2.3.3 получаем

$$\Gamma \vdash (\neg(\mathcal{B} \vee \mathcal{C})).$$

Это завершает доказательство теоремы. □

Теорема Э. Поста. Для любой формулы \mathcal{A} языка логики высказываний $L_{ЛВ}$ имеет место эквивалентность:

$$\models \mathcal{A} \iff \vdash \mathcal{A}.$$

Д о к а з а т е л ь с т в о. 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 φ

$$A'_1, \dots, A'_{n-1}, A_n \vdash \mathcal{A}, \quad A'_1, \dots, A'_{n-1}, (\neg A_n) \vdash \mathcal{A}.$$

Откуда по следствию 3 теоремы 2.3.13 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

$$\models \mathcal{A}, \quad \models (\mathcal{A} \rightarrow \mathcal{B}),$$

то

$$\models \mathcal{B}.$$

Проведение указанных рассуждений предоставляется читателю в качестве простого, но полезного упражнения. \square

2.4. Дополнительные вопросы Логике и Исчисления Высказываний

Теорема Адекватности. Для любого множества формул Γ и любой формулы \mathcal{A} имеет место эквивалентность:

$$\Gamma \models \mathcal{A} \iff \Gamma \vdash \mathcal{A}.$$

Д о к а з а т е л ь с т в о. Индукцией по длине вывода формулы \mathcal{A} из множества формул Γ убеждаемся в том, что если $\Gamma \vdash \mathcal{A}$, то $\Gamma \models \mathcal{A}$.

Для доказательства обратного утверждения рассмотрим сначала случай, когда Γ – конечное множество. Пусть оно состоит из формул

$$\mathcal{B}_1, \dots, \mathcal{B}_n$$

и $\Gamma \models \mathcal{A}$, т. е.

$$\mathcal{B}_1, \dots, \mathcal{B}_n \models \mathcal{A},$$

Тогда

$$\models (\mathcal{B}_1 \rightarrow (\mathcal{B}_2 \rightarrow (\dots(\mathcal{B}_n \rightarrow \mathcal{A})\dots))).$$

Откуда по теореме Э. Поста получаем

$$\vdash (\mathcal{B}_1 \rightarrow (\mathcal{B}_2 \rightarrow (\dots(\mathcal{B}_n \rightarrow \mathcal{A})\dots))).$$

Применяя n раз **Теорему Дедукции**, получаем

$$\mathcal{B}_1, \dots, \mathcal{B}_n \vdash \mathcal{A},$$

т. е. $\Gamma \vdash \mathcal{A}$.

Если Γ – бесконечное множество формул и $\Gamma \models \mathcal{A}$, то воспользуемся следствием **Теоремы Компактности**, в соответствии с которым найдется конечное подмножество Γ_0 множества Γ такое, что $\Gamma_0 \models \mathcal{A}$. Тогда в силу уже доказанной части теоремы $\Gamma_0 \vdash \mathcal{A}$, а значит, и $\Gamma \vdash \mathcal{A}$. 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 $L_{ИВ}$ **Исчисления Высказываний**.

Начнем с более традиционного подхода.

Определение 2.4.1. Множество формул Γ языка $L_{ИВ}$ **Исчисления Высказываний** называется **полным**, если оно непротиворечиво и для любой формулы \mathcal{A} языка $L_{ИВ}$

$$\Gamma \vdash \mathcal{A} \quad \text{либо} \quad \Gamma \vdash (\neg \mathcal{A}).$$

Предварительно докажем вспомогательную теорему.

Теорема 2.4.1. Если для множества формул Γ и формул \mathcal{A} и \mathcal{B} выполнены условия

$$\Gamma, (\neg \mathcal{A}) \vdash \mathcal{B} \quad \text{и} \quad \Gamma, (\neg \mathcal{A}) \vdash (\neg \mathcal{B}),$$

то

$$\Gamma \vdash \mathcal{A}.$$

Д о к а з а т е л ь с т в о. Если

$$\Gamma, (\neg \mathcal{A}) \vdash \mathcal{B} \quad \text{и} \quad \Gamma, (\neg \mathcal{A}) \vdash (\neg \mathcal{B}),$$

то по следствию 1 теоремы 2.3.7 для любой формулы \mathcal{C} имеем

$$\Gamma, (\neg \mathcal{A}) \vdash (\neg \mathcal{C}).$$

Тогда по пункту 2 следствия 2 теоремы 2.3.11 получаем

$$\Gamma, \mathcal{C} \vdash \mathcal{A}.$$

Взяв в качестве формулы \mathcal{C} любую такую формулу, что

$$\Gamma \vdash \mathcal{C},$$

например, в качестве такой формулы \mathcal{C} можно взять любую логическую аксиому, получим по теореме 2.3.4

$$\Gamma \vdash \mathcal{A}.$$

□

Теорема о пополнении. Для любого непротиворечивого множества формул Γ языка $L_{ИВ}$ **Исчисления Высказываний** существует такое **полное** множество формул Γ^* языка $L_{ИВ}$, что

$$\Gamma \subseteq \Gamma^*.$$

Доказательство. Выше уже отмечалось, что так как алфавит языка $L_{ИВ}$ **Исчисления Высказываний** счетен, то счетным является и множество $F_{ИВ}$ всех формул **Исчисления Высказываний**.

Пусть $F_{ИВ} = (\Phi_n)_{n \in N}$.

Определим последовательность $(\Gamma_n)_{n \in N}$ множеств формул.

Полагаем $\Gamma_1 \Leftarrow \Gamma$.

Если множество Γ_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 Γ_n является непротиворечивым.

Так как $\Gamma_1 \Leftarrow \Gamma$, то по условию теоремы множество формул Γ_1 является непротиворечивым.

Предположим, что уже доказана непротиворечивость множества формул Γ_n .

Допустим, что множество формул Γ_{n+1} является противоречивым. Тогда для любой формулы \mathcal{A}

$$\Gamma_{n+1} \vdash \mathcal{A}.$$

Если $\Gamma_n \vdash \Phi_n$, то

$$\Gamma_{n+1} = \Gamma_n \cup \{\Phi_n\},$$

поэтому

$$\Gamma_n \vdash \mathcal{A}.$$

Так как \mathcal{A} – любая формула, то это противоречит предположению о непротиворечивости множества формул Γ_n .

Значит, $\Gamma_n \not\vdash \Phi_n$, поэтому $\Gamma_{n+1} = \Gamma_n \cup \{(\neg \Phi_n)\}$.

Из противоречивости множества формул Γ_{n+1} следует, что для любой формулы \mathcal{B}

$$\Gamma_{n+1} \vdash \mathcal{B} \quad \text{и} \quad \Gamma_{n+1} \vdash (\neg \mathcal{B}),$$

т. е.

$$\Gamma_n, (\neg \Phi_n) \vdash \mathcal{B} \quad \text{и} \quad \Gamma_n, (\neg \Phi_n) \vdash (\neg \mathcal{B}),$$

но тогда по теореме 2.4.1

$$\Gamma_n \vdash \Phi_n.$$

Но последнее противоречит условию $\Gamma_n \not\vdash \Phi_n$.

Тем самым доказано, что *при любом n множество формул Γ_n является непротиворечивым.*

Полагаем

$$\Gamma^* \Leftarrow \bigcup_{n=1}^{\infty} \Gamma_n.$$

Покажем, что Γ^* – **полное** множество формул и

$$\Gamma \subseteq \Gamma^*.$$

Последнее очевидно, так как

$$\Gamma = \Gamma_1 \subseteq \Gamma^*.$$

Если бы множество формул Γ^* было противоречивым, то для некоторой формулы \mathcal{B} мы имели бы

$$\Gamma^* \vdash \mathcal{B} \quad \text{и} \quad \Gamma^* \vdash (\neg \mathcal{B}).$$

Но тогда найдется **конечное** множество формул $T \subseteq \Gamma^*$ такое, что

$$T \vdash \mathcal{B} \quad \text{и} \quad T \vdash (\neg \mathcal{B}).$$

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

$$\Gamma_n \vdash \mathcal{B} \quad \text{и} \quad \Gamma_n \vdash (\neg \mathcal{B}),$$

что противоречит установленной выше непротиворечивости каждого множества формул Γ_n .

Докажем, что Γ^* – 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 Γ^* – **полное** множество формул языка L_{IV} такое, что

$$\Gamma \subseteq \Gamma^*.$$

□

Теорема Непротиворечивости. Для любого множества формул Γ языка L_{IV} **Исчисления Высказываний** имеет место эквивалентность:

множество формул Γ 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 Γ , являющееся противоречивым.

Тогда для некоторой формулы \mathcal{B}

$$\Gamma \vdash \mathcal{B} \quad \text{и} \quad \Gamma \vdash (\neg\mathcal{B}).$$

Индукцией по длине вывода из множества формул устанавливаем, что для любого множества формул Γ и любой формулы \mathcal{A} из

$$\Gamma \vdash \mathcal{A}$$

следует

$$\Gamma \models \mathcal{A}.$$

Так как по предположению Γ – совместное множество формул, то найдется такая интерпретация φ , 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 Γ является совместным*.

По теореме о пополнении существует **полное** множество формул Γ^* такое, что

$$\Gamma \subseteq \Gamma^*.$$

Покажем, что *множество формул Γ^* является совместным*. Отсюда, конечно, сразу будет следовать совместность и множества формул Γ .

Построим интерпретацию φ 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 Γ^* – **полное** 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 φ определена корректно.

Обычным образом продолжаем отображение φ , заданное на множестве Σ_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 φ .

(ii) Предположим, что указанная эквивалентность имеет место для формул \mathcal{A} и \mathcal{B} и докажем, что тогда она выполняется и для формул

$$(\neg\mathcal{A}), \quad (\mathcal{A} \& \mathcal{B}),$$

$$(\mathcal{A} \vee \mathcal{B}), \quad (\mathcal{A} \rightarrow \mathcal{B}).$$

Так как

$$\Gamma^* \vdash (\neg\mathcal{A}) \iff \Gamma^* \not\vdash \mathcal{A},$$

$$\Gamma^* \not\vdash \mathcal{A} \iff \varphi(\mathcal{A}) = \text{Л}$$

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 2.3.5

$$\Gamma^* \vdash (\mathcal{A} \& \mathcal{B}) \iff \Gamma^* \vdash \mathcal{A} \text{ и } \Gamma^* \vdash \mathcal{B}$$

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 множества формул Γ^* 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 Γ^* — **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 2.3.1 и теорему 2.3.4, получим

$$(\mathcal{B} \rightarrow \mathcal{A}) \vdash ((\mathcal{A} \vee \mathcal{B}) \rightarrow \mathcal{A}).$$

Так как по теореме 2.3.7

$$(\neg \mathcal{B}), \mathcal{B} \vdash \mathcal{A},$$

то применив *Теорему Дедукции*, получим

$$(\neg \mathcal{B}) \vdash (\mathcal{B} \rightarrow \mathcal{A}).$$

Так как

$$\Gamma^* \vdash (\neg \mathcal{B}),$$

то по теореме 2.3.3 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 2.3.3 дает

$$\Gamma^* \vdash ((\mathcal{A} \vee \mathcal{B}) \rightarrow \mathcal{A}).$$

По следствию 2 теоремы 2.3.12 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 2.3.3 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 Γ^* .

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 Γ^* 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

$$\Gamma^* \vdash (\neg \mathcal{B}) \text{ и } \Gamma^* \vdash \mathcal{A}.$$

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 2.3.11 получаем

$$(\neg(\mathcal{A} \rightarrow \mathcal{B})) \vdash (\neg \mathcal{B}),$$

что вместе с

$$\Gamma^* \vdash (\neg(\mathcal{A} \rightarrow \mathcal{B}))$$

по теореме 2.3.4 дает

$$\Gamma^* \vdash (\neg \mathcal{B}).$$

По теореме 2.3.7

$$(\neg \mathcal{A}), \mathcal{A} \vdash \mathcal{B}.$$

Применив **Теорему Дедукции**, получим

$$(\neg \mathcal{A}) \vdash (\mathcal{A} \rightarrow \mathcal{B}).$$

Тогда по пункту 2 следствия 2 теоремы 2.3.11 получаем

$$(\neg(\mathcal{A} \rightarrow \mathcal{B})) \vdash (\neg(\neg\mathcal{A})),$$

что вместе с

$$\Gamma^* \vdash (\neg(\mathcal{A} \rightarrow \mathcal{B}))$$

по теореме 2.3.4 дает

$$\Gamma^* \vdash (\neg(\neg\mathcal{A})).$$

Тогда по следствию теоремы 2.3.6 получаем

$$\Gamma^* \vdash \mathcal{A}.$$

Итак, если

$$\Gamma^* \vdash (\neg(\mathcal{A} \rightarrow \mathcal{B})),$$

то

$$\Gamma^* \vdash \mathcal{A}$$

и

$$\Gamma^* \vdash (\neg\mathcal{B}).$$

По индуктивному предположению тогда получаем

$$\varphi(\mathcal{A}) = \text{И} \quad \text{и} \quad \varphi(\mathcal{B}) = \text{Л}.$$

Значит,

$$\varphi((\mathcal{A} \rightarrow \mathcal{B})) = \text{Л}.$$

Тем самым показано, что

$$\Gamma^* \vdash (\neg(\mathcal{A} \rightarrow \mathcal{B})) \implies \varphi((\mathcal{A} \rightarrow \mathcal{B})) = \text{Л}.$$

Чтобы доказать, что

$$\varphi((\mathcal{A} \rightarrow \mathcal{B})) = \text{Л} \implies \Gamma^* \vdash (\neg(\mathcal{A} \rightarrow \mathcal{B})),$$

предположим, что

$$\varphi((\mathcal{A} \rightarrow \mathcal{B})) = \text{Л}.$$

Но тогда

$$\varphi(\mathcal{A}) = \text{И} \quad \text{и} \quad \varphi(\mathcal{B}) = \text{Л}.$$

Отсюда по индуктивному предположению получаем

$$\Gamma^* \vdash \mathcal{A}$$

и

$$\Gamma^* \vdash (\neg\mathcal{B}).$$

По теореме 2.3.12

$$\mathcal{A}, (\neg \mathcal{B}) \vdash (\neg(\mathcal{A} \rightarrow \mathcal{B})),$$

что вместе с двумя предыдущими фактами по теореме 2.3.4 дает

$$\Gamma^* \vdash (\neg(\mathcal{A} \rightarrow \mathcal{B})).$$

Тем самым доказано, что

$$\varphi((\mathcal{A} \rightarrow \mathcal{B})) = \text{Л} \implies \Gamma^* \vdash (\neg(\mathcal{A} \rightarrow \mathcal{B})).$$

В итоге доказано, что для произвольной формулы \mathcal{A} имеет место эквивалентность:

$$\Gamma^* \vdash \mathcal{A} \iff \varphi(\mathcal{A}) = \text{И}.$$

Если \mathcal{A} – произвольная формула из множества Γ^* , то, очевидно,

$$\Gamma^* \vdash \mathcal{A},$$

поэтому

$$\varphi(\mathcal{A}) = \text{И}.$$

Значит,

$$\varphi(\Gamma^*) = \text{И},$$

поэтому множество формул Γ^* является совместным. \square

Теорема Адекватности. Для любой формулы \mathcal{A} языка $L_{ЛВ}$ и для любого множества формул Γ этого языка имеет место следующая эквивалентность:

формула \mathcal{A} является логическим следствием множества формул Γ тогда и только тогда, когда формула \mathcal{A} выводима из этого множества формул Γ .

Доказательство. В ходе доказательства **Теоремы Непротиворечивости** было показано, что если формула \mathcal{A} выводима из множества формул Γ , то формула \mathcal{A} является логическим следствием этого множества формул Γ .

Докажем, что верно и обратное:

если формула \mathcal{A} является логическим следствием множества формул Γ , то формула \mathcal{A} выводима из этого множества формул Γ .

Пусть формула \mathcal{A} является логическим следствием множества формул Γ .

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 2.4.1

$$\Gamma \vdash \mathcal{A}. \quad \square$$

\square

2.5. Алгебра Линденбаума для Исчисления Высказываний

В этом параграфе рассматривается еще один подход к доказательству **Теоремы Непротиворечивости**. Этот подход можно было бы условно назвать *алгебраическим*.

На множестве F_{IV} 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_{IV} всех формул **Исчисления Высказываний** по этому отношению эквивалентности превращается в булеву алгебру, которая называется **Алгеброй Линденбаума для Исчисления Высказываний**, если положить

$$[\mathcal{A}] \cup [\mathcal{B}] \equiv [\mathcal{A} \vee \mathcal{B}],$$

$$[\mathcal{A}] \cap [\mathcal{B}] \equiv [\mathcal{A} \& \mathcal{B}],$$

$$[\overline{\mathcal{A}}] \equiv [(\neg \mathcal{A})],$$

$$0 \equiv [(\neg(A_1 \vee (\neg A_1)))],$$

$$1 \equiv [(A_1 \vee (\neg A_1))].$$

Для произвольного множества формул Γ полагаем

$$[\Gamma] \equiv \{ [\mathcal{A}] \mid \mathcal{A} \in \Gamma \}.$$

Лемма адекватности. Если Γ – 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 $[\mathcal{A}_1 \& \dots \& \mathcal{A}_n] = 0 = [(\neg(A_1 \vee (\neg A_1)))]$, поэтому

$$\Gamma \vdash ((\mathcal{A}_1 \& \dots \& \mathcal{A}_n) \longleftrightarrow (\neg(A_1 \vee (\neg A_1)))).$$

Значит,

$$\Gamma \vdash ((\mathcal{A}_1 \& \dots \& \mathcal{A}_n) \rightarrow (\neg(A_1 \vee (\neg A_1)))).$$

Тогда по следствию 2 теоремы 2.3.11

$$\Gamma \vdash ((A_1 \vee (\neg A_1)) \rightarrow (\neg(\mathcal{A}_1 \& \dots \& \mathcal{A}_n))).$$

А по **Теореме Дедукции**

$$\Gamma, (A_1 \vee (\neg A_1)) \vdash (\neg(\mathcal{A}_1 \& \dots \& \mathcal{A}_n)).$$

По следствию 2 теоремы 2.3.13 $\Gamma \vdash (A_1 \vee (\neg A_1))$, поэтому по теореме 2.3.3 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* Γ . □

Докажем *совместность* любого непротиворечивого множества формул Γ , что составляет основную часть **Теоремы Непротиворечивости**.

Пусть D – ультрафильтр, содержащий множество $[\Gamma]$.

Полагаем $\varphi(A_i) \Rightarrow \text{И}$ тогда и только тогда, когда $[A_i] \in D$.

Стандартным образом продолжаем отображение φ на множество $F_{\text{ИВ}}$ всех формул **Исчисления Высказываний**.

По той же схеме, что и выше, доказываем справедливость эквивалентности

$$\varphi(\mathcal{A}) = \text{И тогда и только тогда, когда } [\mathcal{A}] \in D,$$

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 Γ **совместно**.

2.6. Метод резолюций для логики высказываний

В этом разделе мы вернемся к уже рассмотренному нами вопросу о **логическом следствии** множества формул.

Напомним, что для любых формул $\mathcal{F}_1, \mathcal{F}_2, \dots, \mathcal{F}_n$ и \mathcal{F} **Логики Высказываний** имеет место эквивалентность:

формула \mathcal{F} является **логическим следствием** множества формул

$$\{\mathcal{F}_1, \mathcal{F}_2, \dots, \mathcal{F}_n\}$$

Логики Высказываний тогда и только тогда, когда множество формул

$$\{\mathcal{F}_1, \mathcal{F}_2, \dots, \mathcal{F}_n, (\neg \mathcal{F})\}$$

невыполнимо (несовместно).

Поэтому вопрос о логических следствиях множеств формул равносильен вопросу о выполнимости (совместности) множеств формул. **Метод резолюций** – один из хорошо известных подходов к изучению последнего вопроса. Мы не будем обсуждать достоинства и недостатки **Метода резолюций** с точки зрения времени, необходимого для получения ответа по произвольным входным данным.

Литералами называются пропозициональные переменные A_n и их отрицания ($\neg A_n$), которые будем обозначать через $\neg A_n$. При этом литералы A_n и $\neg A_n$ будут называться **противоположными**.

Дизъюнктом называется любое выражение вида $A_1 \vee \dots \vee A_n$, где A_1, \dots, A_n – произвольные литералы ($n \geq 0$). При $n = 1$ получаем просто литерал, а при $n = 0$ – *пустой дизъюнкт*, который принято обозначать через $[]$. Считается, что *пустой дизъюнкт* $[]$ ложен в любой интерпретации (невыполним), поэтому формула $A \& []$ тождественно ложна (невыполнима, равносильна $[]$), а формула $A \vee []$ равносильна формуле A .

При работе с дизъюнктами их удобно рассматривать просто как множества литералов, т. е. не различают дизъюнкты, получаемые друг из друга с помощью законов ассоциативности ($(A \vee B) \vee C \equiv A \vee (B \vee C)$), коммутативности ($A \vee B \equiv B \vee A$) и идемпотентности ($A \vee A \equiv A$).

Правилом резолюций в **Логике Высказываний** называется следующее правило вывода

$$\frac{U \vee L \vee V, W \vee \neg L \vee Z}{U \vee V \vee W \vee Z}.$$

Заметим, что из формул $U \vee L \vee V$ и $W \vee \neg L \vee Z$ логически следует формула $U \vee V \vee W \vee Z$.

Определение 2.6.1. **Выводом из множества дизъюнктов** Γ называется любая конечная последовательность дизъюнктов D_1, \dots, D_n такая, что для любого i ($1 \leq i \leq n$) либо 1) $D_i \in \Gamma$, либо 2) найдутся $j, k < i$ такие, что D_i получается из D_j и D_k по правилу резолюций.

Дизъюнкт D называется **выводимым** из множества дизъюнктов Γ , если существует вывод из этого множества дизъюнктов, оканчивающийся дизъюнктом D .

Теорема 2.6.1. Если дизъюнкт D выводим из множества дизъюнктов Γ , то он является логическим следствием этого множества Γ .

До к а з а т е л ь с т в о. Легко видеть, что если дизъюнкт D_i получается из дизъюнктов D_j и D_k по правилу резолюций, то он является их логическим следствием. Поэтому доказательство теоремы легко получается индукцией по длине вывода. \square

Следующая теорема, носящая название **теорема о полноте метода резолюций**, служит основой метода резолюций.

Теорема 2.6.2. Множество дизъюнктов Γ **невыполнимо** тогда и только тогда, когда из него **выводим пустой дизъюнкт** $[]$.

Д о к а з а т е л ь с т в о. Если из множества дизъюнктов Γ выводим пустой дизъюнкт \square , то по предыдущей теореме он является логическим следствием этого множества дизъюнктов Γ . Так как пустой дизъюнкт \square ложен в любой интерпретации, то множество дизъюнктов Γ невыполнимо.

Для доказательства обратного утверждения *предположим, что множество дизъюнктов Γ невыполнимо*. Покажем, что тогда из этого множества выводим пустой дизъюнкт \square .

Если $\square \in \Gamma$, то утверждение очевидно.

Пусть $\square \notin \Gamma$. Доказательство проведем индукцией по параметру $d(\Gamma)$, равному *суммарному числу вхождений литералов в дизъюнкты из множества Γ минус число элементов в Γ (число дизъюнктов)*. Так как в каждый дизъюнкт по предположению входит хотя бы один литерал (в Γ не входит пустой дизъюнкт), то $d(\Gamma) \geq 0$.

Если $d(\Gamma) = 0$, то все дизъюнкты из Γ – это литералы. Так как множество Γ несовместно, то в Γ входит пара противоположных литералов L и $\neg L$. Тогда последовательность $L, \neg L, \square$ является выводом из Γ пустого литерала.

Пусть $d(\Gamma) > 0$. Тогда в Γ входит дизъюнкт, отличный от литерала. Пусть

$$\Gamma = \{D_1, D_2, \dots, D_{n-1}, D_n\}, \quad D_n = L \vee D_n^*.$$

Введем обозначения

$$\Gamma_1 = \{D_1, D_2, \dots, D_{n-1}, L\},$$

$$\Gamma_2 = \{D_1, D_2, \dots, D_{n-1}, D_n^*\}.$$

Ясно, что оба множества дизъюнктов Γ_1 и Γ_2 *несовместны*, так как в противном случае совместным было бы и множество дизъюнктов Γ . Кроме того, $d(\Gamma_1), d(\Gamma_2) < d(\Gamma)$. Поэтому, по индуктивному предположению, из каждого множества дизъюнктов Γ_1 и Γ_2 выводим пустой дизъюнкт \square . Рассмотрим соответствующие выводы

$$\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_{l-1}, \mathcal{A}_l = \square \text{ — вывод из } \Gamma_1,$$

$$\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_{m-1}, \mathcal{B}_m = \square \text{ — вывод из } \Gamma_2.$$

Если в первом выводе отсутствует дизъюнкт (литерал) L , то этот вывод является выводом из множества дизъюнктов Γ пустого дизъюнкта \square .

Аналогично, если во втором выводе отсутствует дизъюнкт D_n^* , то этот вывод является выводом из множества дизъюнктов Γ пустого дизъюнкта \square .

Поэтому остается рассмотреть случай, когда в первом выводе присутствует дизъюнкт (литерал) L и обоснованием правомочности его присутствия в выводе служит утверждение $L \in \Gamma_1$, а во втором выводе присутствует дизъюнкт D_n^* и обоснованием правомочности его присутствия в выводе служит утверждение $D_n^* \in \Gamma_2$. Без ограничения общности можно считать, что $L = \mathcal{A}_1$ и $D_n^* = \mathcal{B}_1$.

Прежде чем преобразовывать эти два вывода в вывод из множества дизъюнктов Γ пустого дизъюнкта \square , введем понятие *зависимости в выводе* одного дизъюнкта от другого.

Если дизъюнкт S получается из дизъюнктов S_1 и S_2 по правилу резолюций, то говорят, что дизъюнкт S *непосредственно зависит* от дизъюнкта S_1 и дизъюнкт S *непосредственно зависит* от дизъюнкта S_2 . Транзитивное замыкание отношения *непосредственной зависимости* называется отношением *зависимости*.

Преобразуем вывод $\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_{m-1}, \mathcal{B}_m = []$ из множества дизъюнктов Γ_2 в вывод $\mathcal{B}_1^*, \mathcal{B}_2^*, \dots, \mathcal{B}_{m-1}^*, \mathcal{B}_m^*$ из множества дизъюнктов Γ . Полагаем \mathcal{B}_1^* равным $L \vee \mathcal{B}_1$, т. е. $L \vee D_n^*$, а при $i \geq 2$ \mathcal{B}_i^* равным $L \vee \mathcal{B}_i$, если \mathcal{B}_i зависит от \mathcal{B}_1 , т. е. от D_n^* , и равным \mathcal{B}_i в противном случае. Нетрудно проверить, что последовательность $\mathcal{B}_1^*, \mathcal{B}_2^*, \dots, \mathcal{B}_{m-1}^*, \mathcal{B}_m^*$ является выводом из множества дизъюнктов Γ .

Если дизъюнкт \mathcal{B}_m не зависил от \mathcal{B}_1 , то $\mathcal{B}_m^* = []$, и мы получили вывод пустого дизъюнкта из множества дизъюнктов Γ . В противном случае $\mathcal{B}_m^* = L$. Рассмотрим последовательность дизъюнктов

$$\mathcal{B}_1^*, \mathcal{B}_2^*, \dots, \mathcal{B}_{m-1}^*, \mathcal{B}_m^* = L = \mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_{l-1}, \mathcal{A}_l = [].$$

Легко понять, что эта последовательность будет выводом пустого дизъюнкта из множества дизъюнктов Γ (поменялся "статус" формулы \mathcal{A}_1 – в первом выводе обоснованием ее присутствия служило утверждение $\mathcal{A}_1 \in \Gamma_1$, а в полученном выводе она получается из некоторых предшествующих ей формул по правилу резолюций). \square

2.7. Независимость систем аксиом

В этом разделе мы покажем, что *рассмотренная система схем аксиом для Ичисления Высказываний* является в некотором смысле минимальной.

Занумеруем схемы аксиом для исчисления высказываний $\mathcal{A}_1, \dots, \mathcal{A}_{10}$. Обозначим через Δ_i ($i = 1, \dots, 10$) множество всех формул, полученных по всем схемам $\mathcal{A}_1, \dots, \mathcal{A}_{10}$, кроме схемы \mathcal{A}_i .

Определение 2.7.1. *Схема аксиом \mathcal{A}_i зависит от остальных схем $\mathcal{A}_1, \dots, \mathcal{A}_{i-1}, \mathcal{A}_{i+1}, \dots, \mathcal{A}_{10}$, если для любой формулы \mathcal{B} , полученной по схеме \mathcal{A}_i , существует такая конечная последовательность формул $\mathcal{B}_1, \dots, \mathcal{B}_n$, что \mathcal{B}_n есть \mathcal{B} и при любом j ($j = 1, \dots, n$) либо $\mathcal{B}_j \in \Delta_i$, либо существуют числа t и s меньшие j такие, что формула \mathcal{B}_j получается из формул \mathcal{B}_t и \mathcal{B}_s по правилу вывода (правилу отделения) MP . В противном случае схема \mathcal{A}_i не зависит от остальных схем $\mathcal{A}_1, \dots, \mathcal{A}_{i-1}, \mathcal{A}_{i+1}, \dots, \mathcal{A}_{10}$.*

Сделаем некоторые пояснения.

Обозначим через IB_i исчисление высказываний с множеством логических аксиом Δ_i ($i = 1, \dots, 10$) и единственным правилом вывода – **Правилом Отделения MP** . Тогда *независимость схемы аксиом \mathcal{A}_i от остальных схем $\mathcal{A}_1, \dots, \mathcal{A}_{i-1}, \mathcal{A}_{i+1}, \dots, \mathcal{A}_{10}$ означает, что существует формула \mathcal{B} , полученная по схеме \mathcal{A}_i , которая невыводима в исчислении высказываний IB_i .*

Теорема 2.7.1. *При любом i ($i = 1, \dots, 10$) схема аксиом \mathfrak{A}_i не зависит от остальных схем аксиом $\mathfrak{A}_1, \dots, \mathfrak{A}_{i-1}, \mathfrak{A}_{i+1}, \dots, \mathfrak{A}_{10}$.*

Рассмотрим систему

$$\mathcal{M} = \langle \langle M, F, \neg_{\mathcal{M}}, \wedge_{\mathcal{M}}, \vee_{\mathcal{M}}, \rightarrow_{\mathcal{M}} \rangle \rangle,$$

где M – непустое множество, F – его подмножество, $\neg_{\mathcal{M}}$ – одноместная функция на M , а $\wedge_{\mathcal{M}}, \vee_{\mathcal{M}}$ и $\rightarrow_{\mathcal{M}}$ – двуместные функции на M . Систему \mathcal{M} будем называть *пропозициональной системой* или *многозначной логикой*, при этом M называется *множеством истинностных значений*, а F – *множеством выделенных истинностных значений*.

Пусть все пропозициональные переменные формулы \mathcal{A} содержатся в списке A_1, \dots, A_n . Для произвольных элементов a_1, \dots, a_n из множества M индукцией по построению формулы \mathcal{A} определим элемент $\mathcal{A}_{\mathcal{M}}(a_1, \dots, a_n)$ из множества M , который будет называться *значением формулы \mathcal{A}* при значениях $A_1 = a_1, \dots, A_n = a_n$ ее пропозициональных переменных.

Если \mathcal{A} – пропозициональная переменная A_i , то полагаем

$$\mathcal{A}_{\mathcal{M}}(a_1, \dots, a_n) = a_i.$$

Если формула \mathcal{A} имеет одну из форм $\neg(\mathcal{B})$, $(\mathcal{B} \& \mathcal{C})$, $(\mathcal{B} \vee \mathcal{C})$, $(\mathcal{B} \rightarrow \mathcal{C})$, то значение $\mathcal{A}_{\mathcal{M}}(a_1, \dots, a_n)$ определяется соответствующим равенством

$$\begin{aligned} (\neg(\mathcal{B}))_{\mathcal{M}}(a_1, \dots, a_n) &= \neg_{\mathcal{M}}(\mathcal{B}_{\mathcal{M}}(a_1, \dots, a_n)), \\ (\mathcal{B} \& \mathcal{C})_{\mathcal{M}}(a_1, \dots, a_n) &= \mathcal{B}_{\mathcal{M}}(a_1, \dots, a_n) \wedge_{\mathcal{M}} \mathcal{C}_{\mathcal{M}}(a_1, \dots, a_n), \\ (\mathcal{B} \vee \mathcal{C})_{\mathcal{M}}(a_1, \dots, a_n) &= \mathcal{B}_{\mathcal{M}}(a_1, \dots, a_n) \vee_{\mathcal{M}} \mathcal{C}_{\mathcal{M}}(a_1, \dots, a_n), \\ (\mathcal{B} \rightarrow \mathcal{C})_{\mathcal{M}}(a_1, \dots, a_n) &= \mathcal{B}_{\mathcal{M}}(a_1, \dots, a_n) \rightarrow_{\mathcal{M}} \mathcal{C}_{\mathcal{M}}(a_1, \dots, a_n). \end{aligned}$$

Если при любых значениях a_1, \dots, a_n из множества M пропозициональных переменных A_1, \dots, A_n формулы \mathcal{A} она принимает значение $\mathcal{A}_{\mathcal{M}}(a_1, \dots, a_n)$ из F , то формула \mathcal{A} называется *общезначимой* в \mathcal{M} .

Пропозициональную систему \mathcal{M} (многозначную логику) назовем *согласованной* с правилом вывода MP , если из того, что формулы \mathcal{A} и $(\mathcal{A} \rightarrow \mathcal{B})$ принимают значения из F , следует, что и \mathcal{B} принимает значение из F .

Д о к а з а т е л ь с т в о. Для доказательства теоремы мы для каждого i ($i = 1, \dots, 10$) построим пропозициональную систему \mathcal{M}_i (многозначную логику), согласованную с правилом вывода MP , в которой общезначимы все формулы из Δ_i , а значит, общезначимы и все формулы, выводимые в исчислении высказываний $ИВ_i$, но существует формула \mathcal{B} , полученная по схеме \mathfrak{A}_i , которая не является общезначимой в \mathcal{M}_i , а значит, она не выводима в исчислении высказываний $ИВ_i$.

Напомним, что **Логической Аксиомой Исчисления Высказываний** является любая формула каждого из следующих видов, где $\mathcal{A}, \mathcal{B}, \mathcal{C}$ – произвольные формулы

I_→.

I.1. $(\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{A}))$.

I.2. $((\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})) \rightarrow ((\mathcal{A} \rightarrow \mathcal{B}) \rightarrow (\mathcal{A} \rightarrow \mathcal{C})))$.

II_&.

II.1. $((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{A})$.

II.2. $((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{B})$.

II.3. $((\mathcal{C} \rightarrow \mathcal{A}) \rightarrow ((\mathcal{C} \rightarrow \mathcal{B}) \rightarrow (\mathcal{C} \rightarrow (\mathcal{A} \& \mathcal{B}))))$.

III_∨.

III.1. $(\mathcal{A} \rightarrow (\mathcal{A} \vee \mathcal{B}))$.

III.2. $(\mathcal{B} \rightarrow (\mathcal{A} \vee \mathcal{B}))$.

III.3. $((\mathcal{A} \rightarrow \mathcal{C}) \rightarrow ((\mathcal{B} \rightarrow \mathcal{C}) \rightarrow ((\mathcal{A} \vee \mathcal{B}) \rightarrow \mathcal{C})))$.

IV_¬.

IV.1. $((\mathcal{A} \rightarrow (\neg \mathcal{B})) \rightarrow (\mathcal{B} \rightarrow (\neg \mathcal{A})))$.

IV.2. $((\neg(\neg \mathcal{A})) \rightarrow \mathcal{A})$.

Для доказательства независимости аксиомы

$$\text{I.1. } (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{A}))$$

от остальных аксиом рассмотрим логическую матрицу

$$\mathcal{M}_1 = \langle \langle M, F, \neg, \wedge, \vee, \rightarrow \rangle \rangle,$$

где $M = \{0, 1, 2\}$, $F = \{2\}$, $\neg x = 2 - x$, $x \wedge y = \min(x, y)$, $x \vee y = \max(x, y)$ и $x \rightarrow y = 2$ при $x \leq y$ и $x \rightarrow y = 0$ при $x > y$.

Непосредственная проверка показывает, что построенная логическая матрица \mathcal{M}_1 согласована с **Правилом Вывода МР** и в ней общезначимы все частные случаи логических аксиом, кроме получаемых по схеме I.1. Аксиома $(A_1 \rightarrow (A_2 \rightarrow A_1))$ принимает значение 0 при A_1 равном 1, $A_2 - 2$.

Для доказательства независимости аксиомы

$$\text{I.2. } ((\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})) \rightarrow ((\mathcal{A} \rightarrow \mathcal{B}) \rightarrow (\mathcal{A} \rightarrow \mathcal{C})))$$

от остальных аксиом рассмотрим пропозициональную систему

$$\mathcal{M}_2 = \langle \langle M, F, \neg, \wedge, \vee, \rightarrow \rangle \rangle,$$

где $M = \{0, 1, 2\}$, $F = \{0\}$, $\neg x = 2 - x$, $x \wedge y = \max(x, y)$, $x \vee y = \min(x, y)$ и $x \rightarrow y = \max(0, y - x)$.

Непосредственная проверка показывает, что построенная пропозициональная система \mathcal{M}_2 согласована с **Правилом Вывода МР** и в ней общезначимы все частные случаи логических аксиом, кроме получаемых по схеме I.2. Аксиома

$$((A_1 \rightarrow (A_2 \rightarrow A_3)) \rightarrow ((A_1 \rightarrow A_2) \rightarrow (A_1 \rightarrow A_3)))$$

принимает значение 1 при A_1 равном 1, $A_2 = 1$ и $A_3 = 2$.

Для доказательства независимости аксиомы

$$\text{II.1. } ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{A})$$

от остальных аксиом рассмотрим пропозициональную систему

$$\mathcal{M}_3 = \langle \langle M, F, \neg, \wedge, \vee, \rightarrow \rangle \rangle,$$

где $M = \{0, 1\}$, $F = \{1\}$, $x \wedge y = y$, а функции $x \vee y$, $x \rightarrow y$ и $\neg x$ определяются обычным образом.

Непосредственная проверка показывает, что построенная пропозициональная система \mathcal{M}_3 согласована с **Правилом Вывода МР** и в ней общезначимы все частные случаи логических аксиом, кроме получаемых по схеме II.1. Аксиома

$$((A_1 \& A_2) \rightarrow A_1)$$

принимает значение 0 при A_1 равном 0 и $A_2 = 1$.

Для доказательства независимости аксиомы

$$\text{II.2. } ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{B})$$

от остальных аксиом рассмотрим пропозициональную систему

$$\mathcal{M}_4 = \langle \langle M, F, \neg, \wedge, \vee, \rightarrow \rangle \rangle,$$

где $M = \{0, 1\}$, $F = \{1\}$, $x \wedge y = x$, а функции $x \vee y$, $x \rightarrow y$ и $\neg x$ определяются обычным образом.

Непосредственная проверка показывает, что построенная пропозициональная система \mathcal{M}_4 согласована с **Правилом Вывода МР** и в ней общезначимы все частные случаи логических аксиом, кроме получаемых по схеме II.2. Аксиома

$$((A_1 \& A_2) \rightarrow A_2)$$

принимает значение 0 при A_1 равном 1 и $A_2 = 0$.

Для доказательства независимости аксиомы

$$\text{II.3. } ((\mathcal{C} \rightarrow \mathcal{A}) \rightarrow ((\mathcal{C} \rightarrow \mathcal{B}) \rightarrow (\mathcal{C} \rightarrow (\mathcal{A} \& \mathcal{B}))))$$

от остальных аксиом рассмотрим пропозициональную систему

$$\mathcal{M}_5 = \langle \langle M, F, \neg, \wedge, \vee, \rightarrow \rangle \rangle,$$

где $M = \{0, 1\}$, $F = \{1\}$, $x \wedge y = 0$, а функции $x \vee y$, $x \rightarrow y$ и $\neg x$ определяются обычным образом.

Непосредственная проверка показывает, что построенная пропозициональная система \mathcal{M}_5 согласованна с **Правилом Вывода МР** и в ней общезначимы все частные случаи логических аксиом, кроме получаемых по схеме II.3. Аксиома

$$((A_1 \rightarrow A_2) \rightarrow ((A_1 \rightarrow A_3) \rightarrow (A_1 \rightarrow (A_2 \& A_3))))$$

принимает значение 0 при A_1, A_2 и A_3 равных 1.

Для доказательства независимости аксиомы

$$\text{III.1. } (\mathcal{A} \rightarrow (\mathcal{A} \vee \mathcal{B}))$$

от остальных аксиом рассмотрим пропозициональную систему

$$\mathcal{M}_6 = \langle \langle M, F, \neg, \wedge, \vee, \rightarrow \rangle \rangle,$$

где $M = \{0, 1\}$, $F = \{1\}$, $x \vee y = y$, а функции $x \wedge y$, $x \rightarrow y$ и $\neg x$ определяются обычным образом.

Непосредственная проверка показывает, что построенная пропозициональная система \mathcal{M}_6 согласована с **Правилом Вывода МР** и в ней общезначимы все частные случаи логических аксиом, кроме получаемых по схеме III.1. Аксиома

$$(A_1 \rightarrow (A_1 \vee A_2))$$

принимает значение 0 при A_1 равном 1 и $A_2 = 0$.

Для доказательства независимости аксиомы

$$\text{III.2. } (\mathcal{B} \rightarrow (\mathcal{A} \vee \mathcal{B}))$$

от остальных аксиом рассмотрим пропозициональную систему

$$\mathcal{M}_7 = \langle \langle M, F, \neg, \wedge, \vee, \rightarrow \rangle \rangle,$$

где $M = \{0, 1\}$, $F = \{1\}$, $x \vee y = x$, а функции $x \wedge y$, $x \rightarrow y$ и $\neg x$ определяются обычным образом.

Непосредственная проверка показывает, что построенная пропозициональная система \mathcal{M}_7 согласована с **Правилом Вывода МР** и в ней общезначимы все частные случаи логических аксиом, кроме получаемых по схеме III.2. Аксиома

$$(A_2 \rightarrow (A_1 \vee A_2))$$

принимает значение 0 при A_1 равном 0 и $A_2 = 1$.

Для доказательства независимости аксиомы

$$\text{III.3. } ((\mathcal{A} \rightarrow \mathcal{C}) \rightarrow ((\mathcal{B} \rightarrow \mathcal{C}) \rightarrow ((\mathcal{A} \vee \mathcal{B}) \rightarrow \mathcal{C})))$$

от остальных аксиом рассмотрим пропозициональную систему

$$\mathcal{M}_8 = \langle \langle M, F, \neg, \wedge, \vee, \rightarrow \rangle \rangle,$$

где $M = \{0, 1\}$, $F = \{1\}$, $x \vee y = 1$, а функции $x \wedge y$, $x \rightarrow y$ и $\neg x$ определяются обычным образом.

Непосредственная проверка показывает, что построенная пропозициональная система \mathcal{M}_8 согласована с **Правилом Вывода МР** и в ней общезначимы все частные случаи логических аксиом, кроме получаемых по схеме III.3. Аксиома

$$((A_1 \rightarrow A_3) \rightarrow ((A_2 \rightarrow A_3) \rightarrow ((A_1 \vee A_2) \rightarrow A_3)))$$

принимает значение 0 при A_1 , A_2 и A_3 равных 0.

Для доказательства независимости аксиомы

$$\text{IV.1. } ((\mathcal{A} \rightarrow (\neg \mathcal{B})) \rightarrow (\mathcal{B} \rightarrow (\neg \mathcal{A})))$$

от остальных аксиом рассмотрим пропозициональную систему

$$\mathcal{M}_9 = \langle \langle M, F, \neg, \wedge, \vee, \rightarrow \rangle \rangle,$$

где $M = \{0, 1\}$, $F = \{1\}$, $\neg x = 0$, а функции $x \wedge y$, $x \rightarrow y$ и $x \vee y$ определяются обычным образом.

Непосредственная проверка показывает, что построенная пропозициональная система \mathcal{M}_9 согласована с **Правилом Вывода МР** и в ней общезначимы все частные случаи логических аксиом, кроме получаемых по схеме IV.1. Аксиома

$$((A_1 \rightarrow (\neg A_2)) \rightarrow (A_2 \rightarrow (\neg A_1)))$$

принимает значение 0 при A_1 равном 0 и A_2 равном 1.

Для доказательства независимости аксиомы

$$\text{IV.2. } ((\neg(\neg \mathcal{A})) \rightarrow \mathcal{A})$$

от остальных аксиом рассмотрим пропозициональную систему

$$\mathcal{M}_{10} = \langle \langle M, F, \neg, \wedge, \vee, \rightarrow \rangle \rangle,$$

где $M = \{0, 1, 2\}$, $F = \{2\}$, $x \wedge y = \min(x, y)$, $x \vee y = \max(x, y)$ и $x \rightarrow y = 2$ при $x \leq y$ и $x \rightarrow y = y$ при $x > y$, $\neg 0 = 2$ и $\neg x = 0$ при $x > 0$.

Непосредственная проверка показывает, что построенная пропозициональная система \mathcal{M}_{10} согласована с **Правилом Вывода МР** и в ней общезначимы все частные случаи логических аксиом, кроме получаемых по схеме IV.2. Аксиома $((\neg(\neg A_1)) \rightarrow A_1)$ принимает значение 1 при A_1 равном 1.

Интересно заметить, что казалось бы "самая простая" аксиома IV.2 потребовала построения "самой сложной" пропозициональной системы. Оказывается

это не случайно! "Простота" аксиомы IV.2 кажущаяся. Существует целое математическое направление, называемое *интуиционизмом*, представители которого, в частности, не принимают эту аксиому. В настоящем пособии не представляется возможным дать сколько-нибудь подробное представление об этом важном направлении математических исследований. \square

2.8. Исчисление Секвенций

Для углубленного изучения двух основных понятий **Исчисления Высказываний** – понятия **вывода** и понятия **выводимой формулы** – мы ввели два более общих понятия – понятие **вывода из множества формул** Γ и понятие **формулы, выводимой из множества формул** Γ и достаточно подробно изучили свойства отношения $\Gamma \vdash A$.

В настоящем разделе мы рассмотрим несколько другой подход к изучению **Логике Высказываний** – **Исчисление Секвенций**.

Алфавит $\Sigma_{ИС}$ – это объединение четырех множеств Σ_1 , Σ_2 , Σ_3 и Σ_4 .

$\Sigma_1 = \{A_1, A_2, \dots, A_n, \dots\}$ – счетное множество пропозициональных переменных,

$\Sigma_2 = \{\neg, \&, \vee, \rightarrow\}$ – множество пропозициональных связок,

$\Sigma_3 = \{(,), , \}$ – множество технических символов – "левая скобка", "правая скобка", "запятая",

$\Sigma_4 = \{\vdash\}$.

Понятие **формула Исчисления Секвенций** определяется в точности также, как и понятие **формула Исчисления Высказываний**.

Секвенцией называется выражение одного из трех видов, где A_1, A_2, \dots, A_n, B – произвольные формулы **Исчисления Секвенций**:

- 1) $A_1, A_2, \dots, A_n \vdash B$ (читается "из A_1, A_2, \dots, A_n следует B "),
- 2) $\vdash B$ (читается " B доказуема"),
- 3) $A_1, A_2, \dots, A_n \vdash$ (читается "система A_1, A_2, \dots, A_n противоречива").

Правилем вывода Исчисления Секвенций называется выражение вида

$$\frac{S_1, S_2, \dots, S_n}{S},$$

где S_1, S_2, \dots, S_n, S – секвенции. Секвенция S называется **непосредственным следствием секвенций** S_1, S_2, \dots, S_n по данному правилу вывода.

Как и в случае **Исчисления Высказываний**, определим понятия **аксиомы и правила вывода Исчисления Секвенций**.

Аксиомы Исчисления Секвенций задаются одной схемой аксиом: $A \vdash A$.

Аксиома Исчисления Секвенций получается из указанной схемы аксиом подстановкой вместо A произвольной формулы \mathcal{F} **Исчисления Секвенций**.

Пусть \mathcal{A} , \mathcal{B} и \mathcal{C} – произвольные формулы **Исчисления Секвенций**, а Γ_1 , Γ_2 , Γ_3 и Γ – произвольные конечные последовательности (возможно, пустые) формул **Исчисления Секвенций**.

Правила вывода Исчисления Секвенций – это выражения одного из следующих видов:

1) *Введение $\&$*

$$\frac{\Gamma_1 \vdash \mathcal{A}; \Gamma_2 \vdash \mathcal{B}}{\Gamma_1, \Gamma_2 \vdash (\mathcal{A} \& \mathcal{B})};$$

2) *Удаление $\&$*

$$\frac{\Gamma \vdash (\mathcal{A} \& \mathcal{B})}{\Gamma \vdash \mathcal{A}};$$

3) *Удаление $\&$*

$$\frac{\Gamma \vdash (\mathcal{A} \& \mathcal{B})}{\Gamma \vdash \mathcal{B}};$$

4) *Введение \vee*

$$\frac{\Gamma \vdash \mathcal{A}}{\Gamma \vdash (\mathcal{A} \vee \mathcal{B})};$$

5) *Введение \vee*

$$\frac{\Gamma \vdash \mathcal{B}}{\Gamma \vdash (\mathcal{A} \vee \mathcal{B})};$$

6) *Удаление \vee*

$$\frac{\Gamma_1 \vdash (\mathcal{A} \vee \mathcal{B}); \Gamma_2, \mathcal{A} \vdash \mathcal{C}; \Gamma_3, \mathcal{B} \vdash \mathcal{C}}{\Gamma_1, \Gamma_2, \Gamma_3 \vdash \mathcal{C}};$$

7) *Введение \rightarrow*

$$\frac{\Gamma, \mathcal{A} \vdash \mathcal{B}}{\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B})};$$

8) *Удаление \rightarrow*

$$\frac{\Gamma_1 \vdash (\mathcal{A} \rightarrow \mathcal{B}), \Gamma_2 \vdash \mathcal{A}}{\Gamma_1, \Gamma_2 \vdash \mathcal{B}};$$

9) *Введение \neg*

$$\frac{\Gamma, \mathcal{A} \vdash}{\Gamma \vdash \neg(\mathcal{A})};$$

10) *Сведение к противоречию*

$$\frac{\Gamma_1 \vdash \mathcal{A}, \Gamma_2 \vdash \neg(\mathcal{A})}{\Gamma_1, \Gamma_2 \vdash};$$

11) *Удаление \neg*

$$\frac{\Gamma, \neg(\mathcal{A}) \vdash}{\Gamma \vdash \mathcal{A}};$$

12) Уточнение

$$\frac{\Gamma \vdash}{\Gamma \vdash \mathcal{A}};$$

13) Расширение

$$\frac{\Gamma \vdash \mathcal{A}}{\Gamma, \mathcal{B} \vdash \mathcal{A}};$$

14) Перестановка

$$\frac{\Gamma_1, \mathcal{A}, \mathcal{B}, \Gamma_2 \vdash \mathcal{C}}{\Gamma_1, \mathcal{B}, \mathcal{A}, \Gamma_2 \vdash \mathcal{C}};$$

15) Сокращение

$$\frac{\Gamma_1, \mathcal{A}, \mathcal{A}, \Gamma_2 \vdash \mathcal{B}}{\Gamma_1, \mathcal{A}, \Gamma_2 \vdash \mathcal{B}}.$$

Выводом в Исчислении Секвенций называется любая конечная последовательность S_1, S_2, \dots, S_n секвенций такая, что для любого i ($1 \leq i \leq n$) либо S_i – аксиома, либо S_i непосредственное следствие некоторых предыдущих секвенций по одному из правил вывода 1 - 15.

Секвенция S называется **выводимой** в **Исчислении Секвенций**, если существует вывод в **Исчислении Секвенций**, оканчивающийся секвенцией S .

Теорема 2.8.1. 1) Если выводима секвенция $\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_n \vdash \mathcal{B}$, то формула $((\mathcal{A}_1 \& \mathcal{A}_2 \& \dots \& \mathcal{A}_n) \rightarrow \mathcal{B})$ тождественно истинна.

2) Если выводима секвенция $\vdash \mathcal{B}$, то формула \mathcal{B} тождественно истинна.

3) Если выводима секвенция $\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_n \vdash$, то формула

$$\neg(\mathcal{A}_1 \& \mathcal{A}_2 \& \dots \& \mathcal{A}_n)$$

тождественно истинна.

Доказательство. Доказательство проводится индукцией по длине вывода и предоставляется читателю в качестве полезного упражнения. \square

Для **Исчисления Секвенций** справедлива следующая теорема о полноте, аналогичная соответствующей теореме для **Исчисления Высказываний**.

Теорема 2.8.2. Секвенция $\vdash \mathcal{A}$ выводима в **Исчислении Секвенций** тогда и только тогда, когда формула \mathcal{A} тождественно истинна.

Доказательство. Если формула \mathcal{A} тождественно истинна, то она выводима в **Исчислении Высказываний**. Индукцией по длине вывода формулы \mathcal{A} в **Исчислении Высказываний** покажем, что секвенция $\vdash \mathcal{A}$ выводима в **Исчислении Секвенций**.

Прежде всего покажем, что если формула \mathcal{A} является логической аксиомой **Исчисления Высказываний**, то секвенция $\vdash \mathcal{A}$ выводима в **Исчислении Секвенций**.

Напомним, что аксиомами **Исчисления Высказываний** служат формулы следующего вида

I_{\rightarrow} .

- I.1. $(\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{A}))$.
- I.2. $((\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})) \rightarrow ((\mathcal{A} \rightarrow \mathcal{B}) \rightarrow (\mathcal{A} \rightarrow \mathcal{C})))$.

$II_{\&}$.

- II.1. $((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{A})$.
- II.2. $((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{B})$.
- II.3. $((\mathcal{C} \rightarrow \mathcal{A}) \rightarrow ((\mathcal{C} \rightarrow \mathcal{B}) \rightarrow (\mathcal{C} \rightarrow (\mathcal{A} \& \mathcal{B}))))$.

III_{\vee} .

- III.1. $(\mathcal{A} \rightarrow (\mathcal{A} \vee \mathcal{B}))$.
- III.2. $(\mathcal{B} \rightarrow (\mathcal{A} \vee \mathcal{B}))$.
- III.3. $((\mathcal{A} \rightarrow \mathcal{C}) \rightarrow ((\mathcal{B} \rightarrow \mathcal{C}) \rightarrow ((\mathcal{A} \vee \mathcal{B}) \rightarrow \mathcal{C})))$.

IV_{\neg} .

- IV.1. $((\mathcal{A} \rightarrow (\neg \mathcal{B})) \rightarrow (\mathcal{B} \rightarrow (\neg \mathcal{A})))$.
- IV.2. $((\neg(\neg \mathcal{A})) \rightarrow \mathcal{A})$.

Установим выводимость соответствующих секвенций в **Исчислении Секвенций**.

I_{\rightarrow} .

- I.1. $\vdash (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{A}))$.
- $\mathcal{A} \vdash \mathcal{A}$ (логическая аксиома),
- $\mathcal{A}, \mathcal{B} \vdash \mathcal{A}$ (правило расширения 13),
- $\mathcal{A} \vdash (\mathcal{B} \rightarrow \mathcal{A})$ (правило введения \rightarrow 7),
- $\vdash (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{A}))$ (правило введения \rightarrow 7).

Используя аксиому и правила расширения 13 и перестановки 14, легко показать, что если $\mathcal{A} \in \Gamma$, то выводима секвенция $\Gamma \vdash \mathcal{A}$. Этим простым фактом мы будем часто пользоваться в дальнейшем.

- I.2. $\vdash ((\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})) \rightarrow ((\mathcal{A} \rightarrow \mathcal{B}) \rightarrow (\mathcal{A} \rightarrow \mathcal{C})))$.

Введем обозначение

$$\Gamma = \{((\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})), ((\mathcal{A} \rightarrow \mathcal{B}), \mathcal{A})\}.$$

Тогда

- $\Gamma \vdash (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C}));$
- $\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B});$
- $\Gamma \vdash \mathcal{A};$
- $\Gamma \vdash \mathcal{B};$
- $\Gamma \vdash (\mathcal{B} \rightarrow \mathcal{C});$
- $\Gamma \vdash \mathcal{C}.$

Применив три раза правило введения \rightarrow , получим выводимость нужной секвенции.

$II_{\&}$.

- II.1. $\vdash ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{A})$.
- $(\mathcal{A} \& \mathcal{B}) \vdash (\mathcal{A} \& \mathcal{B});$

$(\mathcal{A} \& \mathcal{B}) \vdash \mathcal{A};$

$\vdash ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{A});$

II.2. $\vdash ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{B}).$

$(\mathcal{A} \& \mathcal{B}) \vdash (\mathcal{A} \& \mathcal{B});$

$(\mathcal{A} \& \mathcal{B}) \vdash \mathcal{B};$

$\vdash ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{B});$

II.3. $\vdash ((\mathcal{A} \rightarrow \mathcal{B}) \rightarrow ((\mathcal{A} \rightarrow \mathcal{C}) \rightarrow (\mathcal{A} \rightarrow (\mathcal{B} \& \mathcal{C}))))).$

Введем обозначение

$\Gamma = \{(\mathcal{A} \rightarrow \mathcal{B}), (\mathcal{A} \rightarrow \mathcal{C}), \mathcal{A}\}.$

Тогда

$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B});$

$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{C});$

$\Gamma \vdash \mathcal{A};$

$\Gamma \vdash \mathcal{B};$

$\Gamma \vdash \mathcal{C};$

$\Gamma \vdash (\mathcal{B} \& \mathcal{C}).$

Применив три раза *правило введения* \rightarrow , получим выводимость нужной секвенции.

III _{\vee} .

III.1. $\vdash (\mathcal{A} \rightarrow (\mathcal{A} \vee \mathcal{B})).$

$\mathcal{A} \vdash \mathcal{A};$

$\mathcal{A} \vdash (\mathcal{A} \vee \mathcal{B});$

$\vdash (\mathcal{A} \rightarrow (\mathcal{A} \vee \mathcal{B})).$

III.2. $\vdash (\mathcal{B} \rightarrow (\mathcal{A} \vee \mathcal{B})).$

$\mathcal{B} \vdash \mathcal{B};$

$\mathcal{B} \vdash (\mathcal{A} \vee \mathcal{B});$

$\vdash (\mathcal{B} \rightarrow (\mathcal{A} \vee \mathcal{B})).$

III.3. $\vdash ((\mathcal{A} \rightarrow \mathcal{C}) \rightarrow ((\mathcal{B} \rightarrow \mathcal{C}) \rightarrow ((\mathcal{A} \vee \mathcal{B}) \rightarrow \mathcal{C}))).$

Введем обозначение

$\Gamma = \{(\mathcal{A} \rightarrow \mathcal{C}), (\mathcal{B} \rightarrow \mathcal{C}), (\mathcal{A} \vee \mathcal{B})\}.$

Тогда

$\Gamma, \mathcal{A} \vdash \mathcal{C};$

$\Gamma, \mathcal{B} \vdash \mathcal{C};$

$\Gamma \vdash (\mathcal{A} \vee \mathcal{B});$

$\Gamma \vdash \mathcal{C}.$

Применив три раза *правило введения* \rightarrow , получим выводимость нужной секвенции.

IV _{\neg} .

IV.1. $\vdash ((\mathcal{A} \rightarrow (\neg \mathcal{B})) \rightarrow (\mathcal{B} \rightarrow (\neg \mathcal{A}))).$

Введем обозначение

$\Gamma = \{\mathcal{B}, (\mathcal{A} \rightarrow (\neg \mathcal{B}))\}.$

Тогда

$\Gamma \vdash \mathcal{B}$;

$\Gamma, \mathcal{A} \vdash (\neg \mathcal{B})$.

Поэтому $\Gamma, \mathcal{A} \vdash$.

По правилу 9 *введение* \neg получаем $\Gamma \vdash (\neg \mathcal{A})$.

Применив два раза *правило введения* \rightarrow , получим выводимость нужной секвенции.

IV.2. $\vdash ((\neg(\neg \mathcal{A})) \rightarrow \mathcal{A})$.

Введем обозначение

$\Gamma = \{(\neg(\neg \mathcal{A})), (\neg \mathcal{A})\}$.

Тогда

$\Gamma \vdash (\neg(\neg \mathcal{A}))$;

$\Gamma \vdash (\neg \mathcal{A})$.

По правилу 10 получаем

$\Gamma \vdash$,

т. е.

$(\neg(\neg \mathcal{A})), (\neg \mathcal{A}) \vdash$.

По правилу 11 *удаление* \neg получаем

$(\neg(\neg \mathcal{A})) \vdash \mathcal{A}$.

По правилу 7 *введение* \rightarrow получаем

$\vdash ((\neg(\neg \mathcal{A})) \rightarrow \mathcal{A})$.

Если формула \mathcal{B} получена из формул \mathcal{A} и $(\mathcal{A} \rightarrow \mathcal{B})$ по **Правилу Отделения МР**, причем доказуемы секвенции $\vdash \mathcal{A}$ и $\vdash (\mathcal{A} \rightarrow \mathcal{B})$, то, применив правило 8 *удаление* \rightarrow , получим доказуемость секвенции $\vdash \mathcal{B}$. \square

2.9. Другие аксиоматизации для логики высказываний

В этом разделе мы рассмотрим некоторые другие подходы к аксиоматизации логики высказываний. Так как одни пропозициональные связки относительно логики высказываний могут быть выражены через некоторые другие, то имеется возможность включать в алфавит исчисления высказываний лишь часть связок из $\neg, \vee, \&, \rightarrow$.

Рассмотрим несколько теорий, близких к **Исчислению Высказываний**. Алфавиты этих теорий будут отличаться от алфавита **Исчисления Высказываний** лишь набором пропозициональных связок.

Теория L_1 . В алфавит теории L_1 в качестве пропозициональных связок включаются лишь \neg и \vee . Понятие формулы в теории L_1 вводится по той же схеме, что и в случае **Исчисления Высказываний**.

Выражение $(\mathcal{A} \& \mathcal{B})$ *служит сокращением* для формулы

$$(\neg((\neg \mathcal{A}) \vee (\neg \mathcal{B}))),$$

а $(\mathcal{A} \rightarrow \mathcal{B})$ – для формулы

$$((\neg \mathcal{A}) \vee \mathcal{B}).$$

Система логических аксиом теории L_1 определяется четырьмя схемами аксиом.

1. $((\mathcal{A} \vee \mathcal{A}) \rightarrow \mathcal{A})$.
2. $(\mathcal{A} \rightarrow (\mathcal{A} \vee \mathcal{B}))$.
3. $((\mathcal{A} \vee \mathcal{B}) \rightarrow (\mathcal{B} \vee \mathcal{A}))$.
4. $((\mathcal{B} \rightarrow \mathcal{C}) \rightarrow ((\mathcal{A} \vee \mathcal{B}) \rightarrow (\mathcal{A} \vee \mathcal{C})))$.

В теории L_1 , как и в **Исчислении Высказываний**, только одно правило вывода – **Правило Отделения МР (Modus Ponens)**:

$$\frac{\mathcal{A}, (\mathcal{A} \rightarrow \mathcal{B})}{\mathcal{B}}.$$

Как и в случае **Исчисления Высказываний**, определяются понятия **вывод**, **выводимая формула**, **вывод из множества гипотез**, доказываются теорема дедукции и ряд вспомогательных теорем. Это позволяет доказать, как и в случае **Исчисления Высказываний**, основную теорему о теории L_1 .

Теорема 2.9.1. *Формула \mathcal{A} теории L_1 выводима в этой теории тогда и только тогда, когда она тождественно истинна.*

Теория L_2 . В алфавит теории L_2 в качестве пропозициональных связок включаются лишь \neg и $\&$. Понятие формулы в теории L_2 вводится по той же схеме, что и в случае **Исчисления Высказываний**.

Выражение $(\mathcal{A} \vee \mathcal{B})$ служит сокращением для формулы

$$(\neg((\neg \mathcal{A}) \& (\neg \mathcal{B}))),$$

а $(\mathcal{A} \rightarrow \mathcal{B})$ – для формулы

$$(\neg(\mathcal{A} \& (\neg \mathcal{B}))).$$

Система логических аксиом теории L_2 определяется тремя схемами аксиом.

1. $(\mathcal{A} \rightarrow (\mathcal{A} \& \mathcal{A}))$.
2. $((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{A})$.
3. $((\mathcal{A} \rightarrow \mathcal{B}) \rightarrow (\neg(\mathcal{B} \& \mathcal{C}) \rightarrow \neg(\mathcal{C} \& \mathcal{A})))$.

В теории L_2 , как и в **Исчислении Высказываний**, только одно правило вывода – **Правило Отделения МР (Modus Ponens)**:

$$\frac{\mathcal{A}, (\mathcal{A} \rightarrow \mathcal{B})}{\mathcal{B}}.$$

Как и в случае **Исчисления Высказываний**, определяются понятия **вывод**, **выводимая формула**, **вывод из множества гипотез**, доказываются теорема дедукции и ряд вспомогательных теорем. Это позволяет доказать, как и в случае **Исчисления Высказываний**, основную теорему о теории L_2 .

Теорема 2.9.2. *Формула \mathcal{A} теории L_2 выводима в этой теории тогда и только тогда, когда она тождественно истинна.*

Теория L_3 . В алфавит теории L_3 в качестве пропозициональных связок включаются лишь \neg и \rightarrow . Понятие формулы в теории L_3 вводится по той же схеме, что и в случае **Исчисления Высказываний**.

Выражение $(\mathcal{A} \vee \mathcal{B})$ служит сокращением для формулы

$$((\neg \mathcal{A}) \rightarrow \mathcal{B}),$$

а $(\mathcal{A} \& \mathcal{B})$ – для формулы

$$(\neg(\mathcal{A} \rightarrow (\neg \mathcal{B}))).$$

Система логических аксиом теории L_3 определяется тремя схемами аксиом.

1. $(\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{A}))$.
2. $((\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})) \rightarrow ((\mathcal{A} \rightarrow \mathcal{B}) \rightarrow (\mathcal{A} \rightarrow \mathcal{C})))$.
3. $((\neg \mathcal{B}) \rightarrow (\neg \mathcal{A})) \rightarrow ((\neg \mathcal{B}) \rightarrow \mathcal{A} \rightarrow \mathcal{B}))$.

В теории L_3 , как и в **Исчислении Высказываний**, только одно правило вывода – **Правило Отделения МР (Modus Ponens)**:

$$\frac{\mathcal{A}, (\mathcal{A} \rightarrow \mathcal{B})}{\mathcal{B}}.$$

Как и в случае **Исчисления Высказываний**, определяются понятия **вывод**, **выводимая формула**, **вывод из множества гипотез**, доказываются теорема дедукции и ряд вспомогательных теорем. Это позволяет доказать, как и в случае **Исчисления Высказываний**, основную теорему о теории L_3 .

Теорема 2.9.3. *Формула \mathcal{A} теории L_3 выводима в этой теории тогда и только тогда, когда она тождественно истинна.*

Рассмотренные теории L_1 , L_2 и L_3 можно несколько модифицировать, заменив схемы аксиом конкретными аксиомами, но добавив при этом к **Правилу Вывода МР Правило Подстановки**:

если все пропозициональные переменные формулы \mathcal{F} содержатся среди A_1, A_2, \dots, A_n , а $\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_n$ – произвольные формулы, то

$$\frac{\mathcal{F}}{\mathcal{F}_{A_1, A_2, \dots, A_n}[\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_n]}$$

Получим теории L_1^* , L_2^* и L_3^* с системами аксиом

Теория L_1^* . Система логических аксиом теории L_1^* состоит из четырех аксиом.

1. $((A_1 \vee A_1) \rightarrow A_1)$.
2. $(A_1 \rightarrow (A_1 \vee A_2))$.

3. $((A_1 \vee A_2) \rightarrow (A_2 \vee A_1))$.
4. $((A_2 \rightarrow A_3) \rightarrow ((A_1 \vee A_2) \rightarrow (A_1 \vee A_3)))$.

В теории L_1^* два правила вывода – **Правило Отделения МР** (*Modus Ponens*) и **Правило Подстановки**. Естественным образом определяются понятия **вывод**, **выводимая формула**, **вывод из множества гипотез**, доказываются теорема дедукции и ряд вспомогательных теорем. Это позволяет доказать, как и в случае **Исчисления Высказываний**, основную теорему о теории L_1^* .

Теорема 2.9.4. *Формула A теории L_1^* выводима в этой теории тогда и только тогда, когда она тождественно истинна.*

Теория L_2^* . Система логических аксиом теории L_2 состоит из трех аксиом.

1. $(A_1 \rightarrow (A_1 \& A_1))$.
2. $((A_1 \& A_2) \rightarrow A_1)$.
3. $((A_1 \rightarrow A_2) \rightarrow (\neg(A_2 \& A_3) \rightarrow \neg(A_3 \& A_1)))$.

В теории L_2^* два правила вывода – **Правило Отделения МР** (*Modus Ponens*) и **Правило Подстановки**. Естественным образом определяются понятия **вывод**, **выводимая формула**, **вывод из множества гипотез**, доказываются теорема дедукции и ряд вспомогательных теорем. Это позволяет доказать, как и в случае **Исчисления Высказываний**, основную теорему о теории L_2^* .

Теорема 2.9.5. *Формула A теории L_2^* выводима в этой теории тогда и только тогда, когда она тождественно истинна.*

Теория L_3^* . Система логических аксиом теории L_3^* состоит из трех аксиом.

1. $(A_1 \rightarrow (A_2 \rightarrow A_1))$.
2. $((A_1 \rightarrow (A_2 \rightarrow A_3)) \rightarrow ((A_1 \rightarrow A_2) \rightarrow (A_1 \rightarrow A_3)))$.
3. $((\neg A_2) \rightarrow (\neg A_1)) \rightarrow ((\neg A_2) \rightarrow A_1) \rightarrow A_2$.

В теории L_3^* два правила вывода – **Правило Отделения МР** (*Modus Ponens*) и **Правило Подстановки**. Естественным образом определяются понятия **вывод**, **выводимая формула**, **вывод из множества гипотез**, доказываются теорема дедукции и ряд вспомогательных теорем. Это позволяет доказать, как и в случае **Исчисления Высказываний**, основную теорему о теории L_3^* .

Теорема 2.9.6. *Формула A теории L_3^* выводима в этой теории тогда и только тогда, когда она тождественно истинна.*

Рассмотренные подходы к аксиоматизации *Логике Высказываний* представляются достаточно естественными. Существуют и несколько "менее естественные" подходы. Например, предложены системы аксиом, состоящие либо из одной схемы аксиом, либо из одной аксиомы, но "смысл" этой аксиомы не столь прозрачен, как в рассмотренных случаях.

2.10. Интуиционистское исчисление высказываний

При написании этого параграфа мы использовали, в частности, материал из восьмого параграфа пособия В. Е. Плиско "Математическая логика" [31].

В конце XIX – начале XX в. в математике и прежде всего в теории множеств был обнаружен ряд так называемых парадоксов, что принято рассматривать как начало III *кризиса оснований математики*. В ходе попыток найти выход из создавшейся достаточно сложной ситуации выяснилось, что существуют принципиально разные точки зрения как на истоки и причины кризиса, так и на возможные пути выхода из него. Это привело к формированию разных научных школ в области оснований математики. Более подробно об этом говорится в конце пособия. Здесь же мы кратко обсудим некоторые побудительные мотивы введения важного варианта *Исчисления Высказываний – Интуиционистского Исчисления Высказываний*.

Математический интуиционизм – одно из основных направлений исследований в области оснований математики. Основной постулат интуиционизма – "интуиция – единственный источник математики и главный критерий строгости ее построений". Интуиционистская идеология восходит к античной математике, ее основные положения в той или иной мере разделялись такими выдающимися математиками, как К.Ф. Гаусс, Л. Кронекер, А. Пуанкаре, А. Лебег, Э. Борель, Г. Вейль. В 1880-х годах Л. Кронекер утверждал, что процветавшие тогда методы К. Вейерштрасса, Р. Дедекинда и Г. Кантора ненадежны, что используемые ими фундаментальные понятия – просто слова, так как они не дают возможность проверить, удовлетворяет ли рассматриваемый объект определению.

Но основным идеологом интуиционизма по праву считается Л. Э. Я. Брауэр, который в начале XX века выступил с развернутой критикой основных положений классической математики и радикальной интуиционистской программой перестройки математического здания.

Лейтзен Эгберт Ян Брауэр (27.2.1881, Оверси – 2.12.1966, Амстердам), голландский математик, с 1908 года последовательно проводил критику так называемых чистых доказательств существования, опирающихся на закон исключенного третьего, что в итоге положило начало особому направлению в области оснований математики – *математическому интуиционизму*. Особую ценность имеет проведенный Л. Э. Я. Брауэром анализ математических доказательств существования объектов с точки зрения возможности построе-

ния соответствующих объектов.

В статье "Недостоверность логических принципов", опубликованной в 1908 году, Л. Э. Я. Брауэр поставил под сомнение абсолютную веру в правила классической логики, которые оставались неизменными со времен Аристотеля (384-322 гг. до н. э.). Г. Вейль так излагал точку зрения Л. Э. Я. Брауэра *"Согласно его взглядам и пониманию истории, классическая логика была абстрагирована от математики конечных множеств и их подмножеств... Забывая об этом ограниченном происхождении, впоследствии эту логику приняли ошибочно за нечто высшее и первичное по отношению ко всей математике и в конце концов стали применять ее без какого-либо оправдания к математике бесконечных множеств"*. Можно привести простые примеры утверждений, истинных для конечных множеств натуральных чисел, но ложные для бесконечных. Формирование интуиционистской идеологии шло в достаточно острой полемике с возглавляемым Д. Гильбертом еще одним из основных направлений исследований в области оснований математики – **математическим формализмом**. Л. Э. Я. Брауэр не принимал теоретико-множественные основания математики, веру в актуальный характер бесконечных множеств, правомерность переноса в область бесконечного логических принципов, выработанных при работе с конечными множествами. В частности, им отвергался **закон исключенного третьего**. С точки зрения интуиционистов, предметом исследования в математике являются *умственные построения*, которые рассматриваются "безотносительно к таким вопросам о природе конструируемых объектов, как вопрос, существуют ли это объекты независимо от нашего знания о них" (А. Гейтинг). Математические утверждения, по мнению интуиционистов, дают некоторую информацию о выполненных построениях. Классическая и интуиционистская математики придерживаются существенно разных точек зрения на бесконечные множества. Классическая математика рассматривает бесконечность как *актуальную, экзистенциальную или завершенную*. Бесконечные множества рассматриваются как завершенные объекты, с которыми можно выполнять дальнейшие построения, в частности, они могут быть элементами других множеств. Интуиционистская математика рассматривает бесконечность как *потенциальную или становящуюся*. Эта точка зрения на бесконечность восходит к Г. Ф. Гауссу, который утверждал *"Я возражаю... против употребления бесконечной величины, как чего-либо завершенного, что никогда не позволительно в математике"*. Г. Вейль считал, что "Брауэр выяснил и, как мне кажется, не оставил сомнения в том, что не существует доводов, защищающих веру в экзистенциальный характер совокупности всех натуральных чисел... Этот ряд чисел, который растет, не останавливаясь ни на какой стадии, за счет перехода к следующему числу, представляет собой многообразие возможностей, открытых для бесконечности; он вечно остается в состоянии становления, а не является замкнутым царством вещей, существующих в себе. То, что мы слепо превращаем одно в другое, является истинным источником наших трудностей, в том числе антиномий, – источником более глубокой природы, чем указанный Расселом принцип порочного круга. Брауэр открыл нам

глаза и показал, как далеко классическая математика, вскормленная превосходящей всякую человеческую способность реализации верой в "абсолютное", идет дальше таких утверждений, которые могут претендовать на реальный смысл и истинность, основанную на доказательствах".

Интуиционистская и классическая математики несколько по-разному понимают (трактуют) логические связки. Например, с точки зрения интуиционистской математики доказательство утверждения "*существует объект a , обладающий свойством A* ", должно давать *метод (алгоритм) построения конкретного объекта a , обладающего свойством A* . Однако в классической математике достаточно широко распространены косвенные доказательства существования, в которых из предположения $(\forall x)(\neg A)$ выводится противоречие, на основании чего делается вывод, что $\neg(\forall x)(\neg A)$, а затем получают, что $(\exists x)A$. Нередко из такого доказательства не видно, как построить конкретный объект a , обладающий свойством A . Ярким примером может служить традиционное доказательство методом от противного частного случая теоремы Л. Э. Я. Брауэра о неподвижной точке "*Любое непрерывное отображение единичного круга D в себя имеет неподвижную точку*", которое приводится в конце пособия. Подобное *чистое доказательство существования* не принимается интуиционистской математикой.

Существует специфика и в понимании интуиционистами логической связки дизъюнкции \vee – их понимание дизъюнкции $A \vee B$ отличается от классического, но об этом будет сказано позже.

Л. Э. Я. Брауэр и его единомышленники в серии работ начиная с 1918 года выполнили построение основных разделов интуиционистской математики – теории множеств, геометрии, топологии, математического анализа. В теории чисел неинтуиционистские методы не играют существенной роли, так как во многих случаях неконструктивные доказательства существования можно заменить конструктивными, хотя, как правило, существенно более длинными. В то же время в математическом анализе неинтуиционистские методы играют очень важную роль, начиная с построения действительных чисел, которые трактуются как бесконечные множества рациональных чисел. Т. е. уже на начальном этапе используется актуальная бесконечность. **Закон исключенного третьего** также играет существенную роль при определении отношения порядка для действительных чисел. К концу XX века интуиционистская математика была уже достаточно глубоко разработана. Отказ от рассмотрения в качестве объекта исследования бесконечных множеств как актуально заданных и требование эффективности всех осуществляемых построений привели к тому, что ряд интуиционистских вариантов традиционных разделов математики имеют с точки зрения классической математики достаточно своеобразный вид. Приведем в изложении Гейтинга некоторые взгляды Л. Э. Я. Брауэра "Согласно Брауэру, математика тождественна с точной частью нашего мышления... Никакая наука - в частности, ни философия, ни логика - не может служить предпосылкой для математики. Было бы порочным кругом применять в качестве средств для доказательства какие-либо философские или логические принципы,

потому что в формулировке этих принципов уже предполагаются математические понятия". Для математики не остается "никакого другого источника, кроме интуиции, которая с непосредственной ясностью помещает перед нашими глазами математические понятия и выводы". Эта интуиция "является не чем иным, как способностью рассматривать в отдельности различные понятия и выводы, регулярно встречающиеся в обычном мышлении". "В интуиционистской математике выводы не извлекаются по фиксированным правилам, которые можно объединить в логику, а каждый вывод в отдельности непосредственно подтверждается своей очевидностью". Кроме того, "имеются общие правила, посредством которых из данных математических теорем можно интуитивно ясным образом получать другие; теорию этих соотношений можно рассматривать в некоторой "математической логике", которая при этом является отраслью математики и не имеет ощутимых применений вне математики".

Л. Э. Я. Брауэр возражал против попыток формализации интуиционистской математики и логики, так как считал критерием верности построений прежде всего интуицию. Однако значительные успехи в изучении интуиционистской логики были достигнуты после того, как ее основные законы были сформулированы в виде соответствующих исчислений, которые были исследованы методами математической логики. Это позволило понять значение и особенности интуиционистской логики по сравнению с традиционной, что невозможно было сделать без точных формулировок. Л. Э. Я. Брауэр и его единомышленники в своих исследованиях выяснили, какая получается математика при последовательном проведении генетической точки зрения на образование математических понятий.

Отметим еще одну особенность. При изучении *Логики Высказываний* и *Исчисления Высказываний* мы начинали именно с *Логики Высказываний*, т. е. с семантики. Средствами *Логики Высказываний* было определено понятие *Логического Закона Логики Высказываний* или *Тождественно Истинной Формулы Логики Высказываний*, а *Исчисление Высказываний* давало другое описание множества *Тождественно Истинных Формул Логики Высказываний*.

В случае же *Интуиционистского Исчисления Высказываний* начинают именно с *Интуиционистского Исчисления Высказываний*, определяют в его рамках понятие *Выводимая Формула Интуиционистского Исчисления Высказываний*, а затем подбирают подходящую семантику, например, в терминах *моделей Крипке*.

Алфавит *Интуиционистского Исчисления Высказываний* совпадает с алфавитом *Исчисления Высказываний*.

Понятие формулы *Интуиционистского Исчисления Высказываний* совпадает с понятием формулы *Исчисления Высказываний*.

Аксиомами Интуиционистского Исчисления Высказываний служат формулы следующего вида

$I \rightarrow$.

I.1. $(A \rightarrow (B \rightarrow A))$.

$$\text{I.2. } ((\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})) \rightarrow ((\mathcal{A} \rightarrow \mathcal{B}) \rightarrow (\mathcal{A} \rightarrow \mathcal{C}))).$$

II_&.

$$\text{II.1. } ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{A}).$$

$$\text{II.2. } ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{B}).$$

$$\text{II.3. } ((\mathcal{C} \rightarrow \mathcal{A}) \rightarrow ((\mathcal{C} \rightarrow \mathcal{B}) \rightarrow (\mathcal{C} \rightarrow (\mathcal{A} \& \mathcal{B}))))).$$

III_∨.

$$\text{III.1. } (\mathcal{A} \rightarrow (\mathcal{A} \vee \mathcal{B})).$$

$$\text{III.2. } (\mathcal{B} \rightarrow (\mathcal{A} \vee \mathcal{B})).$$

$$\text{III.3. } ((\mathcal{A} \rightarrow \mathcal{C}) \rightarrow ((\mathcal{B} \rightarrow \mathcal{C}) \rightarrow ((\mathcal{A} \vee \mathcal{B}) \rightarrow \mathcal{C}))).$$

IV_¬.

$$\text{IV.1. } ((\mathcal{A} \rightarrow (\neg \mathcal{B})) \rightarrow (\mathcal{B} \rightarrow (\neg \mathcal{A}))).$$

$$\text{IV.2. } ((\neg \mathcal{A}) \rightarrow (\mathcal{A} \rightarrow \mathcal{B})).$$

Правилом вывода Интуиционистского Исчисления Высказываний служит **Правило Отделения МР (Modus Ponens)**

$$\frac{\mathcal{A}, (\mathcal{A} \rightarrow \mathcal{B})}{\mathcal{B}}.$$

Понятия **вывода** и **выводимой формулы** в **Интуиционистском Исчислении Высказываний** определяются аналогично тому, как это было сделано в **Исчислении Высказываний**.

Легко понять, что любая формула, выводимая в **Интуиционистском Исчислении Высказываний**, выводима и в **Исчислении Высказываний**. Обратное утверждение неверно, например, в **Интуиционистском Исчислении Высказываний** невыводимы формулы $((\neg(\neg \mathcal{A})) \rightarrow \mathcal{A})$ и $((\neg \mathcal{A}) \vee \mathcal{A})$. В то же время справедлива следующая теорема

Теорема 2.10.1. *Если формула \mathcal{A} выводима в Исчислении Высказываний, то в Интуиционистском Исчислении Высказываний выводима формула $(\neg(\neg \mathcal{A}))$.*

Пропозициональные системы для Интуиционистского Исчисления Высказываний

Произвольной булевой алгебре \mathcal{B} с основным множеством B , с операциями \cap , \cup и \neg , с единичным элементом 1 и нулевым элементом 0 сопоставим пропозициональную систему

$$\mathcal{M}_B = \langle \langle B, \{1\}, \neg_{\mathcal{M}_B}, \wedge_{\mathcal{M}_B}, \vee_{\mathcal{M}_B}, \rightarrow_{\mathcal{M}_B} \rangle \rangle,$$

где $\neg_{\mathcal{M}_B} a = \bar{a}$ — дополнение элемента a булевой алгебры \mathcal{B} , $a \wedge_{\mathcal{M}_B} b = a \cap b$, $a \vee_{\mathcal{M}_B} b = a \cup b$ и $a \rightarrow_{\mathcal{M}_B} b = \bar{a} \cup b$. Систему \mathcal{M}_B будем называть пропозициональной системой или многозначной логикой, соответствующей булевой

алгебре \mathcal{B} , при этом B будет множеством *истинностных значений*, а множество $F = \{1\}$ *выделенных истинностных значений* состоит лишь из единичного элемента булевой алгебры \mathcal{B} .

Пусть все пропозициональные переменные формулы \mathcal{A} содержатся в списке A_1, \dots, A_n . Для произвольных элементов a_1, \dots, a_n из множества B индукцией по построению формулы \mathcal{A} естественным образом определяется элемент $\mathcal{A}_{\mathcal{M}_{\mathcal{B}}}(a_1, \dots, a_n)$ из множества B , который называется *значением формулы \mathcal{A} при значениях $A_1 = a_1, \dots, A_n = a_n$ ее пропозициональных переменных*.

Если \mathcal{A} – пропозициональная переменная A_i , то полагаем

$$\mathcal{A}_{\mathcal{M}_{\mathcal{B}}}(a_1, \dots, a_n) = a_i.$$

Если формула \mathcal{A} имеет одну из форм $\neg(\mathcal{C})$, $(\mathcal{C} \& \mathcal{D})$, $(\mathcal{C} \vee \mathcal{D})$, $(\mathcal{C} \rightarrow \mathcal{D})$, то значение $\mathcal{A}_{\mathcal{M}_{\mathcal{B}}}(a_1, \dots, a_n)$ определяется соответствующим равенством

$$\begin{aligned} (\neg(\mathcal{C}))_{\mathcal{M}_{\mathcal{B}}}(a_1, \dots, a_n) &= \neg_{\mathcal{M}_{\mathcal{B}}}(\mathcal{C}_{\mathcal{M}_{\mathcal{B}}}(a_1, \dots, a_n)), \\ (\mathcal{C} \& \mathcal{D})_{\mathcal{M}_{\mathcal{B}}}(a_1, \dots, a_n) &= \mathcal{C}_{\mathcal{M}_{\mathcal{B}}}(a_1, \dots, a_n) \wedge_{\mathcal{M}_{\mathcal{B}}} \mathcal{D}_{\mathcal{M}_{\mathcal{B}}}(a_1, \dots, a_n), \\ (\mathcal{C} \vee \mathcal{D})_{\mathcal{M}_{\mathcal{B}}}(a_1, \dots, a_n) &= \mathcal{C}_{\mathcal{M}_{\mathcal{B}}}(a_1, \dots, a_n) \vee_{\mathcal{M}_{\mathcal{B}}} \mathcal{D}_{\mathcal{M}_{\mathcal{B}}}(a_1, \dots, a_n), \\ (\mathcal{C} \rightarrow \mathcal{D})_{\mathcal{M}_{\mathcal{B}}}(a_1, \dots, a_n) &= \mathcal{C}_{\mathcal{M}_{\mathcal{B}}}(a_1, \dots, a_n) \rightarrow_{\mathcal{M}_{\mathcal{B}}} \mathcal{D}_{\mathcal{M}_{\mathcal{B}}}(a_1, \dots, a_n). \end{aligned}$$

Если при любых значениях a_1, \dots, a_n из множества B пропозициональных переменных A_1, \dots, A_n формулы \mathcal{A} она принимает значение $\mathcal{A}_{\mathcal{M}}(a_1, \dots, a_n)$, равное единице 1 булевой алгебры \mathcal{B} , то формула \mathcal{A} называется **общезначимой** в пропозициональной системе $\mathcal{M}_{\mathcal{B}}$, соответствующей булевой алгебре \mathcal{B} .

Легко проверить, что любая пропозициональная система $\mathcal{M}_{\mathcal{B}}$, соответствующая произвольной булевой алгебре \mathcal{B} , согласована с **Правилем Вывода МР**, т. е. из того, что формулы \mathcal{A} и $(\mathcal{A} \rightarrow \mathcal{B})$ приминают значение 1 следует, что и \mathcal{B} приминает значение 1.

Теорема 2.10.2. Формула \mathcal{A} выводима в **Исчислении Высказываний** тогда и только тогда, когда она общезначима в каждой пропозициональной системе $\mathcal{M}_{\mathcal{B}}$, соответствующей произвольной булевой алгебре \mathcal{B} .

Д о к а з а т е л ь с т в о. Непосредственная проверка показывает, что каждая логическая аксиома **Исчисления Высказываний** общезначима в любой пропозициональной системе $\mathcal{M}_{\mathcal{B}}$, соответствующей произвольной булевой алгебре \mathcal{B} . А так как каждая пропозициональная система $\mathcal{M}_{\mathcal{B}}$, соответствующая произвольной булевой алгебре \mathcal{B} , согласована с **Правилем Вывода МР**, то любая формула \mathcal{A} , выводимая в **Исчислении Высказываний**, общезначима в каждой пропозициональной системе $\mathcal{M}_{\mathcal{B}}$, соответствующей произвольной булевой алгебре \mathcal{B} .

Для доказательства обратного утверждения рассмотрим булеву алгебру

$$\mathcal{B}_2 = \langle \langle \{0, 1\}, \cap, \cup, - \rangle \rangle,$$

где $a \cap b = \min\{a, b\}$, $a \cup b = \max\{a, b\}$, $\bar{0} = 1$ и $\bar{1} = 0$.

Заметим, что *тождественная истинность формулы A Исчисления Высказываний* равносильна ее общезначимости в пропозициональной системе M_{B_2} , соответствующей булевой алгебре B_2 .

Если формула A *Исчисления Высказываний* общезначима в каждой пропозициональной системе M_B , соответствующей произвольной булевой алгебре B , то она, в частности, общезначима в пропозициональной системе M_{B_2} , соответствующей булевой алгебре B_2 . Значит, формула A тождественно истинна в *Логике Высказываний*, а следовательно, она выводима в *Исчислении Высказываний*. \square

Если назвать множество всех формул *Логике Высказываний*, истинных на каждой пропозициональной системе из класса K , *пропозициональной теорией класса K* , то доказанная теорема может быть сформулирована более кратко: *пропозициональная теория класса всех пропозициональных систем*

$$M_B = \langle \langle B, \{1\}, \neg_{M_B}, \wedge_{M_B}, \vee_{M_B}, \rightarrow_{M_B} \rangle \rangle,$$

соответствующих всевозможным булевым алгебрам B , совпадает с Исчислением Высказываний.

Следствие 2.10.2.1. *Формула A выводима в Исчислении Высказываний тогда и только тогда, когда она общезначима в пропозициональной системе M_{B_2} , соответствующей булевой алгебре B_2 .*

Следствие также допускает более краткую формулировку *пропозициональная теория пропозициональной системы M_{B_2} , соответствующей булевой алгебре B_2 , совпадает с Исчислением Высказываний.*

Заметим, что следствие характеризует выводимые в *Исчислении Высказываний* формулы как формулы, общезначимые в пропозициональной системе M_{B_2} , соответствующей двуэлементной булевой алгебре B_2 . Она же дает *разрешающий алгоритм*, позволяющий для произвольной формулы A *Исчисления Высказываний* ответить на вопрос, выводима ли формула A в *Исчислении Высказываний*.

Следствие 2.10.2.2. *Для любой ненулевой булевой алгебры B имеет место эквивалентность:*

формула A выводима в Исчислении Высказываний тогда и только тогда, когда она общезначима в пропозициональной системе M_B , соответствующей булевой алгебре B .

Доказательство следствия сразу получается из предыдущего следствия, если заметить, что любая ненулевая булева алгебра B содержит в качестве подалгебры двуэлементную булеву алгебру B_2 .

Последнее следствие также допускает более краткую формулировку

*пропозициональная теория пропозициональной системы \mathcal{M}_B , соответствующей произвольной ненулевой булевой алгебре B , совпадает с **Исчислением Высказываний**.*

В случае **Интуиционистского Исчисления Высказываний** ситуация несколько более сложная. Хотя разрешающий алгоритм для **Интуиционистского Исчисления Высказываний** существует, но он не столь простой, как в случае **Исчисления Высказываний**. Для **Интуиционистского Исчисления Высказываний** справедлива теорема, аналогичная теореме 2.10.2, однако в ней вместо булевых алгебр будет использовано более общее понятие – понятие *псевдобулевой алгебры*.

На множестве $F_{ИИВ}$ всех формул **Интуиционистского Исчисления Высказываний** определим отношение \equiv , полагая

$$A \equiv B \iff \vdash_{ИИВ} (A \leftrightarrow B).$$

Покажем, что отношение \equiv является *отношением эквивалентности*. Рефлексивность отношения \equiv следует из доказуемости в **Интуиционистском Исчислении Высказываний** любой формулы вида

$$(A \leftrightarrow A),$$

A – произвольная формула, что устанавливается так же, как и в **Исчислении Высказываний**.

Симметричность этого отношения следует из того, что

$$\text{если } \vdash_{ИИВ} (C \& D), \text{ то } \vdash_{ИИВ} (D \& C).$$

Покажем, что это отношение транзитивно. Пусть $A \equiv B$ и $B \equiv C$. Тогда $\vdash_{ИИВ} (A \rightarrow B)$ и $\vdash_{ИИВ} (B \rightarrow C)$. Используя аксиомы I.1 и I.2, нетрудно получить $\vdash_{ИИВ} (A \rightarrow C)$. Аналогично получаем, что $\vdash_{ИИВ} (C \rightarrow A)$. Поэтому $A \equiv C$.

Через $[A]$ будем обозначать *класс эквивалентности* по отношению \equiv , определяемый формулой A . Множество классов эквивалентности, т. е. фактормножество $F_{ИИВ} / \equiv$, возьмем в качестве основного множества M следующей пропозициональной системы

$$\mathcal{M}_{ИИВ} = \langle M, F, \neg_M, \wedge_M, \vee_M, \rightarrow_M \rangle.$$

В дальнейшем для сокращения индекс ИИВ в записи $\mathcal{M}_{ИИВ}$ будем опускать, т. е. будем просто писать \mathcal{M} . Полагаем

$$\begin{aligned} \neg_M([A]) &\equiv [(\neg A)], & \wedge_M([A], [B]) &\equiv [(A \& B)], \\ \vee_M([A], [B]) &\equiv [(A \vee B)], & \rightarrow_M([A], [B]) &\equiv [(A \rightarrow B)], \\ & & \equiv_M([A], [B]) &\equiv [(A \equiv B)]. \end{aligned}$$

Если формулы \mathcal{A} и \mathcal{B} таковы, что $\vdash_{ИИВ} \mathcal{A}$ и $\vdash_{ИИВ} \mathcal{B}$, то

$$\vdash_{ИИВ} (\mathcal{A} \longleftrightarrow \mathcal{B}),$$

поэтому $\mathcal{A} \equiv \mathcal{B}$. Обозначим через $1_{\mathcal{M}}$ класс эквивалентности $[(A_1 \rightarrow A_1)]$. Заметим, что этот класс эквивалентности состоит в точности из всех формул, доказуемых в ИИВ.

$$F \equiv \{[(A_1 \rightarrow A_1)]\}.$$

Нетрудно проверить, что построенная пропозициональная система $\mathcal{M}_{ИИВ}$ согласована с правилом вывода MP , т. е. из того, что формулы \mathcal{A} и $(\mathcal{A} \rightarrow \mathcal{B})$ при любых значениях из множества M своих пропозициональных переменных принимают значения из F следует, что и формула \mathcal{B} при любых значениях из множества M своих пропозициональных переменных принимает значение из F .

В дальнейшем часто для любой операции

$$*_M \in \{\wedge_M, \vee_M, \rightarrow_M\}$$

вместо записи $*_M(a, b)$ будем использовать запись $a *_M b$.

Отметим два простых, но важных для дальнейшего свойства построенной пропозициональной системы $\mathcal{M}_{ИИВ}$. Во-первых, для любого элемента a из M $a \rightarrow_M a = 1_M$ и

$$a \vee_M 1_M = 1_M \vee_M a = 1_M.$$

Первое утверждение следует из доказуемости в ИИВ формулы $(A_1 \rightarrow A_1)$, а второе из доказуемости в ИИВ формул $(\mathcal{A} \rightarrow (A_1 \vee \mathcal{A}))$, $(\mathcal{A} \rightarrow (\mathcal{A} \vee A_1))$ и доказуемости для любой доказуемой в ИИВ формулы \mathcal{A} формул

$$((\mathcal{A} \vee A_1) \rightarrow \mathcal{A}) \text{ и } ((A_1 \vee \mathcal{A}) \rightarrow \mathcal{A}).$$

Чтобы подчеркнуть, что все пропозициональные переменные формулы \mathcal{A} содержатся в списке A_1, \dots, A_n , будем использовать для нее обозначение

$$\mathcal{A}(A_1, \dots, A_n).$$

В такой ситуации для произвольных формул $\mathcal{A}_1, \dots, \mathcal{A}_n$ результат

$$\mathcal{A}_{A_1, \dots, A_n}[\mathcal{A}_1, \dots, \mathcal{A}_n]$$

одновременной замены в формуле \mathcal{A} пропозициональной переменной A_1 на формулу \mathcal{A}_1 , \dots , пропозициональной переменной A_n на формулу \mathcal{A}_n будем обозначать через

$$\mathcal{A}(\mathcal{A}_1, \dots, \mathcal{A}_n).$$

Индукцией по длине формулы \mathcal{A} легко доказывается, что при сделанных предположениях выполняется равенство

$$\mathcal{A}_{\mathcal{M}}([\mathcal{A}_1], \dots, [\mathcal{A}_n]) = [\mathcal{A}(\mathcal{A}_1, \dots, \mathcal{A}_n)].$$

Для построенной пропозициональной системы $\mathcal{M}_{ИИВ}$ справедлива следующая теорема.

Теорема 2.10.3. *Формула \mathcal{A} при любых значениях из множества M своих пропозициональных переменных принимает значение 1_M тогда и только тогда, когда формула \mathcal{A} выводима в **Интуиционистском Исчислении Высказываний**.*

Доказательство. Если формула \mathcal{A} при любых значениях a_1, \dots, a_n из множества M своих пропозициональных переменных A_1, \dots, A_n принимает значение $\mathcal{A}_M(a_1, \dots, a_n)$ из множества F , т. е.

$$\mathcal{A}_M(a_1, \dots, a_n) = 1_M,$$

то, в частности,

$$\mathcal{A}_M([A_1], \dots, [A_n]) = 1_M.$$

Но

$$\mathcal{A}_M([A_1], \dots, [A_n]) = [\mathcal{A}(A_1, \dots, A_n)] = [\mathcal{A}],$$

поэтому $\vdash_{ИИВ} \mathcal{A}$.

Обратно, если $\vdash_{ИИВ} \mathcal{A}$, то и для произвольных формул A_1, \dots, A_n

$$\vdash_{ИИВ} \mathcal{A}(\mathcal{A}_1, \dots, \mathcal{A}_n).$$

Значит, $[\mathcal{A}(\mathcal{A}_1, \dots, \mathcal{A}_n)] = 1_M$. Поэтому $\mathcal{A}_M([A_1], \dots, [A_n]) = 1_M \in F$. \square

Доказанная теорема может быть сформулирована более кратко:
*пропозициональная теория пропозициональной системы M совпадает с **Интуиционистским Исчислением Высказываний**.*

Следующее следствие было доказано в ходе доказательства предыдущей теоремы.

Следствие 2.10.3.1. *Формула \mathcal{A} при значениях $[A_1], \dots, [A_n]$ своих пропозициональных переменных A_1, \dots, A_n принимает значение*

$$\mathcal{A}_{M_{ИИВ}}([A_1], \dots, [A_n]) = 1_{M_{ИИВ}}$$

*тогда и только тогда, когда эта формула \mathcal{A} выводима в **Интуиционистском Исчислении Высказываний**.*

Построенная система $M_{ИИВ}$ является *псевдобулевой алгеброй*.

Так как множество $F_{ИИВ}$ всех формул **Интуиционистского Исчисления Высказываний** счетно и при любых неравных между собой i и j формулы A_i и A_j неэквивалентны, то множество M *счетно*. К. Гедель установил, что для **Интуиционистского Исчисления Высказываний** построить конечную пропозициональную систему с аналогичным свойством нельзя.

Теорема 2.10.4. Если пропозициональная система

$$\mathcal{M} = \langle \langle M, F, \neg_{\mathcal{M}}, \wedge_{\mathcal{M}}, \vee_{\mathcal{M}}, \rightarrow_{\mathcal{M}} \rangle \rangle$$

удовлетворяет условию: для любой формулы A **Интуиционистского Исчисления Высказываний** справедлива эквивалентность:

формула A при любых значениях из множества M своих пропозициональных переменных принимает значение из F тогда и только тогда, когда формула A выводима в **Интуиционистском Исчислении Высказываний**, то множество M бесконечно.

Д о к а з а т е л ь с т в о. Допустим, что существует пропозициональная система

$$\mathcal{M} = \langle \langle M, F, \neg_{\mathcal{M}}, \wedge_{\mathcal{M}}, \vee_{\mathcal{M}}, \rightarrow_{\mathcal{M}} \rangle \rangle,$$

удовлетворяющая условию: для любой формулы A **Интуиционистского Исчисления Высказываний** справедлива эквивалентность:

формула A при любых значениях из множества M своих пропозициональных переменных принимает значение из F тогда и только тогда, когда формула A выводима в **Интуиционистском Исчислении Высказываний**, причем множество M конечно и состоит из t элементов.

Рассмотрим формулу

$$\mathcal{F}_m \equiv \bigcup_{1 \leq i < j \leq m+1} (A_i \equiv A_j).$$

Если $[A_1], \dots, [A_{m+1}]$ – произвольный набор значений из множества M пропозициональных переменных A_1, \dots, A_{m+1} формулы \mathcal{F}_m , то при некоторых $t < s$ $[A_t] = [A_s]$.

Значит, $\vdash_{ИИВ} A_t \equiv A_s$.

Поэтому $\vdash_{ИИВ} \mathcal{F}_m(A_1, \dots, A_{m+1})$.

Рассмотрим пропозициональную систему

$$\mathcal{M}_m = \langle \langle M_m, F_m, \neg_{\mathcal{M}_m}, \wedge_{\mathcal{M}_m}, \vee_{\mathcal{M}_m}, \rightarrow_{\mathcal{M}_m} \rangle \rangle,$$

где $M_m = \{0, 1, \dots, m\}$, $F_m = \{0\}$, $a \wedge_{\mathcal{M}_m} b = \max(a, b)$, $a \vee_{\mathcal{M}_m} b = \min(a, b)$, $a \rightarrow_{\mathcal{M}_m} b$ равно 0 при $a \geq b$ и равно b при $a < b$, $\neg_{\mathcal{M}_m} a$ равно 0 при $a = m$ и равно m в противном случае.

Нетрудно проверить, что все выводимые в ИИВ формулы, *общезначаимы* в пропозициональной системе \mathcal{M}_m . В то же время формула \mathcal{F}_m при значениях $A_1 = 0, A_2 = 1, \dots, A_{m+1} = m$ своих пропозициональных переменных принимает значение 1, значит, она не выводима в **Интуиционистском Исчислении Высказываний**. Что противоречит условию теоремы. \square

Произвольной *псевдобулевой алгебре* \mathcal{B} с основным множеством B , с операциями $\cap, \cup \Rightarrow$ и \sim , с единичным элементом 1 и нулевым элементом 0 сопоставим пропозициональную систему

$$\mathcal{M}_{\mathcal{B}} = \langle \langle B, \{1\}, \wedge_{\mathcal{M}_{\mathcal{B}}}, \vee_{\mathcal{M}_{\mathcal{B}}}, \Rightarrow_{\mathcal{M}_{\mathcal{B}}}, \neg_{\mathcal{M}_{\mathcal{B}}} \rangle \rangle,$$

где $\neg_{\mathcal{M}_B} a = \sim a$ – *псевдодополнение* элемента a псевдобулевой алгебры \mathcal{B} , $a \wedge_{\mathcal{M}_B} b = a \cap b$, $a \vee_{\mathcal{M}_B} b = a \cup b$ и $a \Rightarrow_{\mathcal{M}_B} b = a \Rightarrow b$. Систему \mathcal{M}_B будем называть *пропозициональной системой* или *многозначной логикой*, соответствующей псевдобулевой алгебре \mathcal{B} , при этом B будет множеством *истинностных значений*, а множество $F = \{1\}$ *выделенных истинностных значений* состоит лишь из единичного элемента псевдобулевой алгебры \mathcal{B} .

Пусть все пропозициональные переменные формулы \mathcal{A} содержатся в списке A_1, \dots, A_n . Для произвольных элементов a_1, \dots, a_n из множества B индукцией по построению формулы \mathcal{A} естественным образом определяется элемент $\mathcal{A}_{\mathcal{M}_B}(a_1, \dots, a_n)$ из множества B , который называется *значением формулы \mathcal{A} при значениях $A_1 = a_1, \dots, A_n = a_n$ ее пропозициональных переменных*.

Если \mathcal{A} – пропозициональная переменная A_i , то полагаем

$$\mathcal{A}_{\mathcal{M}_B}(a_1, \dots, a_n) = a_i.$$

Если формула \mathcal{A} имеет одну из форм $\neg(\mathcal{C})$, $(\mathcal{C} \& \mathcal{D})$, $(\mathcal{C} \vee \mathcal{D})$, $(\mathcal{C} \rightarrow \mathcal{D})$, то значение $\mathcal{A}_{\mathcal{M}_B}(a_1, \dots, a_n)$ определяется соответствующим равенством

$$\begin{aligned} (\neg(\mathcal{C}))_{\mathcal{M}_B}(a_1, \dots, a_n) &= \neg_{\mathcal{M}_B}(\mathcal{C}_{\mathcal{M}_B}(a_1, \dots, a_n)) = \sim \mathcal{C}_{\mathcal{M}_B}(a_1, \dots, a_n), \\ (\mathcal{C} \& \mathcal{D})_{\mathcal{M}_B}(a_1, \dots, a_n) &= \mathcal{C}_{\mathcal{M}_B}(a_1, \dots, a_n) \wedge_{\mathcal{M}_B} \mathcal{D}_{\mathcal{M}_B}(a_1, \dots, a_n) = \\ &= \mathcal{C}_{\mathcal{M}_B}(a_1, \dots, a_n) \cap \mathcal{D}_{\mathcal{M}_B}(a_1, \dots, a_n), \\ (\mathcal{C} \vee \mathcal{D})_{\mathcal{M}_B}(a_1, \dots, a_n) &= \mathcal{C}_{\mathcal{M}_B}(a_1, \dots, a_n) \vee_{\mathcal{M}_B} \mathcal{D}_{\mathcal{M}_B}(a_1, \dots, a_n) = \\ &= \mathcal{C}_{\mathcal{M}_B}(a_1, \dots, a_n) \cup \mathcal{D}_{\mathcal{M}_B}(a_1, \dots, a_n), \\ (\mathcal{C} \rightarrow \mathcal{D})_{\mathcal{M}_B}(a_1, \dots, a_n) &= \mathcal{C}_{\mathcal{M}_B}(a_1, \dots, a_n) \Rightarrow_{\mathcal{M}_B} \mathcal{D}_{\mathcal{M}_B}(a_1, \dots, a_n) = \\ &= \mathcal{C}_{\mathcal{M}_B}(a_1, \dots, a_n) \Rightarrow \mathcal{D}_{\mathcal{M}_B}(a_1, \dots, a_n). \end{aligned}$$

Если при любых значениях a_1, \dots, a_n из множества B пропозициональных переменных A_1, \dots, A_n формулы \mathcal{A} она принимает значение $\mathcal{A}_{\mathcal{M}}(a_1, \dots, a_n)$, равное единице 1 псевдобулевой алгебры \mathcal{B} , то формула \mathcal{A} называется *общезначимой* в пропозициональной системе \mathcal{M}_B , соответствующей псевдобулевой алгебре \mathcal{B} .

Используя неравенство (7) теоремы 4.3.1 из **Дополнения**, легко получаем, что *любая пропозициональная система \mathcal{M}_B , соответствующая произвольной псевдобулевой алгебре \mathcal{B} , согласована с **Правилом Вывода МР***, т. е. из того, что формулы \mathcal{A} и $(\mathcal{A} \rightarrow \mathcal{B})$ принимают значение 1 следует, что и \mathcal{B} принимает значение 1.

Теорема 2.10.5. *Формула \mathcal{A} выводима в **Интуиционистском Исчислении Высказываний** тогда и только тогда, когда она общезначима в каждой пропозициональной системе \mathcal{M}_B , соответствующей произвольной псевдобулевой алгебре \mathcal{B} .*

Д о к а з а т е л ь с т в о. Непосредственная проверка с использованием теоремы 4.3.1 из **Дополнения** показывает, что каждая логическая аксиома **Ин-**

туиционистского Исчисления Высказываний общезначима в любой пропозициональной системе \mathcal{M}_B , соответствующей произвольной псевдобулевой алгебре B .

Так как любая пропозициональная система \mathcal{M}_B , соответствующая произвольной псевдобулевой алгебре B , согласована с **Правилем Вывода МР**, то индукцией по длине вывода легко устанавливается, что любая формула A , выводимая в **Интуиционистском Исчислении Высказываний**, общезначима в каждой пропозициональной системе \mathcal{M}_B , соответствующей произвольной псевдобулевой алгебре B .

Справедливость обратного утверждения следует из теоремы 2.10.3. \square

Доказанная теорема не дает разрешающего алгоритма для **Интуиционистского Исчисления Высказываний**. Из следующей более общей теоремы такой алгоритм будет нетрудно получить.

Теорема 2.10.6. *Для произвольной формулы A в языке **Интуиционистского Исчисления Высказываний** эквивалентны следующие утверждения:*

- 1) *формула A выводима в **Интуиционистском Исчислении Высказываний**;*
- 2) *формула A общезначима в каждой пропозициональной системе \mathcal{M}_B , соответствующей произвольной псевдобулевой алгебре B ;*
- 3) *формула A при значениях $[A_1], \dots, [A_n]$ своих пропозициональных переменных A_1, \dots, A_n принимает значение*

$$\mathcal{A}_{\mathcal{M}_{ИИВ}}([A_1], \dots, [A_n]) = 1_{\mathcal{M}_{ИИВ}}$$

в пропозициональной системе $\mathcal{M}_{ИИВ}$;

- 4) *формула A общезначима в каждой пропозициональной системе \mathcal{M}_B , соответствующей произвольной конечной псевдобулевой алгебре B ;*
- 5) *формула A общезначима в каждой пропозициональной системе \mathcal{M}_B , соответствующей произвольной конечной псевдобулевой алгебре B с числом элементов не более, чем 2^{2^m} , где m – число всех подформул формулы A .*

Д о к а з а т е л ь с т в о. Так как уже установлено, что 1) и 2) эквивалентны, 1) и 3) эквивалентны, из 2) следует 4), а из 4) следует 5), то для завершения доказательства теоремы достаточно показать, что из 5) следует 3).

Предположим, что формула A при значениях $[A_1], \dots, [A_n]$ в пропозициональной системе $\mathcal{M}_{ИИВ}$ своих пропозициональных переменных A_1, \dots, A_n принимает значение $\mathcal{A}_{\mathcal{M}_{ИИВ}}([A_1], \dots, [A_n]) \neq 1_{\mathcal{M}_{ИИВ}}$. Покажем, что формула A необщезначима в некоторой пропозициональной системе \mathcal{M}_B , соответствующей подходящей конечной псевдобулевой алгебре B с числом элементов не более, чем 2^{2^m} , где m – число всех подформул формулы A .

Обозначим через X подмножество

$$\{ [B] \mid B - \text{подформула формулы } A \}$$

псевдобулевой алгебры $\mathcal{M}_{ИИВ}$.

Так как подмножество X состоит из не более, чем m элементов, то по теореме 4.3.2 подалгебра $\mathcal{M}_{ИИВ}(X)$ псевдобулевой алгебры $\mathcal{M}_{ИИВ}$, порожденная подмножеством X состоит из не более, чем 2^{2^m} элементов.

Непосредственная проверка показывает, что формула \mathcal{A} при значениях $[A_1], \dots, [A_n]$ в пропозициональных системах $\mathcal{M}_{ИИВ}$ и $\mathcal{M}_{ИИВ}(X)$ своих пропозициональных переменных A_1, \dots, A_n принимает одинаковые значения, т. е. выполняется равенство

$$\mathcal{A}_{\mathcal{M}_{ИИВ}(X)}([A_1], \dots, [A_n]) = \mathcal{A}_{\mathcal{M}_{ИИВ}}([A_1], \dots, [A_n]).$$

Так как $1_{\mathcal{M}_{ИИВ}(X)} = 1_{\mathcal{M}_{ИИВ}}$, то

$$\mathcal{A}_{\mathcal{M}_{ИИВ}(X)}([A_1], \dots, [A_n]) = \mathcal{A}_{\mathcal{M}_{ИИВ}}([A_1], \dots, [A_n]) \neq 1_{\mathcal{M}_{ИИВ}} = 1_{\mathcal{M}_{ИИВ}(X)}.$$

Значит, формула \mathcal{A} необщезначима в пропозициональной системе, соответствующей конечной псевдобулевой алгебре $\mathcal{M}_{ИИВ}(X)$ с числом элементов не более, чем 2^{2^m} , где m – число всех подформул формулы \mathcal{A} .

Тем самым установлено, что из 5) следует 3). Это завершает доказательство теоремы. \square

Из доказанной теоремы легко получить разрешающий алгоритм для **Интуиционистского Исчисления Высказываний**.

Чтобы по произвольной формуле \mathcal{A} определить, выводима ли она в **Интуиционистском Исчислении Высказываний**, запускаем алгоритм \mathfrak{A} .

Алгоритм \mathfrak{A} строит всевозможные конечные псевдобулевы алгебры с числом элементов не более, чем 2^{2^m} , где m – число всех подформул формулы \mathcal{A} . Причем в качестве основных множеств этих псевдобулевых алгебр выступают начальные отрезки множества натуральных чисел. И для каждой построенной псевдобулевой алгебры этот алгоритм проверяет, является ли формула \mathcal{A} общезначимой в ней.

Если формула \mathcal{A} общезначима на каждой из построенных конечных псевдобулевых алгебр, то она выводима в **Интуиционистском Исчислении Высказываний**.

Если же в процессе работы алгоритма \mathfrak{A} удастся обнаружить конечную псевдобулеву алгебру с числом элементов не более, чем 2^{2^m} , где m – число всех подформул формулы \mathcal{A} , на которой формула \mathcal{A} не является общезначимой, формула \mathcal{A} не выводима в **Интуиционистском Исчислении Высказываний**.

Теоремы 2.10.5 и 2.10.6 показывают, что на основе псевдобулевых алгебр можно построить семантику **Интуиционистского Исчисления Высказываний**.

В качестве примера применения псевдобулевых алгебр к **Интуиционистскому Исчислению Высказываний** установим невыводимость в нем некоторых формул.

Рассмотрим псевдобулеву алгебру \mathcal{B} с основным множеством

$$B = \{0, 1/2, 1\},$$

с операциями \cap , $\cup \Rightarrow$ и \sim , с единичным элементом 1 и нулевым элементом 0, где:

$$(a \cap b) = \min(a, b); \quad (a \cup b) = \max(a, b);$$

$$(a \Rightarrow b) = \begin{cases} 1, & \text{если } a \leq b, \\ b, & \text{если } a > b; \end{cases} \quad (\sim a) = (a \Rightarrow 0) = \begin{cases} 1, & \text{если } a = 0, \\ 0, & \text{если } a \neq 0. \end{cases}$$

Описанным выше способом сопоставим псевдобулевой алгебре \mathcal{B} пропозициональную систему

$$\mathcal{M}_{\mathcal{B}} = \langle \langle B, \{1\}, \wedge_{\mathcal{M}_{\mathcal{B}}}, \vee_{\mathcal{M}_{\mathcal{B}}}, \Rightarrow_{\mathcal{M}_{\mathcal{B}}}, \neg_{\mathcal{M}_{\mathcal{B}}} \rangle \rangle,$$

где $\neg_{\mathcal{M}_{\mathcal{B}}} a = \sim a$ – псевдодополнение элемента a псевдобулевой алгебры \mathcal{B} , $a \wedge_{\mathcal{M}_{\mathcal{B}}} b = a \cap b$, $a \vee_{\mathcal{M}_{\mathcal{B}}} b = a \cup b$ и $a \Rightarrow_{\mathcal{M}_{\mathcal{B}}} b = a \Rightarrow b$. Напомним, что эта система $\mathcal{M}_{\mathcal{B}}$ называется пропозициональной системой или многозначной логикой, соответствующей псевдобулевой алгебре \mathcal{B} , при этом B является множеством истинностных значений, а множество $F = \{1\}$ выделенных истинностных значений состоит лишь из единичного элемента псевдобулевой алгебры \mathcal{B} .

Докажем невыводимость в **Интуиционистском Исчислении Высказываний** следующих трех формул

$$\mathcal{A}_1 = (A_1 \vee (\neg A_1)), \quad \mathcal{A}_2 = ((\neg(\neg A_1)) \Rightarrow A_1),$$

$$((A_1 \Rightarrow A_2) \Rightarrow ((\neg A_1) \Rightarrow A_2) \Rightarrow A_2)).$$

Напомним, что первая формула – это известный нам из **Логике Высказываний** **Закон исключенного третьего**, а вторая формула – это известный нам из **Логике Высказываний** **Закон снятия двойного отрицания**. Отметим, что вторая формула входит в список логических аксиом **Исчисления Высказываний**, а первая формула выводима в **Исчислении Высказываний**.

Для установления невыводимости в **Интуиционистском Исчислении Высказываний** этих трех формул достаточно заметить, что каждая из них принимает значение $1/2$ при значениях $A_1 = 1/2$ и $A_2 = 1/2$, входящих в них пропозициональных переменных.

Более широкое распространение получила семантика **Интуиционистского Исчисления Высказываний**, основанная на **моделях Крипке**.

Модель Крипке для **Логике Высказываний** – это

$$\mathcal{K} = \langle K, \preceq, \models \rangle,$$

где $\langle K, \preceq \rangle$ – частично упорядоченное множество, называемое **шкалой Крипке**, а \models – некоторое соответствие между множеством K и множеством V всех пропозициональных переменных, удовлетворяющее условию:

если α и β – элементы множества K , A_n – пропозициональная переменная из V , $\alpha \models A_n$ и $\alpha \preceq \beta$, то $\beta \models A_n$.

При этом соответствие \models называется **оценкой Крипке**.

Интуитивный смысл **моделей Крипке** отражает интуиционистское представление о становящемся характере истинности высказывания. С позиций интуиционизма истинность высказывания тесно связана с возможностью его доказательства – высказывание считается истинным, если имеется его доказательство. Элементы множества K можно интуитивно трактовать как моменты времени, при этом если $\alpha \preceq \beta$, то мы считаем, что момент времени α предшествует моменту времени β . Кроме того, каждому моменту времени соответствует состояние знаний в этом момент. Поэтому если α и β – элементы множества K (моменты времени), A_n – пропозициональная переменная и $\alpha \models A_n$, т. е. высказывание A_n доказано к моменту времени α , а $\alpha \preceq \beta$, т. е. момент времени β позже α , то $\beta \models A_n$. Это условие называется **принципом сохранения истинности**:

все то, что истинно (доказано) в данный момент, остается истинным (доказанным) в будущем.

Модель Крипке $\mathcal{K} = \langle K, \preceq, \models \rangle$ с конечным множеством K называется конечной. Мы не будем более подробно останавливаться на интуитивном смысле рассматриваемых понятий, который во многом прояснится после расширения соответствия \models до соответствия между множеством K и множеством всех пропозициональных формул, что будет сделано индукцией по построению пропозициональных формул.

Если α – элемент множества K , а \mathcal{A} и \mathcal{B} – пропозициональные формулы, то полагаем

$\alpha \models (\mathcal{A} \& \mathcal{B})$ тогда и только тогда, когда

$$\alpha \models \mathcal{A} \text{ и } \alpha \models \mathcal{B},$$

$\alpha \models (\mathcal{A} \vee \mathcal{B})$ тогда и только тогда, когда

$$\alpha \models \mathcal{A} \text{ или } \alpha \models \mathcal{B},$$

$\alpha \models (\mathcal{A} \Rightarrow \mathcal{B})$ тогда и только тогда, когда

$$(\forall \beta \succ \alpha) \beta \not\models \mathcal{A} \text{ или } \beta \models \mathcal{B},$$

$\alpha \models (\neg \mathcal{A})$ тогда и только тогда, когда

$$(\forall \beta \succ \alpha) \beta \not\models \mathcal{A}.$$

Индукцией по построению формул нетрудно доказать, что **принцип сохранения истинности** верен и для формул:

если \mathcal{A} – произвольная формула, $\alpha \models \mathcal{A}$ и $\alpha \preceq \beta$, то $\beta \models \mathcal{A}$.

Формула \mathcal{A} называется **истинной в модель Крипке**

$$\mathcal{K} = \langle K, \preceq, \models \rangle,$$

если для любого α из K : $\alpha \models \mathcal{A}$.

Запись $K \models A$ означает, что формула A *истинна в модели Крипке* K .

Если формула A *не истинна в модели Крипке* K , то K называют *контромоделью* для формулы A .

Следующая фундаментальная теорема играет для **Интуиционистского Исчисления Высказываний** роль, аналогичную теореме Э. Поста для классического **Исчисления Высказываний**, — она устанавливает корректность и полноту **Интуиционистского Исчисления Высказываний** относительно *моделей Крипке*.

Теорема 2.10.7. *Пропозициональная формула выводима в Интуиционистском Исчислении Высказываний тогда и только тогда, когда она истинна в любой конечной модели Крипке.*

Используя эту теорему, еще раз покажем, что в **Интуиционистском Исчислении Высказываний** невыводим **Закон исключенного третьего**, т. е. невыводима формула $(A_1 \vee (\neg A_1))$. Построим для этой формулы контромодель Крипке. Полагаем $K = \{0, 1\}$, $0 \preceq 0$, $0 \preceq 1$, $1 \preceq 1$ и лишь $1 \models A_1$. А значит, $0 \not\models A_1$.

Покажем, что $0 \not\models (A_1 \vee (\neg A_1))$.

Допустим, что $0 \models (A_1 \vee (\neg A_1))$. Тогда либо $0 \models A_1$, либо $0 \models (\neg A_1)$. Однако первое не выполнено по определению. Из второго следует, что $0 \not\models A_1$ и $1 \not\models A_1$. Но последнее невозможно, так как по определению $1 \models A_1$. Поэтому предположение $0 \models (A_1 \vee (\neg A_1))$ неверно, значит, $0 \not\models (A_1 \vee (\neg A_1))$ и построенная модель Крипке служит контромоделью для этой формулы.

ГЛАВА 3.

ЛОГИКА И ИСЧИСЛЕНИЕ ПРЕДИКАТОВ

3.1. Языки первого порядка

Пусть \mathbb{N} – множество натуральных чисел.

Определение 3.1.1. *Сигнатурой* называется пятерка

$$\tau = \langle C, F, P, \theta, \varphi \rangle,$$

где C, F и P – множества, а $\theta : F \rightarrow \mathbb{N}$, $\varphi : P \rightarrow \mathbb{N}$.

Множества C, F или P могут быть, в частности, пустыми.

C называется множеством символов **индивидуальных констант**, а его элементы – **символами индивидуальных констант** или просто **константами**.

F называется множеством **функциональных символов**, и если $f \in F$, то f называется $\theta(f)$ -местным **функциональным символом**.

P называется множеством **предикатных символов**, и если $p \in P$, то p называется $\varphi(p)$ -местным **предикатным символом**.

Язык L считается заданным, если выполнены следующие условия:

(1) задан алфавит Σ языка, т. е. некоторое множество символов – символов языка L . Слова в алфавите Σ , т. е. конечные последовательности символов из Σ , называются **выражениями языка L** ;

(2) определено подмножество \mathcal{F} множества всех выражений языка L ; элементы этого множества \mathcal{F} называются **формулами**.

Если имеется эффективная процедура, позволяющая по данному выражению языка L определить, является ли оно формулой, то говорят, что L – **язык с эффективным понятием формулы**.

Каждой сигнатуре $\tau = \langle C, F, P, \theta, \varphi \rangle$ следующим образом сопоставляется язык первого порядка L_τ .

Алфавит Σ_τ языка L_τ является объединением следующих пяти множеств символов: $V, \Sigma_1, \Sigma_2, \Sigma_3, C, F$ и P , где

(i) $V = \{x_1, x_2, \dots\}$ – счетное множество **предметных** (**индивидных**) **переменных**. Каждый элемент x_i множества V называется **индивидной (предметной) переменной**. Смысл этого названия будет ясен из дальнейшего употребления элементов множества V .

(ii) $\Sigma_1 = \{\neg, \vee, \&, \rightarrow\}$ – множество 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 связками**, причем \neg – **одноместной связкой**, а \vee , $\&$ и \rightarrow – **двуместными связками**.

(iii) множество Σ_2 состоит из двух символов \exists и \forall , называемых соответственно **квантором существования** и **квантором общности**.

(iv) множество Σ_3 состоит из трех технических символов: (– **левая скобка**,) – **правая скобка** и , – **запятая**.

Итак, **алфавит** Σ_τ языка L_τ – это

$$V \cup \Sigma_1 \cup \Sigma_2 \cup \Sigma_3 \cup C \cup F \cup P.$$

Заметим, что символы $\neg, \vee, \&, \rightarrow, \exists$ и \forall называются **логическими** символами языка L_τ , а символы из $C \cup F \cup P$ – **нелогическими**.

Термы языка L_τ . С помощью следующего индуктивного определения выделим некоторое подмножество \mathcal{T}_τ множества всех выражений языка L_τ – множество всех **термов** сигнатуры τ . Понятие терма определяется с помощью следующих трех пунктов:

(i) каждая предметная переменная x_i ($x_i \in V$) и каждая предметная константа c ($c \in C$) является термом;

(ii) если f – n -местный функциональный символ (т. е. $\theta(f) = n$) и t_1, \dots, t_n – термы, то выражение $f(t_1, \dots, t_n)$ тоже терм;

(iii) выражение t языка L_τ является термом тогда и только тогда, когда это следует из пунктов (i) и (ii).

Формулы языка L_τ . Понятие **формулы** языка L_τ определяется следующими четырьмя пунктами:

(i) если t_1, \dots, t_n – термы языка L_τ , а p – n -местный предикатный символ сигнатуры τ (т. е. $p \in P$ и $\varphi(p) = n$), то выражение $p(t_1, \dots, t_n)$ – **формула** языка L_τ , называемая **атомной** или **элементарной формулой**;

(ii) если \mathcal{A} и \mathcal{B} – формулы языка L_τ , то и следующие выражения являются формулами языка L_τ :

$$(\neg \mathcal{A}), (\mathcal{A} \vee \mathcal{B}), (\mathcal{A} \& \mathcal{B}), (\mathcal{A} \rightarrow \mathcal{B});$$

(iii) если \mathcal{A} – формула языка L_τ , а v – индивидная переменная, то $(\exists v)\mathcal{A}$ и $(\forall v)\mathcal{A}$ – формулы языка L_τ ;

(iv) выражение языка L_τ является формулой этого языка тогда и только тогда, когда это следует из пунктов (i) – (iii).

Формула $(\neg \mathcal{A})$ называется **отрицанием** формулы \mathcal{A} и читается ” не \mathcal{A} ” или ” **отрицание \mathcal{A}** ”, формула $(\mathcal{A} \vee \mathcal{B})$ называется ” **дизъюнкцией \mathcal{A}, \mathcal{B}** ” и

читается "дизъюнкция \mathcal{A}, \mathcal{B} " или " \mathcal{A} или \mathcal{B} ", формула $(\mathcal{A} \& \mathcal{B})$ называется "**конъюнкцией** \mathcal{A}, \mathcal{B} " и читается "конъюнкция \mathcal{A}, \mathcal{B} " или " \mathcal{A} и \mathcal{B} ", формула $(\mathcal{A} \rightarrow \mathcal{B})$ называется "**импликацией** \mathcal{A}, \mathcal{B} " и читается " \mathcal{A} влечет \mathcal{B} " или "из \mathcal{A} следует \mathcal{B} ", формула $(\forall v)\mathcal{A}$ читается "для всех v \mathcal{A} ", формула $(\exists v)\mathcal{A}$ читается "существует v такое, что \mathcal{A} ".

Приведенное определение понятия формулы дает следующий способ доказательства теорем о формулах языка L_τ – *доказательство индукцией по формулам*.

Суть его в следующем: чтобы доказать, что каждая формула языка L_τ обладает свойством \mathcal{D} , достаточно показать, что

- (i) каждая элементарная формула языка L_τ обладает свойством \mathcal{D} ;
- (ii) если формулы \mathcal{A} и \mathcal{B} обладают свойством \mathcal{D} , то и формулы

$$(\neg \mathcal{A}), (\mathcal{A} \vee \mathcal{B}), (\mathcal{A} \& \mathcal{B}), (\mathcal{A} \rightarrow \mathcal{A}), (\forall v)\mathcal{A}, (\exists v)\mathcal{A}$$

обладают свойством \mathcal{D} .

Теперь введем понятие **свободного** и **связанного** вхождения переменной x_i в формулу \mathcal{A} . Мы это сделаем индукцией в соответствии с определением понятия формулы:

- (i) если \mathcal{A} – атомная формула, то каждое вхождение каждой входящей в \mathcal{A} переменной x_i называется **свободным** вхождением переменной x_i в формулу \mathcal{A} и никакое вхождение никакой переменной в атомную формулу \mathcal{A} не является **связанным**;
- (ii) если V – вхождение переменной x_i в формулу $(\mathcal{A} \bullet \mathcal{B})$, где

$$\bullet \in \{\vee, \&, \rightarrow\},$$

т. е. $V = X_1 * x_i * X_2$ и $(\mathcal{A} \bullet \mathcal{B}) = X_1 x_i X_2$, то ясно, что существуют такие слова Y и Z , что либо: (1) $X_1 = (Y$ и $\mathcal{A} = Y x_i Z$, либо (2) $X_2 = Z$) и $\mathcal{B} = Y x_i Z$, т. е. рассматриваемое вхождение V переменной x_i в формулу $(\mathcal{A} \bullet \mathcal{B})$ *индуцируется* либо (1) вхождением $Y * x_i * Z$ переменной x_i в \mathcal{A} , либо (2) вхождением $Y * x_i * Z$ переменной x_i в \mathcal{B} . В случае (1) вхождение V переменной x_i в формулу $(\mathcal{A} \bullet \mathcal{B})$ называется **свободным** или **связанным** в зависимости от того, будет ли вхождение $Y * x_i * Z$ переменной x_i в формулу \mathcal{A} свободным или связанным, аналогично в случае (2) вхождение V переменной x_i в формулу $(\mathcal{A} \bullet \mathcal{B})$ называется **свободным** или **связанным** в зависимости от того, будет ли свободным или связанным вхождение $Y * x_i * Z$ переменной x_i в формулу \mathcal{B} .

Коротко сказанное выше означает, что свободными вхождениями переменной x_i в формулу $(\mathcal{A} \bullet \mathcal{B})$ являются те и только те вхождения этой переменной в формулу \mathcal{A} и в \mathcal{B} , которые являются свободными в \mathcal{A} (соответственно в \mathcal{B}).

Если V – вхождение переменной x_i в формулу $(\neg \mathcal{A})$, то найдутся слова X и Y такие, что $V = (\neg X * x_i * Y)$ и $(\neg \mathcal{A}) = (\neg X x_i Y)$, значит, $\mathcal{A} = X x_i Y$. Данное вхождение V переменной x_i в формулу $(\neg \mathcal{A})$ называется **свободным** или **связанным** в зависимости от того, будет ли свободным или связанным вхождение $X * x_i * Y$ переменной x_i в формулу \mathcal{A} .

Если V – вхождение переменной x_i в формулу $(Qx_j)\mathcal{A}$, где $Q \in \{\forall, \exists\}$, то либо $i = j$, и тогда вхождение V называется **связанным** вхождением переменной x_i , либо существуют слова X и Y такие, что

$$V = (Qx_j)X * x_i * Y,$$

тогда $\mathcal{A} = Xx_iY$, и вхождение V переменной x_i в формулу $(Qx_j)\mathcal{A}$ в этом случае называется **свободным** или **связанным** в зависимости от того, будет ли свободным или связанным вхождение $X * x_i * Y$ переменной x_i в формулу \mathcal{A} .

Из сказанного выше видно, что единственный способ избавиться от свободного вхождения переменной x_i в формулу \mathcal{A} – это перейти от \mathcal{A} к $(Qx_i)\mathcal{A}$, где $Q \in \{\forall, \exists\}$. Подчеркнем, что понятия “**свободное**” и “**связанное**” относятся к вхождениям переменной, а не просто к переменной: переменная может иметь и свободные, и связанные вхождения в одну и ту же формулу. Соответствующие примеры читатель построит сам без труда.

Определение 3.1.2. *Формула \mathcal{A} , не содержащая свободных вхождений переменных, называется **предложением**, или **высказыванием**, или **замкнутой** формулой.*

Тем самым язык L_τ первого порядка определен полностью. Отметим, что из сказанного выше ясно, что *каждый язык L_τ первого порядка полностью определяется своими нелогическими символами, т. е. сигнатурой τ .*

Определение 3.1.3. *Если t и a – термы, а v – индивидуальная переменная, то через $a_v[t]$ будем обозначать выражение, полученное из a одновременной заменой каждого вхождения v на t .*

Определение 3.1.4. *Пусть \mathcal{A} – формула, t – терм, v – индивидуальная переменная, тогда через $\mathcal{A}_v[t]$ будем обозначать выражение, полученное из формулы \mathcal{A} одновременной заменой каждого свободного вхождения переменной v на терм t .*

Отметим, что если терм a не содержит вхождений переменной v , то $a_v[t]$ – это сам терм a , аналогично, если формула \mathcal{A} не имеет свободных вхождений переменной v , то $\mathcal{A}_v[t]$ – это сама формула \mathcal{A} .

В качестве несложного, но полезного упражнения предлагается доказать, что при сделанных выше предположениях $a_v[t]$ – терм, а $\mathcal{A}_v[t]$ – формула.

Определение 3.1.5. *Будем говорить, что терм t свободен для переменной x_i в формуле \mathcal{A} (или терм t допустим для подстановки вместо x_i в \mathcal{A}), если для каждой переменной v , входящей в t , в \mathcal{A} нет под слова вида $(Qv)\mathcal{B}$, где $Q \in \{\forall, \exists\}$, \mathcal{B} – формула, содержащая вхождение x_i , которое свободно в \mathcal{A} .*

Условимся, что если в дальнейшем встречается выражение $\mathcal{A}_v[t]$, то \mathcal{A} , v и t таковы, что терм t допустим для подстановки вместо v в \mathcal{A} . Заметим, что это условие заведомо выполняется в каждом из следующих случаев:

- (i) терм t не содержит переменных;
- (ii) никакая переменная терма t не является связанной в \mathcal{A} ;
- (iii) формула \mathcal{A} не имеет связанных вхождений переменных;
- (iv) формула \mathcal{A} не имеет свободных вхождений переменной v .

Введенные понятия естественно обобщаются на случай нескольких переменных.

Определение 3.1.6. Если t, a_1, \dots, a_n – термы, v_1, \dots, v_n – попарно различные переменные, то через $t_{v_1, \dots, v_n}[a_1, \dots, a_n]$ будем обозначать терм, полученный из терма t одновременной заменой всех вхождений v_1 на a_1 , v_2 на a_2, \dots, v_n на a_n .

Определение 3.1.7. Если \mathcal{A} – формула, a_1, \dots, a_n – термы, v_1, \dots, v_n – попарно различные переменные, то через $\mathcal{A}_{v_1, \dots, v_n}[a_1, \dots, a_n]$ будем обозначать формулу, полученную из формулы \mathcal{A} одновременной заменой всех свободных вхождений v_1 на a_1 , v_2 на a_2, \dots, v_n на a_n .

Соглашение. Если в дальнейшем нам встретится выражение

$$\mathcal{A}_{v_1, \dots, v_n}[a_1, \dots, a_n],$$

то будем предполагать, что $\mathcal{A}, v_1, \dots, v_n, a_1, \dots, a_n$ таковы, что при любом i ($i = 1, \dots, n$) терм a_i допустим для подстановки вместо переменной v_i в формулу \mathcal{A} .

Лемма 3.1.1. Пусть все свободные переменные термов a и t содержатся среди x, v_2, \dots, v_n , а r, r_1, \dots, r_n – любые термы. Тогда выполняется следующее равенство

$$(a_x[t])_{x, v_1, \dots, v_n}[r, r_1, \dots, r_n] = a_{x, v_1, \dots, v_n}[t_{x, v_1, \dots, v_n}[r, r_1, \dots, r_n], r_1, \dots, r_n].$$

Доказательство. Проведем индукцию по длине терма a .

Для некоторого сокращения обозначений будем вместо v_1, \dots, v_n писать \bar{v} , вместо r_1, \dots, r_n писать \bar{r} и т. д.

Если терм a имеет длину 1, то либо он является индивидуальной константой и в этом случае правая и левая части доказываемого равенства – это просто сам терм a , либо он является некоторой индивидуальной переменной y .

Если $y \neq x$, то левая часть доказываемого равенства принимает вид

$$(y_x[t])_{x, \bar{v}}[r, \bar{r}],$$

что равно $y_{\bar{v}}[\bar{r}]$, а правая часть принимает вид $y_{\bar{v}}[\bar{r}]$, т. е. доказываемое равенство выполняется.

Если же $y = x$, то левая часть доказываемого равенства принимает вид

$$(x_x[t])_{x, \bar{v}}[r, \bar{r}],$$

что равно $t_{x,\bar{v}}[r, \bar{r}]$, а правая часть принимает вид $x_{x,\bar{v}}[t_{x,\bar{v}}[r, \bar{r}], \bar{r}]$, что равно $t_{x,\bar{v}}[r, \bar{r}]$, т. е. доказываемое равенство выполняется.

Завершается доказательство стандартным образом: предполагаем, что доказываемое равенство верно для всех термов длины меньшей k ($k > 1$), и докажем его справедливость для термов длины k .

Терм t имеет вид

$$f(t_1, \dots, t_n),$$

где f — n -местный функциональный символ, а t_1, \dots, t_n — термы.

Преобразуем отдельно левую и правую части доказываемого равенства

$$(a_x[t])_{x,\bar{v}}[r, \bar{r}] = (f(t_1, \dots, t_n)_x[t])_{x,\bar{v}}[r, \bar{r}] = f(((t_1)_x[t])_{x,\bar{v}}[r, \bar{r}], \dots, ((t_n)_x[t])_{x,\bar{v}}[r, \bar{r}]).$$

Правая же часть доказываемого равенства преобразуется следующим образом:

$$a_{x,\bar{v}}[t_{x,\bar{v}}[r, \bar{r}], \bar{r}] = f(t_1, \dots, t_n)_{x,\bar{v}}[t_{x,\bar{v}}[r, \bar{r}], \bar{r}] = f(((t_1)_{x,\bar{v}}[t_{x,\bar{v}}[r, \bar{r}], \bar{r}], \dots, (t_n)_{x,\bar{v}}[t_{x,\bar{v}}[r, \bar{r}], \bar{r}])$$

и остается заметить, что по индуктивному предположению при любом i выполняется равенство

$$((t_i)_x[t])_{x,\bar{v}}[r, \bar{r}] = (t_i)_{x,\bar{v}}[t_{x,\bar{v}}[r, \bar{r}], \bar{r}].$$

□

Лемма 3.1.2. Пусть все свободные переменные формулы \mathcal{A} и терма t содержатся среди x, v_2, \dots, v_n , а r, r_1, \dots, r_n — любые термы. Тогда если терм t допустим для подстановки вместо переменной x в формулу \mathcal{A} , то выполняется следующее равенство

$$(\mathcal{A}_x[t])_{x,v_1,\dots,v_n}[r, r_1, \dots, r_n] = \mathcal{A}_{x,v_1,\dots,v_n}[t_{x,v_1,\dots,v_n}[r, r_1, \dots, r_n], r_1, \dots, r_n].$$

Доказательство. Проведем индукцию по формулам.

1) Если \mathcal{A} — атомная формула, то \mathcal{A} имеет вид

$$p(t_1, \dots, t_n),$$

где p — n -местный предикатный символ, а t_1, \dots, t_n — термы.

Тогда, используя введенные в ходе доказательства леммы 3.1.1 обозначения, получаем, что левая часть доказываемого равенства равна

$$(p(t_1, \dots, t_n)_x[t])_{x,\bar{v}}[r, \bar{r}],$$

что равно

$$p(((t_1)_x[t])_{x,\bar{v}}[r, \bar{r}], \dots, ((t_1)_x[t])_{x,\bar{v}}[r, \bar{r}]).$$

Правая же часть доказываемого равенства равна

$$p(t_1, \dots, t_n)_{x,\bar{v}}[t_{x,\bar{v}}[r, \bar{r}], \bar{r}],$$

что равно

$$p((t_1)_{x,\bar{v}}[t_{x,\bar{v}}[r, \bar{r}], \bar{r}], \dots, (t_n)_{x,\bar{v}}[t_{x,\bar{v}}[r, \bar{r}], \bar{r}]).$$

И для завершения рассмотрения этого случая остается применить лемму 3.1.1.

2) Покажем, что если утверждение верно для формулы \mathcal{A} , то оно верно и для формулы $(\neg \mathcal{A})$.

$$\begin{aligned} ((\neg \mathcal{A})_x[t])_{x,\bar{v}}[r, \bar{r}] &= \neg (\mathcal{A}_x[t]_{x,\bar{v}}[r, \bar{r}]) = \\ &= \neg (\mathcal{A}_{x,\bar{v}}[t_{x,\bar{v}}[r, \bar{r}], \bar{r}]) = (\neg \mathcal{A})_{x,\bar{v}}[t_{x,\bar{v}}[r, \bar{r}], \bar{r}]. \end{aligned}$$

3) Совершенно аналогично доказывается, что если доказываемое равенство верно для формул \mathcal{A} и \mathcal{B} , то оно верно и для формул $(\mathcal{A} \bullet \mathcal{B})$, где $\bullet \in \{ \vee, \&, \rightarrow \}$.

4) Остается показать, что если равенство выполняется для формулы \mathcal{A} , то оно выполняется и для формулы $(Qy)\mathcal{A}$, где $Q \in \{ \exists, \forall \}$.

Рассмотрим три случая.

i) y есть x . В этом случае сначала преобразуем левую часть доказываемого равенства.

$$(\mathcal{A}_x[t])_{x,\bar{v}}[r, \bar{r}] = \mathcal{A}_{x,\bar{v}}[r, \bar{r}] = \mathcal{A}_{\bar{v}}[\bar{r}].$$

Теперь преобразуем правую часть доказываемого равенства.

$$\mathcal{A}_{x,\bar{v}}[t_{x,\bar{v}}[r, \bar{r}], \bar{r}] = \mathcal{A}_{\bar{v}}[\bar{r}].$$

ii) y есть некоторая переменная v_i . Без ограничения общности можно считать, что y — это переменная v_n . Так как по предположению терм t допустим для подстановки вместо x в формулу \mathcal{A} , то в этом случае переменная v_i не входит в терм t , поэтому

$$t_{x,v_1,\dots,v_n}[r, r_1, \dots, r_n] = t_{x,v_1,\dots,v_{n-1}}[r, r_1, \dots, r_{n-1}].$$

Преобразуем левую часть доказываемого равенства

$$\begin{aligned} (\mathcal{A}_x[t])_{x,v_1,\dots,v_n}[r, r_1, \dots, r_n] &= \\ &= (\mathcal{A}_x[t])_{x,v_1,\dots,v_{n-1}}[r, r_1, \dots, r_{n-1}]. \end{aligned}$$

Затем преобразуем правую часть доказываемого равенства

$$\begin{aligned} \mathcal{A}_{x,v_1,\dots,v_n}[t_{x,v_1,\dots,v_n}[r, r_1, \dots, r_n], r_1, \dots, r_n] &= \\ \mathcal{A}_{x,v_1,\dots,v_{n-1}}[t_{x,v_1,\dots,v_{n-1}}[r, r_1, \dots, r_{n-1}], r_1, \dots, r_{n-1}]. \end{aligned}$$

Поэтому доказываемое равенство в рассматриваемом случае принимает вид

$$(\mathcal{A}_x[t])_{x,v_1,\dots,v_{n-1}}[r, r_1, \dots, r_{n-1}] = \mathcal{A}_{x,v_1,\dots,v_{n-1}}[t_{x,v_1,\dots,v_{n-1}}[r, r_1, \dots, r_{n-1}], r_1, \dots, r_{n-1}].$$

Повторив это рассуждение нужное число раз, мы рассматриваемый случай ii) сведем либо к уже рассмотренному случаю i), либо к следующему случаю iii) переменная y отлична от переменных x, v_1, \dots, v_n . В этом случае, используя индуктивное предположение, получаем

$$\begin{aligned} (\mathcal{A}_x[t])_{x,\bar{v}}[r, \bar{r}] &= (((Qy)\mathcal{B})_x[t])_{x,\bar{v}}[r, \bar{r}] = \\ &= ((Qy)\mathcal{B}_x[t])_{x,\bar{v}}[r, \bar{r}] = (Qy)\mathcal{B}_{x,\bar{v}}[t_{x,\bar{v}}[r, \bar{r}], \bar{r}] = \\ &= ((Qy)\mathcal{B})_{x,\bar{v}}[t_{x,\bar{v}}[r, \bar{r}], \bar{r}] = \mathcal{A}_{x,\bar{v}}[t_{x,\bar{v}}[r, \bar{r}], \bar{r}]. \end{aligned}$$

□

Условимся в дальнейшем вместо $(\mathcal{A} * \mathcal{B})$, где $*$ $\in \{\vee, \&, \rightarrow\}$, писать просто $\mathcal{A} * \mathcal{B}$.

Введем некоторые соглашения, по которым мы будем опускать скобки.

(i) Опускаем скобки, когда они не являются необходимыми для определения группировки символов, например, будем писать $a = b \rightarrow c = d$ вместо $((a = b) \rightarrow (c = d))$.

(ii) Соглашение *правого сочетания отсутствующих скобок*. Это означает, что $\mathcal{A} * \mathcal{B} * \mathcal{C}$, где $*$ $\in \{\vee, \&, \rightarrow\}$, следует читать как $(\mathcal{A} * (\mathcal{B} * \mathcal{C}))$; $\mathcal{A} * \mathcal{B} * \mathcal{C} * \mathcal{D}$ следует читать как $(\mathcal{A} * (\mathcal{B} * (\mathcal{C} * \mathcal{D})))$ и т. д.

Все рассмотренные выше понятия составляют *синтаксис* языка L_τ .

3.2. Логика предикатов

В этом параграфе мы приступаем к изучению другой стороны языка L_τ – его *семантики*.

Введем одно из основных понятий этого раздела – понятие **интерпретации** языка L_τ .

Для задания **интерпретации** I языка L_τ сигнатуры $\tau = \langle C, F, P, \theta, \varphi \rangle$ необходимо:

- (i) задать непустое множество A , называемое *основным множеством* (универсумом или носителем) **интерпретации** I ;
- (ii) задать отображение $I : C \rightarrow A$ множества C индивидуальных констант во множество A ;
- (iii) задать отображение I множества F функциональных символов во множество алгебраических операций на множестве A такое, что если $f \in F$, то $I(f)$ – это $\theta(f)$ -местная алгебраическая операция на A ;

(iv) задать отображение I множества P предикатных символов во множество предикатов, определенных на A , такое, что если $p \in P$, то $\gamma_2(p)$ – это $\varphi(p)$ -местный предикат на A .

Сделаем некоторые пояснения.

$I(f)$ – это отображение множества $A^{\theta(f)}$ во множество A .

Алгебраическая операция $I(f)$ иногда обозначается через f^I .

$I(p)$ – это отображение множества $A^{\varphi(p)}$ во множество $B = \{И, Л\}$.

Предикат $I(p)$ иногда обозначается через p^I .

Если $c \in C$, то $I(c)$ называется *выделенным элементом* множества A .

Элемент $I(c)$ множества A иногда обозначается через c^I .

Чтобы иметь возможность формулировать утверждения об элементах множества A , расширим сигнатуру τ языка первого порядка L_τ .

Для каждого индивида $a \in A$ мы выберем новую константу \bar{a} и назовем ее **именем** индивида a . При этом придерживаемся соглашения: если $\bar{a} = \bar{b}$, то $a = b$, т. е. *для разных индивидов выбираются разные имена*.

Обозначим через $\tau(A)$ сигнатуру, полученную из сигнатуры τ добавлением к множеству C индивидных констант сигнатуры τ множества \bar{A} всех *имен индивидов* из A , т. е.

$$\tau(A) = \langle C \cup A, F, P, \theta, \varphi \rangle.$$

Язык $L_{\tau(A)}$ первого порядка сигнатуры $\tau(A)$ будем обозначать через $L_\tau(A)$ или просто через $L(A)$ и говорить, что он *получен из языка L добавлением всех имен индивидов из A* .

Будем говорить, что терм t *свободен от переменных* (или t – *замкнутый терм*), если он не содержит переменных.

Пусть t – свободный от переменных терм языка $L(A)$.

Индукцией по построению терма t определим индивид (элемент) $I(t)$ из A , который *будет соответствовать терму t* при интерпретации I .

Так как терм t свободен от переменных, то он не может быть переменной.

(i) Если t – константа сигнатуры $\tau(A)$, то либо t – константа сигнатуры τ , и тогда полагаем

$$I(t) \equiv t^I,$$

т. е. это индивид из основного множества A системы \mathcal{A} , который соответствует t ; либо t – имя \bar{a} некоторого индивида a из A , в этом случае полагаем

$$I(t) \equiv a.$$

(ii) Если терм t имеет вид $f(t_1, \dots, t_n)$, где f – n -местный функциональный символ сигнатуры τ , то полагаем

$$I(t) \equiv f^I(I(t_1), \dots, I(t_n)).$$

Для каждой *замкнутой* (т. е. не содержащей свободных вхождений переменных) формулы Φ языка $L(A)$ определим *истинностное значение* формулы

Φ в интерпретации I индукцией по построению формулы Φ (т. е. сопоставим Φ значение **И** или **Л**).

Используем знак \iff как сокращение фразы "... тогда и только тогда, когда ...".

(i) Пусть Φ – атомная формула вида $p(t_1, \dots, t_n)$, где p – n -местный предикатный символ сигнатуры τ , а t_1, \dots, t_n – свободные от переменных термы сигнатуры $\tau(A)$, тогда полагаем

$$I(\Phi) = \text{И} \iff p^A(I(t_1), \dots, I(t_n)) = \text{И}.$$

(ii) Теперь если Φ и Ψ – замкнутые формулы, то полагаем

$$\begin{aligned} I((\neg\Phi)) &= \text{И} \iff I(\Phi) = \text{Л} \\ I((\Phi \vee \Psi)) &= \text{И} \iff I(\Phi) = \text{И} \text{ или } I(\Psi) = \text{И}, \\ I((\Phi \& \Psi)) &= \text{И} \iff I(\Phi) = \text{И} \text{ и } I(\Psi) = \text{И}, \\ I((\Phi \rightarrow \Psi)) &= \text{Л} \iff I(\Phi) = \text{И} \text{ и } I(\Psi) = \text{Л}. \end{aligned}$$

(iii) Если Φ – формула, не содержащая свободных переменных, отличных от x , то полагаем

$$I((\exists x)\Phi) = \text{И} \iff I(\Phi_x[\bar{a}]) = \text{И} \text{ для имени } \bar{a} \text{ некоторого индивида } a \text{ из } A,$$

$$I((\forall x)\Phi) = \text{И} \iff I(\Phi_x[\bar{a}]) = \text{И} \text{ для имени } \bar{a} \text{ любого индивида } a \text{ из } A.$$

Заметим, что если формула Φ вообще не содержит свободных переменных, то $\Phi_x[\bar{a}]$ – это просто сама формула Φ .

Пусть Φ – произвольная формула языка L , а v_1, \dots, v_n – все ее свободные переменные. Если $\bar{a}_1, \dots, \bar{a}_n$ – имена произвольных индивидов a_1, \dots, a_n из A , то формулу

$$\Phi_{v_1, \dots, v_n}[\bar{a}_1, \dots, \bar{a}_n]$$

будем называть *A-частным случаем* формулы Φ .

Определение 3.2.1. Произвольная формула Φ языка L называется **истинной в интерпретации** I , если для любого *A-частного случая* Φ' формулы Φ : $I(\Phi') = \text{И}$.

В частности, если Φ – замкнутая формула, то легко понять, что

$$\Phi \text{ истинна в интерпретации } I \iff I(\Phi) = \text{И}.$$

Будем считать, что множество индивидуальных переменных упорядочено, и этот порядок назовем *алфавитным*.

Если формула Φ содержит лишь свободные переменные v_1, \dots, v_n (в алфавитном порядке) ($n \geq 0$), то \forall -замыканием формулы Φ назовем формулу вида $(\forall v_1) \dots (\forall v_n) \Phi$.

\forall -замыкание формулы Φ обозначим через $\forall \Phi$.

Ясно, что $\forall \Phi$ – замкнутая формула, и если Φ – замкнутая формула, то $\forall \Phi$ – это просто Φ .

В качестве простого упражнения предлагается доказать, что

формула Φ языка L **истинна в интерпретации** I тогда и только тогда, когда $I(\forall \Phi) = \text{И}$.

Определение 3.2.2. Если формула Φ языка L истинна в каждой интерпретации I этого языка, то она называется **тождественно истинной** или **общезначимой**.

Замечание. Запись $\models \Phi$ будет служить сокращением для утверждения “формула Φ является тождественно истинной.”

Пусть Φ – формула **Логики Высказываний**, все пропозициональные переменные которой содержатся среди A_1, \dots, A_n , а Φ_1, \dots, Φ_n – произвольные формулы **Логики Предикатов**. Индукцией по построению формул нетрудно доказать, что $\Phi_{A_1, \dots, A_n}[\Phi_1, \dots, \Phi_n]$ – формула **Логики Предикатов**. Она называется *формулой, полученной из формулы Логики Высказываний Φ заменой пропозициональных переменных A_1, \dots, A_n на формулы Логики Предикатов Φ_1, \dots, Φ_n* .

Индукцией по построению формул легко доказывается следующая теорема. Доказательство предоставляется провести читателю в качестве полезного упражнения.

Теорема 3.2.1. Если Φ – тождественно истинная формула **Логики Высказываний**, все пропозициональные переменные которой содержатся среди A_1, \dots, A_n , а Φ_1, \dots, Φ_n – произвольные формулы **Логики Предикатов**, то $\Phi_{A_1, \dots, A_n}[\Phi_1, \dots, \Phi_n]$ – тождественно истинная формула **Логики Предикатов**.

Определение 3.2.3. Формула Φ языка L_τ называется **выполнимой**, если существует интерпретация, в которой эта формула истинна.

Определение 3.2.4. Множество формул Γ языка L_τ называется **совместным**, если существует интерпретация, в которой все формулы из этого множества истинны.

Замечание. Для произвольного множества формул Γ языка L_τ и для любой интерпретации I запись

$$I(\Gamma) = \text{И}$$

будет служить сокращением для утверждения “все формулы множества Γ истинны в интерпретации I .”

Определение 3.2.5. Формулы Φ и Ψ языка L называются **эквивалентными** или **равносильными**, если формула

$$(\Phi \rightarrow \Psi) \& (\Psi \rightarrow \Phi)$$

является тождественно истинной.

В качестве упражнения читателю предлагается доказать, что если переменная x не входит свободно в формулу Φ , то равносильны формулы

$$\begin{aligned} &(\exists x)\Phi \text{ и } \Phi \quad \text{и} \quad (\forall x)\Phi \text{ и } \Phi; \\ &(\exists x)(\Psi \vee \Phi) \quad \text{и} \quad (\exists x)\Psi \vee \Phi; \\ &(\exists x)(\Phi \vee \Psi) \quad \text{и} \quad \Phi \vee (\exists x)\Psi; \\ &(\forall x)(\Psi \vee \Phi) \quad \text{и} \quad (\forall x)\Psi \vee \Phi; \\ &(\forall x)(\Phi \vee \Psi) \quad \text{и} \quad \Phi \vee (\forall x)\Psi; \\ &(\exists x)(\Psi \rightarrow \Phi) \quad \text{и} \quad (\forall x)\Psi \rightarrow \Phi; \\ &(\exists x)(\Phi \rightarrow \Psi) \quad \text{и} \quad \Phi \rightarrow (\exists x)\Psi; \\ &(\forall x)(\Psi \rightarrow \Phi) \quad \text{и} \quad (\exists x)\Psi \rightarrow \Phi; \\ &(\forall x)(\Phi \rightarrow \Psi) \quad \text{и} \quad \Phi \vee (\forall x)\Psi. \end{aligned}$$

В качестве полезного упражнения предлагается доказать равносильность формул

$$\begin{aligned} &(\Phi \rightarrow \Psi) \quad \text{и} \quad (\neg\Phi \vee \Psi); \\ &\neg(\Phi \vee \Psi) \quad \text{и} \quad (\neg\Phi \& \neg\Psi); \\ &\neg(\Phi \& \Psi) \quad \text{и} \quad (\neg\Phi \vee \neg\Psi); \\ &(\forall x)(\Phi \& \Psi) \quad \text{и} \quad ((\forall x)\Phi \& (\forall x)\Psi); \\ &(\exists x)(\Phi \vee \Psi) \quad \text{и} \quad ((\exists x)\Phi \vee (\exists x)\Psi). \end{aligned}$$

Определение 3.2.6. Формула \mathcal{A} языка L_τ называется **логическим следствием** множества формул Γ этого языка L_τ , если для любой интерпретации φ , в которой все формулы из этого множества Γ истинны, истинна и формула \mathcal{A} .

Замечание. Запись $\Gamma \models \mathcal{A}$ будет служить сокращением для утверждения "формула \mathcal{A} является **логическим следствием** множества формул Γ ."

Как следствие объединения и взаимного проникновения друг в друга алгебры и математической логики во второй половине XX века бурно развивалась пограничная между алгеброй и математической логикой дисциплина, получившая название *теория моделей*. Одним из основных понятий *теории моделей*

является понятие *алгебраической системы*. Оно в определенном смысле равносильно уже введенному нами понятию *интерпретация*. Однако в некоторых ситуациях язык теории моделей является более удобным, чем язык интерпретаций. Если мы начинаем с языка L_τ сигнатуры τ , то удобно говорить об его интерпретации I . Если же мы начинаем с некоторой алгебраической системы, то строим язык для описания ее свойств. Эти два подхода эквивалентны, но в одном из них в определенной мере доминирует математическая логика, а в другом – алгебра.

Определение 3.2.7. *Алгебраической системой \mathcal{A} сигнатуры*

$$\tau = \langle C, F, P, \theta, \varphi \rangle$$

называется пятерка

$$\langle A, \tau, \gamma_1, \gamma_2, \gamma_3 \rangle,$$

где

- (i) A – непустое множество, называемое основным множеством (универсумом или носителем) системы \mathcal{A} ;
- (ii) τ – сигнатура;
- (iii) γ_1 – отображение множества F функциональных символов во множество алгебраических операций на множестве A , причем, если $f \in F$, то $\gamma_1(f)$ – это $\theta(f)$ -местная алгебраическая операция на A ;
- (iv) γ_2 – отображение множества P предикатных символов во множество предикатов, определенных на A , такое, что если $p \in P$, то $\gamma_2(p)$ – это $\varphi(p)$ -местный предикат на A ;
- (v) γ_3 – отображение множества C в A .

Сделаем некоторые пояснения.

$\gamma_1(f)$ – это отображение множества $A^{\theta(f)}$ во множество A .

Алгебраическую операцию $\gamma_1(f)$ будем обозначать через f^A .

$\gamma_2(p)$ – это отображение множества $A^{\varphi(p)}$ во множество $B = \{И, Л\}$.

Предикат $\gamma_2(p)$ будем обозначать через p^A .

Если $c \in C$, то $\gamma_3(c)$ называется *выделенным элементом* множества A или системы \mathcal{A} .

Элемент $\gamma_3(c)$ множества A будем обозначать через c^A .

Если множество C пусто, то говорят, что \mathcal{A} – *система без выделенных элементов*.

Если пусто множество P , то алгебраическая система \mathcal{A} называется *универсальной алгеброй* или просто *алгеброй*.

Если же пусто множество F , то система \mathcal{A} называется *моделью*.

Пусть τ – сигнатура, L_τ – язык первого порядка сигнатуры τ , а \mathcal{A} – алгебраическая система сигнатуры τ , тогда \mathcal{A} называется также *структурой для языка L_τ* .

Как и в случае интерпретации, для каждого индивида $a \in A$ мы выбираем новую константу \bar{a} , называемую *именем* индивида a , при этом считаем, что если $\bar{a} = \bar{b}$, то $a = b$, т. е. *для разных индивидов выбираются разные имена*.

Как и в случае интерпретации, через $\tau(A)$ мы обозначаем сигнатуру, полученную из сигнатуры τ добавлением к множеству S индивидуальных констант сигнатуры τ множества \bar{A} всех имен индивидов из A , а через $L_\tau(A)$ или просто через $L(A)$ – язык $L_{\tau(A)}$ первого порядка сигнатуры $\tau(A)$ говорим, что он получен из языка L добавлением всех имен индивидов из A .

Будем говорить, что терм t *свободен от переменных* (или t – *замкнутый терм*), если он не содержит переменных.

Пусть t – свободный от переменных терм языка $L(A)$.

Индукцией по построению терма t определим индивид $\mathcal{A}(t)$ из A , который *будет соответствовать терму t* .

Так как терм t свободен от переменных, то он не может быть переменной.

(i) Если t – константа сигнатуры $\tau(A)$, то либо t – константа сигнатуры τ , и тогда полагаем

$$\mathcal{A}(t) \equiv t^A,$$

т. е. это индивид из основного множества A системы \mathcal{A} , который соответствует t ; либо t – имя \bar{a} некоторого индивида a из A , в этом случае полагаем

$$\mathcal{A}(t) \equiv a.$$

(ii) Если терм t имеет вид $f(t_1, \dots, t_n)$, где f – n -местный функциональный символ сигнатуры τ , то полагаем

$$\mathcal{A}(t) \equiv f^A(\mathcal{A}(t_1), \dots, \mathcal{A}(t_n)).$$

Для каждой *замкнутой* (т. е. не содержащей свободных вхождений переменных) формулы Φ языка $L(A)$ определим *истинностное значение* $\mathcal{A}(\Phi)$ формулы Φ в системе \mathcal{A} индукцией по построению формулы Φ (т. е. сопоставим Φ значение $\mathcal{A}(\Phi)$, равное И или Л).

Условимся писать:

$$\begin{aligned} \mathcal{A} \models \Phi, & \text{ если } \mathcal{A}(\Phi) = \text{И}, \\ \mathcal{A} \not\models \Phi, & \text{ если } \mathcal{A}(\Phi) = \text{Л}. \end{aligned}$$

Кроме того, используем знак \iff как сокращение фразы ”... тогда и только тогда, когда ...”.

(i) Пусть Φ – атомная формула вида $p(t_1, \dots, t_n)$, где p – n -местный предикатный символ сигнатуры τ , а t_1, \dots, t_n – свободные от переменных термы сигнатуры $\tau(A)$, тогда полагаем

$$\mathcal{A} \models \Phi \iff p^A(\mathcal{A}(t_1), \dots, \mathcal{A}(t_n)) = \text{И}.$$

(ii) Теперь, если Φ и Ψ – замкнутые формулы, то полагаем

$$\begin{aligned}\mathcal{A} \models (\neg\Phi) &\iff \mathcal{A} \not\models \Phi, \\ \mathcal{A} \models (\Phi \vee \Psi) &\iff \mathcal{A} \models \Phi \text{ или } \mathcal{A} \models \Psi, \\ \mathcal{A} \models (\Phi \&\Psi) &\iff \mathcal{A} \models \Phi \text{ и } \mathcal{A} \models \Psi, \\ \mathcal{A} \not\models (\Phi \rightarrow \Psi) &\iff \mathcal{A} \models \Phi \text{ и } \mathcal{A} \not\models \Psi.\end{aligned}$$

(iii) Если Φ – формула, не содержащая свободных переменных, отличных от x , то полагаем

$$\mathcal{A} \models (\exists x)\Phi \iff \mathcal{A} \models \Phi_x[\bar{a}] \text{ для имени } \bar{a} \text{ некоторого индивида } a \text{ из } A,$$

$$\mathcal{A} \models (\forall x)\Phi \iff \mathcal{A} \models \Phi_x[\bar{a}] \text{ для имени } \bar{a} \text{ любого индивида } a \text{ из } A.$$

Заметим, что если формула Φ вообще не содержит свободных переменных, то $\Phi_x[\bar{a}]$ – это просто сама формула Φ .

Пусть Φ – произвольная формула языка L , а v_1, \dots, v_n – все ее свободные переменные. Если $\bar{a}_1, \dots, \bar{a}_n$ – имена произвольных индивидов a_1, \dots, a_n из A , то формулу

$$\Phi_{v_1, \dots, v_n}[\bar{a}_1, \dots, \bar{a}_n]$$

будем называть \mathcal{A} -частным случаем формулы Φ .

Определение 3.2.8. Произвольная формула Φ языка L называется **истинной** в \mathcal{A} , если для любого \mathcal{A} -частного случая Φ' формулы Φ $\mathcal{A} \models \Phi'$.

В частности, если Φ – замкнутая формула, то легко понять, что

$$\Phi \text{ истинна в } \mathcal{A} \iff \mathcal{A} \models \Phi.$$

Напомним, что через $\forall\Phi$ обозначается \forall -замыкание формулы Φ .

В качестве простого упражнения предлагается доказать, что формула Φ языка L истинна в \mathcal{A} тогда и только тогда, когда $\mathcal{A} \models \forall\Phi$.

Докажем следующую важную лемму, утверждающую, что формула $\Phi_x[t]$ ”утверждает” про индивид, обозначенный через t то же самое, что формула Φ ”утверждает” про индивид, обозначенный через x . Точнее, имеет место

Лемма 3.2.1. Пусть \mathcal{A} – структура для языка L , t – свободный от переменных терм языка L , $\bar{\mathcal{A}}(t)$ – имя индивида $\mathcal{A}(t)$ из A , соответствующего терму t .

Если r – терм языка $L(A)$, не содержащий переменных, отличных от x , то

$$\mathcal{A}(r_x[t]) = \mathcal{A}(r_x[\overline{\mathcal{A}(t)}]). \quad (1)$$

Если формула Φ не содержит свободных переменных, отличных от x , то

$$\mathcal{A}(\Phi_x[t]) = \mathcal{A}(\Phi_x[\overline{\mathcal{A}(t)}]). \quad (2)$$

Д о к а з а т е л ь с т в о. Первое утверждение докажем индукцией по построению терма r .

(i) Если r – переменная, то это x , тогда

$$\begin{aligned} r_x[\overline{\mathcal{A}(t)}] &= \overline{\mathcal{A}(t)}, \\ r_x[t] &= t, \\ \mathcal{A}(\overline{\mathcal{A}(t)}) &= \mathcal{A}(t), \end{aligned}$$

т. е. равенство (1) выполнено.

Если r – константа из $\tau(A)$, то

$$r_x[\overline{\mathcal{A}(t)}] = r, \quad r_x[t] = r,$$

поэтому равенство (1) опять выполнено.

(ii) r имеет вид $f(t_1, \dots, t_n)$, где f – n -местный функциональный символ сигнатуры τ , а t_1, \dots, t_n – термы языка $L(A)$.

Тогда, используя индуктивное предположение и соответствующие определения, получаем

$$\begin{aligned} \mathcal{A}(r_x[t]) &= \mathcal{A}(f(t_{1x}[t], \dots, t_{nx}[t])) = \\ &= f^{\mathcal{A}}(\mathcal{A}(t_{1x}[t]), \dots, \mathcal{A}(t_{nx}[t])) = \\ &= f^{\mathcal{A}}(\mathcal{A}(t_{1x}[\overline{\mathcal{A}(t)}]), \dots, \mathcal{A}(t_{nx}[\overline{\mathcal{A}(t)}])) = \\ &= \mathcal{A}(f(t_{1x}[\overline{\mathcal{A}(t)}], \dots, t_{nx}[\overline{\mathcal{A}(t)}])) = \\ &= \mathcal{A}(r_x[\overline{\mathcal{A}(t)}]). \end{aligned}$$

Равенство (2) докажем индукцией по построению формулы Φ .

(i) Если Φ – атомная формула вида

$$p(t_1, \dots, t_n),$$

где p – n -местный предикатный символ сигнатуры τ , отличный от $=$, а t_1, \dots, t_n – термы языка $L(A)$, тогда

$$\begin{aligned} \mathcal{A}(\Phi_x[t]) &= \mathcal{A}(p(t_{1x}[t], \dots, t_{nx}[t])) = \\ &= p^{\mathcal{A}}(\mathcal{A}(t_{1x}[t]), \dots, \mathcal{A}(t_{nx}[t])) = \\ &= p^{\mathcal{A}}(\mathcal{A}(t_{1x}[\overline{\mathcal{A}(t)}]), \dots, \mathcal{A}(t_{nx}[\overline{\mathcal{A}(t)}])) = \\ &= \mathcal{A}(p(t_{1x}[\overline{\mathcal{A}(t)}], \dots, t_{nx}[\overline{\mathcal{A}(t)}])) = \mathcal{A}(\Phi_x[\overline{\mathcal{A}(t)}]). \end{aligned}$$

(ii) Рассмотрим функции

$$H_{\neg}(x), H_{\rightarrow}(x, y), H_{\vee}(x, y), H_{\&}(x, y),$$

определенные на множестве $\{И, Л\}$ и принимающие значения в этом же множестве, такие что

$$\begin{aligned} H_{\neg}(И) &= Л, & H_{\neg}(Л) &= И; \\ H_{\rightarrow}(И, И) &= H_{\rightarrow}(Л, И) = H_{\rightarrow}(Л, Л) = И, & H_{\rightarrow}(И, Л) &= Л; \\ H_{\vee}(И, И) &= H_{\vee}(Л, И) = H_{\vee}(И, Л) = И, & H_{\vee}(Л, Л) &= Л; \\ H_{\&}(И, И) &= И, & H_{\&}(Л, И) &= H_{\&}(И, Л) = H_{\&}(Л, Л) = Л. \end{aligned}$$

Для произвольного терма t выполняется равенство

$$(\neg\Phi)_x[t] \equiv \neg(\Phi_x[t]),$$

поэтому

$$\begin{aligned} \mathcal{A}((\neg\Phi)_x[t]) &= \mathcal{A}(\neg(\Phi_x[t])) = \\ &= H_{\neg}(\mathcal{A}(\Phi_x[t])) = H_{\neg}(\mathcal{A}(\Phi_x[\overline{\mathcal{A}(t)}])) = \\ &= \mathcal{A}(\neg\Phi_x[\overline{\mathcal{A}(t)}]) = \mathcal{A}((\neg\Phi)_x[\overline{\mathcal{A}(t)}]). \end{aligned}$$

Пусть $*$ $\in \{\vee, \&, \rightarrow\}$.

Тогда

$$\begin{aligned} \mathcal{A}((\Phi * \Psi)_x[t]) &= \mathcal{A}(\Phi_x[t] * \Psi_x[t]) = \\ &= H_*(\mathcal{A}(\Phi_x[t]), \mathcal{A}(\Psi_x[t])) = \\ &= H_*(\mathcal{A}(\Phi_x[\overline{\mathcal{A}(t)}]), \mathcal{A}(\Psi_x[\overline{\mathcal{A}(t)}])) = \\ &= \mathcal{A}(\Phi_x[\overline{\mathcal{A}(t)}] * \Psi_x[\overline{\mathcal{A}(t)}]) = \mathcal{A}((\Phi * \Psi)_x[\overline{\mathcal{A}(t)}]). \end{aligned}$$

(iii) Пусть теперь формула Φ имеет вид $(\exists y)\Psi$.

Тогда, если y — это x , то

$$\Phi_x[t] \equiv \Phi, \quad \Phi_x[\overline{\mathcal{A}(t)}] \equiv \Phi,$$

и, конечно, равенство (2) выполнено.

Пусть теперь $y \neq x$.

Тогда

$$\begin{aligned} ((\exists y)\Psi)_x[t] &\equiv (\exists y)\Psi_x[t], \\ ((\exists y)\Psi)_x[\overline{\mathcal{A}(t)}] &\equiv (\exists y)\Psi_x[\overline{\mathcal{A}(t)}]. \end{aligned}$$

Если

$$\mathcal{A} \models \Phi_x[t],$$

т. е.

$$\mathcal{A} \models ((\exists y)\Psi)_x[t],$$

а значит,

$$\mathcal{A} \models (\exists y)\Psi_x[t],$$

то для некоторого имени \bar{a} индивида $a \in A$

$$\mathcal{A} \models (\Psi_x[t])_y[\bar{a}].$$

Так как термы t и \bar{a} свободны от переменных и $x \neq y$, то

$$(\Psi_x[t])_y[\bar{a}] = (\Psi_y[\bar{a}])_x[t],$$

поэтому

$$\mathcal{A} \models (\Psi_y[\bar{a}])_x[t].$$

Тогда по индуктивному предположению

$$\mathcal{A} \models (\Psi_y[\bar{a}])_x[\overline{\mathcal{A}(t)}].$$

Так как

$$(\Psi_y[\bar{a}])_x[\overline{\mathcal{A}(t)}] = (\Psi_x[\overline{\mathcal{A}(t)}])_y[\bar{a}],$$

то

$$\mathcal{A} \models (\Psi_x[\overline{\mathcal{A}(t)}])_y[\bar{a}].$$

Поэтому

$$\mathcal{A} \models (\exists y)\Psi_x[\overline{\mathcal{A}(t)}],$$

значит,

$$\mathcal{A} \models ((\exists y)\Psi)_x[\overline{\mathcal{A}(t)}],$$

т. е.

$$\mathcal{A} \models \Phi_x[\overline{\mathcal{A}(t)}].$$

Аналогичное рассуждение показывает, что если

$$\mathcal{A} \models \Phi_x[\overline{\mathcal{A}(t)}],$$

то

$$\mathcal{A} \models \Phi_x[t].$$

(iv) Если формула Φ имеет вид $(\forall y)\Psi$, то аналогичное рассуждение показывает, что

$$\mathcal{A} \models \Phi_x[t] \iff \mathcal{A} \models \Phi_x[\overline{\mathcal{A}(t)}].$$

Тем самым лемма 3.2.1 доказана. \square

Нашей ближайшей целью будет изучение одного из основных понятий логики предикатов – понятия **логического следствия**.

Напомним, что формула Φ языка L называется **логическим следствием** множества формул Γ языка L , если Φ истинна в каждой интерпретации I , в которой истинны все формулы из множества Γ . Запись $\Gamma \models \Phi$ служит сокращением для утверждения "формула Φ является **логическим следствием** множества формул Γ ".

Для углубленного изучения понятия **совместности** множества формул и отношения **логического следствия** нам будут полезны их финитные аналоги.

Определение 3.2.9. Множество формул Γ языка L_τ называется **локально совместным**, если любое его **конечное подмножество** совместно.

Определение 3.2.10. Формула A языка L_τ называется **локальным логическим следствием** множества формул Γ этого языка L_τ , если она является логическим следствием некоторого **конечного подмножества** Γ_0 множества Γ .

Замечание. Запись $\Gamma \models_{fin} A$ будет служить сокращением для утверждения "формула A является **локальным логическим следствием** множества формул Γ ".

Определение 3.2.11. Множество формул Γ языка L_τ назовем **локально полным**, если оно локально совместно и для любой замкнутой формулы A языка L_τ либо $\Gamma \models_{fin} A$, либо $\Gamma \models_{fin} (\neg A)$.

Замечание. Если Γ – локально совместное множество формул, то не существует такой замкнутой формулы A , что $\Gamma \models_{fin} A$ и $\Gamma \models_{fin} (\neg A)$. В самом деле, предположим, что существует такая замкнутая формула A , что $\Gamma \models_{fin} A$ и $\Gamma \models_{fin} (\neg A)$. В соответствии с определением найдутся такие конечные подмножества Γ_1 и Γ_2 множества Γ , 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 Γ .

Теорема 3.2.2. Для любого локально совместного множества формул Γ языка L_τ **Логики Предикатов** существует такое локально полное множество формул Γ^* языка L_τ , что

$$\Gamma \subseteq \Gamma^*.$$

Д о к а з а т е л ь с т в о. Дадим два варианта доказательства. В первом варианте доказательства будем считать, что сигнатура τ *счетная*. Тогда счетными будут и алфавит языка L_τ **Логики Предикатов**, и множество F_τ всех замкнутых формул **Логики Предикатов** этой сигнатуры.

Пусть $F_\tau = (\Phi_n)_{n \in \mathbb{N}}$.

Определим последовательность $(\Gamma_n)_{n \in \mathbb{N}}$ множеств формул.

Полагаем

$$\Gamma_1 \equiv \Gamma.$$

Если множество Γ_n уже определено, то полагаем

$$\Gamma_{n+1} \equiv \begin{cases} \Gamma_n \cup \{\Phi_n\}, & \text{если } \Gamma_n \models_{fin} \Phi_n \\ \Gamma_n \cup \{\neg\Phi_n\}, & \text{если } \Gamma_n \not\models_{fin} \Phi_n. \end{cases}$$

Индукцией по n докажем, что каждое из множеств формул Γ_n является **локально совместным**.

Так как $\Gamma_1 \equiv \Gamma$, то множество формул Γ_1 является **локально совместным** по условию теоремы.

Предположим, что уже доказана **локальная совместность** множества формул Γ_n . Докажем **локальную совместность** множества формул Γ_{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 Γ' – конечное подмножество множества Γ_n . Пусть Γ'' – такое конечное подмножество множества Γ_n , что $\Gamma'' \models \Phi_n$. Для конечного подмножества $\Gamma' \cup \Gamma''$ локально совместного множества формул Γ_n существует интерпретация φ такая, что $\varphi(\Gamma' \cup \Gamma'') = \mathbb{I}$. Тогда $\varphi(\Phi_n) = \mathbb{I}$ и $\varphi(\Gamma' \cup \{\Phi_n\}) = \mathbb{I}$. Значит, множество $\Gamma' \cup \{\Phi_n\}$ совместно, поэтому в рассматриваемом случае множество Γ_{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 Γ_{n+1} не является локально совместным, то найдется такое конечное подмножество Γ' множества Γ_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 $\Gamma_n \not\models_{fin} \Phi_n$. Значит, и в этом случае множество формул Γ_{n+1} является **локально совместным**.

Тем самым доказано, что *при любом n множество формул Γ_n является локально совместным*.

Полагаем

$$\Gamma^* \equiv \bigcup_{n=1}^{\infty} \Gamma_n.$$

Покажем, что Γ^* – **локально полное множество формул** и

$$\Gamma \subseteq \Gamma^*.$$

Последнее очевидно, так как

$$\Gamma = \Gamma_1 \subseteq \Gamma^*.$$

Если бы множество формул Γ^* 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 Γ_n .

Значит, Γ^* – **локально совместное** множество формул.

Пусть \mathcal{A} – произвольная замкнутая формула. Тогда найдется такое число n , что $\mathcal{A} = \Phi_n$.

Если $\Gamma_n \models_{fin} \Phi_n$, то $\Gamma^* \models_{fin} \Phi_n$, а, значит, $\Gamma^* \models_{fin} \mathcal{A}$.

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. $\Gamma^* \models_{fin} (\neg\mathcal{A})$.

Итак доказано, что Γ^* – **локально полное** множество формул языка L_τ такое, что $\Gamma \subseteq \Gamma^*$.

В случае произвольной сигнатуры τ возможно аналогичное доказательство, однако при этом вместо достаточно простой индукции по n необходимо использовать *трансфинитную индукцию*. Мы не будем рассматривать этот вариант доказательства, а приведем доказательство с использованием **леммы Тейхмюллера – Тьюки**.

Напомним, что семейство подмножеств \mathcal{X} множества E имеет **конечный характер**, если для каждого подмножества A множества E имеет место эквивалентность:

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

В первой главе было установлено, что следующее утверждение, эквивалентно **Аксиоме Выбора**.

Лемма Тейхмюллера – Тьюки. *Каждое семейство подмножеств \mathcal{X} множества E , имеющее конечный характер, обладает максимальным элементом.*

Рассмотрим следующее семейство подмножеств \mathcal{X} множества F_τ всех замкнутых формул языка L_τ

$$T \in \mathcal{X} \iff T \cup \Gamma \text{ — локально совместно.}$$

Из определения семейства подмножеств \mathcal{X} сразу следует, что оно имеет *конечный характер*. По лемме Тейхмюллера – Тьюки в семействе подмножеств \mathcal{X} имеется **максимальный элемент** T^* . Покажем, что множество $\Gamma^* = \Gamma \cup T^*$ является **локально полным**.

Из определения семейства подмножеств \mathcal{X} сразу следует, что множество Γ^* является **локально совместным**.

Для доказательства его **локальной полноты** предположим противное. Тогда найдется такая замкнутая формула, что $\Gamma^* \not\models_{fin} \mathcal{A}$ и $\Gamma^* \not\models_{fin} (\neg\mathcal{A})$. Значит, $\mathcal{A} \notin \Gamma^*$.

Покажем, что $\Gamma^* \cup \{\mathcal{A}\}$ **локально совместно**. В противном случае найдется такое конечное подмножество Γ_0 множества Γ^* , что $\Gamma_0 \cup \{\mathcal{A}\}$ не является локально совместным. Значит, для любой интерпретации φ из того, что все формулы из Γ_0 истинны в интерпретации φ , следует, что формула \mathcal{A} ложна в этой интерпретации. Последнее означает, что $\Gamma_0 \models (\neg\mathcal{A})$, поэтому $\Gamma^* \models_{fin} (\neg\mathcal{A})$, но это противоречит сделанному выше предположению $\Gamma^* \not\models_{fin} (\neg\mathcal{A})$.

Установленная **локальная совместность** множества

$$\Gamma^* \cup \{\mathcal{A}\} = \Gamma \cup T^* \cup \{\mathcal{A}\}$$

противоречит **максимальности** множества T^* .

Итак, Γ^* – **локально полное расширение локально совместного множества** Γ . \square

На первый взгляд кажется, что второй вариант доказательства ”проще” первого, однако это обманчивое впечатление – во втором варианте вся идейная трудность доказательства перенесена в доказательство эквивалентности **Леммы Тейхмюллера – Тьюки Аксиоме Выбора**.

Будем говорить, что для множества формул Σ языка первого порядка L_τ сигнатуры τ выполнено **свойство Генкина**, если для любой формулы F с одной свободной переменной v из того, что $\Sigma \models_{fin} (\exists v)F$, следует, что найдется такой замкнутый терм t , что $\Sigma \models_{fin} F_v[t]$.

Теорема 3.2.3. *Для любого локально совместного множества формул Γ языка L_τ сигнатуры τ можно построить локально совместное множество формул Γ^+ языка L_{τ^+} сигнатуры τ^+ такое, что $\Gamma \subseteq \Gamma^+$, сигнатура τ^+ получается из сигнатуры τ добавлением новых индивидуальных констант и для множества формул Γ^+ выполнено свойство Генкина.*

Д о к а з а т е л ь с т в о. Доказательство проведем лишь в случае счетной сигнатуры. Общий случай рассматривается по аналогичной схеме.

Рассмотрим сигнатуру τ^+ , полученную из сигнатуры τ добавлением **счетного множества** $\{c_1, c_2, \dots, c_m, \dots\}$ новых индивидуальных констант.

Заметим, что любую интерпретацию языка L_τ сигнатуры τ можно продолжить до интерпретации языка L_{τ^+} сигнатуры τ^+ , определив лишь ее значения для новых индивидуальных констант $\{c_1, c_2, \dots, c_m, \dots\}$, а любую интерпретацию языка L_{τ^+} сигнатуры τ^+ можно сузить до интерпретации языка L_τ сигнатуры τ , ”игнорируя” ее значения для новых индивидуальных констант $\{c_1, c_2, \dots, c_m, \dots\}$.

Локально совместное множество формул Γ языка L_τ сигнатуры τ мы рассматриваем как локально совместное множество формул языка L_{τ^+} сигнатуры τ^+ .

Так как сигнатура τ по предположению **счетная**, то счетными будут сигнатура τ^+ , алфавит языка L_{τ^+} **Логики Предикатов** этой сигнатуры и множество F_{τ^+} всех формул **Логики Предикатов** этой сигнатуры τ^+ .

Занумеруем $(F_n)_{n \in \mathbb{N}}$ все формулы языка L_{τ^+} , содержащие в точности одну свободную переменную. Для каждой формулы F_n через v_n будем обозначать ее единственную свободную переменную.

Индукцией по n построим последовательность $d_1, d_2, \dots, d_n, \dots$ из новых констант $\{c_1, c_2, \dots, c_m, \dots\}$ и локально совместные множества формул Γ_n .

Пусть d_1 – это любая новая константа c_i , не входящая в формулу F_1 . Полагаем $\Gamma_1 = \Gamma \cup \{((\exists v_1)F \rightarrow F_{v_1}[d_1])\}$.

Докажем локальную совместность множества формул Γ_1 . Пусть Γ_0 – произвольное конечное подмножество множества Γ . Существует интерпретация φ с основным множеством A языка $L_{\tau+}$, в которой все формулы из множества Γ_0 истинны. Заметим, что если мы изменим значения интерпретации φ на некоторых новых константах c_i , то в новой интерпретации φ' значения всех формул языка L_{τ} не изменятся, в частности, все формулы из множества Γ_0 будут истинны.

Если $\varphi((\exists v_1)F_1) = \text{И}$ и a – такой элемент из основного множества A , что $\varphi(F_{1,v_1}[\bar{a}]) = \text{И}$, то изменим значение $\varphi(d_1)$, определив новое значение равенством $\varphi'(d_1) = a$. Тогда $\varphi'((\exists v_1)F_1 \rightarrow F_{1,v_1}[d_1]) = \text{И}$.

Если же $\varphi((\exists v_1)F_1) = \text{Л}$, то $\varphi((\exists v_1)F_1 \rightarrow F_{1,v_1}[d_1]) = \text{И}$.

Так как в формулы множества Γ_0 не входят новые константы, то для любой формулы F из Γ_0 получаем $\varphi(F) = \varphi'(F) = \text{И}$.

Значит, $\Gamma_0 \cup \{((\exists v_1)F \rightarrow F_{v_1}[d_1])\}$ **совместно**, поэтому

$$\Gamma_1 = \Gamma \cup \{((\exists v_1)F \rightarrow F_{v_1}[d_1])\}$$

локально совместно.

Пусть уже построены начальный отрезок d_1, d_2, \dots, d_n последовательности из новых констант и локально совместное множество формул Γ_n , причем $\Gamma_n = \Gamma_{n-1} \cup \{((\exists v_n)F \rightarrow F_{v_n}[d_n])\}$.

Пусть d_{n+1} – это любая новая константа c_i , отличная от уже определенных констант d_1, d_2, \dots, d_n и не входящая в формулы F_1, F_2, \dots, F_n и F_{n+1} . Полагаем

$$\Gamma_{n+1} = \Gamma_n \cup \{((\exists v_{n+1})F \rightarrow F_{v_{n+1}}[d_{n+1}])\}.$$

Докажем **локальную совместность** множества формул Γ_{n+1} .

Пусть Γ_0 – произвольное конечное подмножество множества Γ_n . Существует интерпретация φ с основным множеством A языка $L_{\tau+}$, в которой все формулы из множества Γ_0 истинны. Заметим, что константа d_{n+1} не входит в формулы из множества Γ_n , поэтому если для интерпретации φ изменить лишь значение $\varphi(d_{n+1})$, то для полученной новой интерпретации φ' для любой формулы F из Γ_n получаем $\varphi(F) = \varphi'(F)$. Поэтому, в частности, все формулы из множества Γ_0 будут истинны в интерпретации φ' .

Если $\varphi((\exists v_{n+1})F_{n+1}) = \text{И}$ и a – такой элемент из основного множества A , что $\varphi(F_{n+1,v_{n+1}}[\bar{a}]) = \text{И}$, то изменим значение $\varphi(d_{n+1})$, определив новое значение равенством $\varphi'(d_{n+1}) = a$. Тогда

$$\varphi'((\exists v_{n+1})F_{n+1} \rightarrow F_{n+1,v_{n+1}}[d_{n+1}]) = \text{И}.$$

Если же $\varphi((\exists v_{n+1})F_{n+1}) = \text{Л}$, то $\varphi((\exists v_{n+1})F_{n+1} \rightarrow F_{n+1,v_{n+1}}[d_{n+1}]) = \text{И}$.

Так как в формулы множества Γ_0 не входит новая константа d_{n+1} , то для любой формулы F из Γ_0 получаем $\varphi'(F) = \varphi(F) = \text{И}$.

Значит, $\Gamma_0 \cup \{((\exists v_{n+1})F \rightarrow F_{v_{n+1}}[d_{n+1}])\}$ **совместно**, поэтому

$$\Gamma_{n+1} = \Gamma_n \cup \{((\exists v_{n+1})F \rightarrow F_{v_{n+1}}[d_{n+1}])\}$$

локально совместно.

Полагаем

$$\Gamma^+ \Leftrightarrow \bigcup_{n=1}^{\infty} \Gamma_n.$$

Покажем, что Γ^+ – **локально совместное множество формул, обладающее свойством Генкина** и

$$\Gamma \subseteq \Gamma^+.$$

Последнее очевидно. Для доказательства **локальной совместности** множества формул Γ^+ рассмотрим произвольное его конечное подмножество Γ_0 . Так как при любом k $\Gamma_k \subseteq \Gamma_{k+1}$, то найдется такое n , что $\Gamma_0 \subseteq \Gamma_n$. Так как выше уже доказано, что Γ_n **локально совместно**, то Γ_0 совместно, поэтому Γ^+ **локально совместно**.

Докажем, что множество формул Γ^+ обладает **свойством Генкина**.

Пусть F – произвольная формула с одной свободной переменной v . Найдется такое n , что F – это F_n , а v – это v_n . Тогда

$$((\exists v_n)F \rightarrow F_{v_n}[d_n]) \in \Gamma_n \subseteq \Gamma^+$$

т. е.

$$((\exists v)F \rightarrow F_v[d_n]) \in \Gamma_n \subseteq \Gamma^+.$$

Если $\Gamma^+ \models_{fin} (\exists v)F$, то найдется такое конечное подмножество Γ_0 множества Γ^+ , что $\Gamma_0 \models (\exists v)F$. Но тогда

$$\Gamma_0 \cup \{((\exists v)F \rightarrow F_v[d_n])\} \models F_v[d_n],$$

значит, $\Gamma^+ \models_{fin} F_v[d_n]$. □

Замечание. Построенное множество формул Γ^+ обладает следующим важным для дальнейшего свойством: если F – произвольная формула с одной свободной переменной v , то найдется такая константа c , что

$$((\exists v)F \rightarrow F_v[c]) \in \Gamma^+.$$

Поэтому если T – любое множество формул той же сигнатуры, что и Γ^+ , причем $\Gamma^+ \subseteq T$, то

$$((\exists v)F \rightarrow F_v[c]) \in T.$$

В частности, для T выполнено свойство Генкина.

Теорема компактности или локальная теорема К. Геделя – А.И. Мальцева. Множество замкнутых формул Γ языка L_τ является **совместным** тогда и только тогда, когда оно является **локально совместным**.

Доказательство. Если множество формул Γ языка L_τ является **совместным**, то, очевидно, является совместным и любое его подмножество. В частности, является совместным и любое конечное подмножество множества формул Γ . Значит, Γ **локально совместно**.

Обратно, предположим, что множество Γ **локально совместно**, т. е. любое его конечное подмножество является совместным. Докажем, что тогда совместно и все множество Γ .

Мы дадим два доказательства этого важного факта, чтобы продемонстрировать некоторые общие методы математической логики, работающие и в более сложных ситуациях.

Первое доказательство.

Применив две предыдущие теоремы, мы получим **локально полное, обладающее свойством Генкина** множество формул

$$\bar{\Gamma} = (\Gamma^+)^*$$

языка первого порядка L_{τ^+} сигнатуры τ^+ , полученной из сигнатуры τ добавлением новых индивидуальных констант такое, что $\Gamma \subseteq \bar{\Gamma}$.

Покажем, что множество формул $\bar{\Gamma}$ является **совместным**. Отсюда, конечно, сразу будет следовать **совместность и множества формул** Γ .

Построим интерпретацию φ такую, что $\varphi(\bar{\Gamma}) = \text{И}$.

Для языка первого порядка L_{τ^+} сигнатуры τ^+ , используя **локально полное, обладающее свойством Генкина** множество формул $\bar{\Gamma}$, построим **естественную структуру** \mathcal{A}_{τ^+} – алгебраическую систему сигнатуры τ^+ , основным множеством A которой будет множество \mathcal{T}_{τ^+} всех замкнутых термов языка L_{τ^+} .

Каждой индивидуальной константе c сигнатуры τ^+ сопоставим терм c – элемент основного множества A естественной структуры \mathcal{A}_{τ^+} .

Каждому n -местному функциональному символу f сигнатуры τ^+ сопоставим n -местную алгебраическую операцию $f^{\mathcal{A}_{\tau^+}}$ на основном множестве A естественной структуры \mathcal{A}_{τ^+} , полагая для произвольных элементов t_1, \dots, t_n множества A , т. е. термов языка L_{τ^+} ,

$$f^{\mathcal{A}_{\tau^+}}(t_1, \dots, t_n) \doteq f(t_1, \dots, t_n).$$

Каждому n -местному предикатному символу p сигнатуры τ^+ сопоставим n -местный предикат $p^{\mathcal{A}_{\tau^+}}$ на основном множестве A естественной структуры \mathcal{A}_{τ^+} , полагая для произвольных элементов t_1, \dots, t_n множества A , т. е. термов языка L_{τ^+} ,

$$p^{\mathcal{A}_{\tau^+}}(t_1, \dots, t_n) = \text{И} \iff \bar{\Gamma} \models_{fin} p(t_1, \dots, t_n).$$

Для каждого индивида $t \in A$, т. е. терма t сигнатуры τ^+ , его *именем* будет он сам t . Тогда сигнатура $\tau^+(A)$, полученная из сигнатуры τ^+ добавлением к множеству S индивидуальных констант сигнатуры τ^+ множества \bar{A} всех *имен индивидов* из A , будет совпадать с исходной сигнатурой τ^+ , а язык $L_{\tau^+(A)}$ – с исходным языком L_{τ^+} .

Для каждого свободного от переменных терма t языка $L_{\tau+}$ обычным образом индукцией по построению терма t определяем индивид $\mathcal{A}(t)$ из A , который *будет соответствовать терму t* .

Нетрудно понять, что в рассматриваемом случае $\mathcal{A}(t)$ – это t , но это разные t – первое t – это терм t языка $L_{\tau+}$, а второе t – это элемент t основного множества A естественной структуры $\mathcal{A}_{\tau+}$ языка $L_{\tau+}$.

Обычным способом для каждой замкнутой (т. е. не содержащей свободных переменных) формулы Φ языка $L_{\tau+(A)}$ определяем ее *истинностное значение* $\varphi(\Phi)$ в системе $\mathcal{A}_{\tau+}$ индукцией по построению формулы Φ (т. е. сопоставим Φ значение И или Л).

Условимся писать:

$$\begin{aligned}\mathcal{A}_{\tau+} &\models \Phi, & \text{если } \varphi(\Phi) = \text{И}, \\ \mathcal{A}_{\tau+} &\not\models \Phi, & \text{если } \varphi(\Phi) = \text{Л}.\end{aligned}$$

(i) Если Φ – атомная формула вида $p(t_1, \dots, t_n)$, где p – n -местный предикатный символ сигнатуры τ^+ , а t_1, \dots, t_n – свободные от переменных термы сигнатуры $\tau^+(A)$, то полагаем

$$\mathcal{A}_{\tau+} \models \Phi \iff p^{\mathcal{A}_{\tau+}}(\mathcal{A}_{\tau+}(t_1), \dots, \mathcal{A}_{\tau+}(t_n)) = \text{И},$$

т. е.

$$\mathcal{A}_{\tau+} \models \Phi \iff \bar{\Gamma} \models_{fin} p(t_1, \dots, t_n).$$

(ii) Теперь если Φ и Ψ – замкнутые формулы, то полагаем

$$\begin{aligned}\mathcal{A}_{\tau+} &\models (\neg\Phi) \iff \mathcal{A}_{\tau+} \not\models \Phi, \\ \mathcal{A}_{\tau+} &\models (\Phi \vee \Psi) \iff \mathcal{A}_{\tau+} \models \Phi \text{ или } \mathcal{A}_{\tau+} \models \Psi, \\ \mathcal{A}_{\tau+} &\models (\Phi \& \Psi) \iff \mathcal{A}_{\tau+} \models \Phi \text{ и } \mathcal{A}_{\tau+} \models \Psi, \\ \mathcal{A}_{\tau+} &\not\models (\Phi \rightarrow \Psi) \iff \mathcal{A}_{\tau+} \models \Phi \text{ и } \mathcal{A}_{\tau+} \not\models \Psi.\end{aligned}$$

(iii) Если Φ – формула, не содержащая свободных переменных, отличных от x , то полагаем

$$\begin{aligned}\mathcal{A}_{\tau+} &\models (\exists x)\Phi \iff \\ \mathcal{A}_{\tau+} &\models \Phi_x[t] \text{ для имени } t \text{ некоторого индивида } t \text{ из } A, \text{ т. е. терма } t,\end{aligned}$$

$$\begin{aligned}\mathcal{A}_{\tau+} &\models (\forall x)\Phi \iff \\ \mathcal{A}_{\tau+} &\models \Phi_x[t] \text{ для имени } t \text{ любого индивида } t \text{ из } A, \text{ т. е. терма } t.\end{aligned}$$

Напомним, что $\bar{\Gamma}$ – **локально полное множество формул**, поэтому для любой замкнутой формулы Φ

$$\bar{\Gamma} \models_{fin} \Phi \text{ или } \bar{\Gamma} \models_{fin} \neg\Phi,$$

но не то и другое одновременно, в частности, это верно и для произвольной атомной формулы вида $p(t_1, \dots, t_n)$, где p — n -местный предикатный символ сигнатуры τ^+ . Поэтому интерпретация φ определена корректно.

Индукцией по построению формул (либо по их длине, либо по числу входящих в них логических связок и кванторов) докажем, что для произвольной формулы Φ имеет место эквивалентность:

$$\bar{\Gamma} \models_{fin} \Phi \iff \varphi(\Phi) = И.$$

(i) Для элементарных формул Φ указанная эквивалентность имеет место по определению интерпретации φ .

(ii) Предположим, что указанная эквивалентность имеет место для формул Φ и Ψ и докажем, что тогда она выполняется и для формул

$$(\neg\Phi), \quad (\Phi \& \Psi), \quad (\Phi \vee \Psi), \quad (\Phi \rightarrow \Psi), \quad (\forall x)\Phi, \quad (\exists x)\Phi.$$

Так как

$$\bar{\Gamma} \models_{fin} (\neg\Phi) \iff \bar{\Gamma} \not\models_{fin} \Phi$$

и

$$\varphi(\Phi) = Л \iff \varphi(\neg\Phi) = И,$$

то

$$\bar{\Gamma} \models_{fin} (\neg\Phi) \iff \varphi((\neg\Phi)) = И.$$

Нетрудно показать, что

$$\bar{\Gamma} \models_{fin} (\Phi \& \Psi) \iff \bar{\Gamma} \models_{fin} \Phi \text{ и } \bar{\Gamma} \models_{fin} \Psi.$$

Кроме того, по определению интерпретации φ

$$\varphi(\Phi) = И \text{ и } \varphi(\Psi) = И \iff \varphi((\Phi \& \Psi)) = И.$$

Значит,

$$\bar{\Gamma} \models_{fin} (\Phi \& \Psi) \iff \varphi((\Phi \& \Psi)) = И.$$

Покажем, что для **локально полного** множества формул $\bar{\Gamma}$ и произвольных формул Φ и Ψ имеет место эквивалентность

$$\bar{\Gamma} \models_{fin} (\Phi \vee \Psi) \iff \bar{\Gamma} \models_{fin} \Phi \text{ или } \bar{\Gamma} \models_{fin} \Psi$$

В самом деле, если

$$\bar{\Gamma} \models_{fin} \Phi \text{ или } \bar{\Gamma} \models_{fin} \Psi,$$

то, конечно,

$$\bar{\Gamma} \models_{fin} (\Phi \vee \Psi).$$

Обратно, предположим, что

$$\bar{\Gamma} \models_{fin} (\Phi \vee \Psi).$$

Покажем, что тогда

$$\bar{\Gamma} \models_{fin} \Phi \quad \text{или} \quad \bar{\Gamma} \models_{fin} \Psi.$$

Предположим противное, т. е., что

$$\bar{\Gamma} \not\models_{fin} \Phi \quad \text{и} \quad \bar{\Gamma} \not\models_{fin} \Psi.$$

Так как $\bar{\Gamma}$ – **локально полное** множество формул, то тогда

$$\bar{\Gamma} \models_{fin} (\neg\Phi) \quad \text{и} \quad \bar{\Gamma} \models_{fin} (\neg\Psi),$$

а значит,

$$\bar{\Gamma} \models_{fin} ((\neg\Phi) \& (\neg\Psi)),$$

поэтому

$$\bar{\Gamma} \models_{fin} \neg(\Phi \vee \Psi).$$

Так как выше мы предположили, что

$$\bar{\Gamma} \models_{fin} (\Phi \vee \Psi),$$

то получаем противоречие с предположением о **локальной совместности** множества формул $\bar{\Gamma}$.

В итоге получаем

$$\bar{\Gamma} \models_{fin} (\Phi \vee \Psi) \quad \Longleftrightarrow \quad \bar{\Gamma} \models_{fin} \Phi \quad \text{или} \quad \bar{\Gamma} \models_{fin} \Psi$$

и

$$\varphi(\Phi) = \text{И} \quad \text{или} \quad \varphi(\Psi) = \text{И} \quad \Longleftrightarrow \quad \varphi((\Phi \vee \Psi)) = \text{И},$$

поэтому

$$\bar{\Gamma} \models_{fin} (\Phi \vee \Psi) \quad \Longleftrightarrow \quad \varphi((\Phi \vee \Psi)) = \text{И}.$$

Доказательство эквивалентности

$$\bar{\Gamma} \models_{fin} (\Phi \rightarrow \Psi) \quad \Longleftrightarrow \quad \varphi(\Phi \rightarrow \Psi) = \text{И}$$

проводится по той же схеме с использованием локальной полноты и локальной совместности множества формул $\bar{\Gamma}$.

Остается рассмотреть формулы вида $(\exists x)\Phi$ и $(\forall x)\Phi$. Именно при их рассмотрении нам понадобится свойство Генкина.

Если Φ – формула, не содержащая свободных переменных, отличных от x , то по определению

$$\begin{aligned} \mathcal{A}_{\tau+} \models (\exists x)\Phi & \Longleftrightarrow \\ \mathcal{A}_{\tau+} \models \Phi_x[t] & \text{ для имени } t \text{ некоторого индивида } t \text{ из } A, \text{ т. е. терма } t. \end{aligned}$$

Покажем, что имеет место эквивалентность:

$$\bar{\Gamma} \models_{fin} (\exists x)\Phi \iff \varphi((\exists x)\Phi) = \text{И}.$$

Если

$$\bar{\Gamma} \models_{fin} (\exists x)\Phi,$$

то в силу свойства Генкина найдется такой замкнутый терм t (даже константа c), что

$$((\exists x)\Phi \rightarrow \Phi_x[t]) \in \Gamma^+ \subseteq \bar{\Gamma},$$

значит,

$$\bar{\Gamma} \models_{fin} ((\exists x)\Phi \rightarrow \Phi_x[t]),$$

поэтому

$$\bar{\Gamma} \models_{fin} \Phi_x[t].$$

По индуктивному предположению тогда $\varphi(\Phi_x[t]) = \text{И}$, поэтому и

$$\varphi((\exists x)\Phi) = \text{И}.$$

Если же $\varphi((\exists x)\Phi) = \text{И}$, то найдется такой замкнутый терм t , что $\varphi(\Phi_x[t]) = \text{И}$. По индуктивному предположению тогда

$$\bar{\Gamma} \models_{fin} \Phi_x[t].$$

Так как

$$\bar{\Gamma} \models_{fin} (\Phi_x[t] \rightarrow (\exists x)\Phi),$$

то

$$\bar{\Gamma} \models_{fin} (\exists x)\Phi.$$

Тем самым доказано, что

$$\bar{\Gamma} \models_{fin} (\exists x)\Phi \iff \varphi((\exists x)\Phi) = \text{И}.$$

По той же схеме доказывается, что

$$\bar{\Gamma} \models_{fin} (\forall x)\Phi \iff \varphi((\forall x)\Phi) = \text{И}.$$

В итоге доказано, что для произвольной формулы Φ имеет место эквивалентность:

$$\bar{\Gamma} \models_{fin} \Phi \iff \varphi(\Phi) = \text{И}.$$

Если Φ – произвольная формула из множества $\bar{\Gamma}$, то, очевидно, $\bar{\Gamma} \models_{fin} \Phi$, поэтому $\varphi(\Phi) = \text{И}$.

Значит, $\varphi(\bar{\Gamma}) = \text{И}$, поэтому множество формул $\bar{\Gamma}$ является **совместным**, а значит, **совместным** является и исходное множество формул Γ . \square

Второй вариант доказательства, использующий понятие фильтрованного произведения, будет дан в следующем параграфе.

Теорема 3.2.4. *Для любого множества формул Γ и замкнутой формулы Φ имеет место эквивалентность:*

$$\Gamma \models_{fin} \Phi \iff \Gamma \models \Phi.$$

Доказательство. Если $\Gamma \models_{fin} \Phi$, то, конечно, $\Gamma \models \Phi$. Пусть $\Gamma \models \Phi$. Покажем, что тогда $\Gamma \models_{fin} \Phi$. Допустим противное, тогда для любого конечного подмножества Γ_0 множества Γ совместно множество $\Gamma_0 \cup \{(\neg\Phi)\}$, поэтому множество $\Gamma \cup \{(\neg\Phi)\}$ **локально совместно**. В силу предыдущей теоремы множество $\Gamma \cup \{(\neg\Phi)\}$ **совместно**, но это противоречит предположению $\Gamma \models \Phi$. \square

3.3. Фильтрованные произведения

Для произвольного множества I множество $P(I)$ всех его подмножеств является булевой алгеброй относительно операций \cup и \cap . В первой главе было введено общее понятие фильтра в произвольной булевой алгебре. Напомним соответствующие определения в случае булевой алгебры $P(I)$. Фильтры в булевой алгебре $P(I)$ называются фильтрами над множеством I .

Определение 3.3.1. *Фильтром над множеством I называется произвольная непустая система подмножеств D множества I , удовлетворяющая следующим условиям:*

- 1) *если $X \in D$ и $Y \in D$, то $X \cap Y \in D$,*
- 2) *если $X \in D$ и $X \subseteq Y$, то $Y \in D$,*
- 3) $\emptyset \notin D$.

Из пунктов 1) и 2) легко получить эквивалентность: для любых подмножеств X и Y множества I : $X \in D$ и $Y \in D$ тогда и только тогда, когда $X \cap Y \in D$.

Если $X \in D$ или $Y \in D$, то $X \cup Y \in D$. Фильтр, для которого верно обратное утверждение, называется *простым*.

Определение 3.3.2. *Фильтр над множеством I называется **простым**, если для любых подмножеств X и Y множества I из того, что $X \cup Y \in D$ следует, что $X \in D$ или $Y \in D$.*

Для простого фильтра D имеет место эквивалентность: для любых подмножеств X и Y множества I : $X \in D$ или $Y \in D$ тогда и только тогда, когда $X \cup Y \in D$.

Определение 3.3.3. *Фильтр над множеством I называется **максимальным**, если он не содержится ни в каком отличном от него фильтре.*

Определение 3.3.4. *Фильтр над множеством I называется ультрафильтром, если для любого подмножества X множества I либо $X \in D$, либо $(I \setminus X) \in D$.*

Используя аксиому выбора, в Дополнении доказано, что понятия простого, максимального и ультрафильтра эквивалентны между собой. Кроме того, доказано, что любой фильтр содержится в максимальном фильтре.

Рассмотрим семейство $(\mathcal{A}_i)_{i \in I}$ алгебраических систем сигнатуры τ с основными множествами A_i ($i \in I$). Чтобы несколько упростить обозначения, алгебраическую операцию $f^{\mathcal{A}_i}$, предикат $p^{\mathcal{A}_i}$ и элемент $c^{\mathcal{A}_i}$, соответствующие в алгебраической системе \mathcal{A}_i соответственно функциональному символу f , предикатному символу p и константе c сигнатуры τ , будем обозначать коротко через f , p и c соответственно. Это не приведет к недоразумениям.

Введем понятие *прямого произведения* семейства алгебраических систем $(\mathcal{A}_i)_{i \in I}$, обобщающее хорошо известные из курса "Алгебра" понятия прямого произведения семейства групп или колец. Прямое произведение семейства алгебраических систем $(\mathcal{A}_i)_{i \in I}$ будем обозначать через $\prod_{i \in I} \mathcal{A}_i$. Основным множеством системы $\prod_{i \in I} \mathcal{A}_i$ служит прямое произведение $\prod_{i \in I} A_i$ основных множеств A_i систем \mathcal{A}_i . Напомним, что элементами множества $\prod_{i \in I} A_i$ являются всевозможные функции g из множества I во множество $\bigcup_{i \in I} A_i$ такие, что при любом i из I $g(i) \in A_i$.

Каждому n -местному функциональному символу f сопоставим n -местную алгебраическую операцию, определенную на множестве $\prod_{i \in I} A_i$, которую будем обозначать через f , что не приведет к недоразумению. Для произвольных элементов g_1, g_2, \dots, g_n множества $\prod_{i \in I} \mathcal{A}_i$ и любого i из I полагаем

$$f(g_1, g_2, \dots, g_n)(i) = f(g_1(i), g_2(i), \dots, g_n(i)).$$

Каждому n -местному предикатному символу p сопоставим n -местный предикат, определенный на множестве $\prod_{i \in I} A_i$, который будем обозначать через p , что не приведет к недоразумению. Для произвольных элементов g_1, g_2, \dots, g_n из $\prod_{i \in I} \mathcal{A}_i$ полагаем

$$p(g_1, g_2, \dots, g_n) = \text{И} \iff \text{при любом } i: p(g_1(i), g_2(i), \dots, g_n(i)) = \text{И}.$$

Каждому константному символу c сопоставим элемент из множества $\prod_{i \in I} A_i$, который будем обозначать через c , что не приведет к недоразумению. Для произвольного i из I полагаем

$$c(i) = c.$$

Прямое произведение $\prod_{i \in I} \mathcal{A}_i$ семейства алгебраических систем $(\mathcal{A}_i)_{i \in I}$ одной и той же сигнатуры τ с точки зрения математической логики особого интереса не представляет. Большой интерес представляет **фильтрованное произведение** семейства алгебраических систем $(\mathcal{A}_i)_{i \in I}$ по произвольному фильтру D , которое будет обозначаться через $\prod_{i \in I} \mathcal{A}_i / D$.

К определению этого понятия мы и переходим.

Пусть $(\mathcal{A}_i)_{i \in I}$ – семейство алгебраических систем сигнатуры τ с основными множествами A_i ($i \in I$), а D – фильтр на множестве индексов I . На прямом произведении $\prod_{i \in I} A_i$ основных множеств A_i систем \mathcal{A}_i введем отношение эквивалентности \equiv_D . Пусть g и h – элементы из $\prod_{i \in I} A_i$. Полагаем

$$g \equiv_D h \iff \{i \mid g(i) = h(i)\} \in D.$$

Рефлексивность и симметричность отношения \equiv_D очевидны, а его транзитивность следует из включения

$$\{i \mid g(i) = h(i)\} \cap \{i \mid h(i) = t(i)\} \subseteq \{i \mid g(i) = t(i)\}.$$

Обозначим через $[g]$ класс эквивалентности с представителем g , т. е.

$$[g] = \{h \mid g \equiv_D h\}.$$

Множество классов эквивалентности, называемое фактормножеством множества $\prod_{i \in I} A_i$ по отношению эквивалентности \equiv_D , обозначается через $\prod_{i \in I} A_i / \equiv_D$.

Наделим множество $\prod_{i \in I} A_i / \equiv_D$ структурой алгебраической системы сигнатуры τ .

Каждому n -местному функциональному символу f сигнатуры τ сопоставим n -местную алгебраическую операцию, определенную на множестве $\prod_{i \in I} A_i / \equiv_D$, которую будем обозначать через f , что не приведет к недоразумению. Для произвольных элементов $[g_1], [g_2], \dots, [g_n]$ из $\prod_{i \in I} A_i / \equiv_D$ полагаем

$$f([g_1], [g_2], \dots, [g_n]) = [f(g_1, g_2, \dots, g_n)].$$

Независимость определения от выбора представителей в классах эквивалентности $[g_1], [g_2], \dots, [g_n]$ следует из включения

$$\begin{aligned} \{i \mid g_1(i) = h_1(i)\} \cap \{i \mid g_2(i) = h_2(i)\} \cap \dots \cap \{i \mid g_n(i) = h_n(i)\} \subseteq \\ \subseteq \{i \mid f(g_1(i), g_2(i), \dots, g_n(i)) = f(h_1(i), h_2(i), \dots, h_n(i))\}. \end{aligned}$$

Каждому n -местному предикатному символу p сопоставим n -местный предикат, определенный на множестве $\prod_{i \in I} A_i / \equiv_D$, который будем обозначать через

p , что не приведет к недоразумению. Для произвольных элементов $[g_1], [g_2], \dots, [g_n]$ из $\prod_{i \in I} A_i / \equiv_D$ полагаем

$$p([g_1], [g_2], \dots, [g_n]) = \mathbb{I} \iff \{i \mid p(g_1(i), g_2(i), \dots, g_n(i)) = \mathbb{I}\} \in D.$$

Независимость определения от выбора представителей в классах эквивалентности $[g_1], [g_2], \dots, [g_n]$ следует из включения

$$\begin{aligned} & \{i \mid g_1(i) = h_1(i)\} \cap \{i \mid g_2(i) = h_2(i)\} \cap \dots \cap \{i \mid g_n(i) = h_n(i)\} \cap \\ & \cap \{i \mid p(g_1(i), g_2(i), \dots, g_n(i)) = \mathbb{I}\} \subseteq \{i \mid p(h_1(i), h_2(i), \dots, h_n(i)) = \mathbb{I}\}. \end{aligned}$$

Каждому константному символу c сигнатуры τ сопоставим элемент $[c]$ из множества $\prod_{i \in I} A_i / \equiv_D$, который будем обозначать через c , что не приведет к недоразумению. Напомним, что в квадратных скобках стоит функция, определенная для произвольного i из I равенством

$$c(i) = c.$$

Построенная алгебраическая система сигнатуры τ обозначается через

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

и называется *фильтрованным произведением семейства алгебраических систем $(A_i)_{i \in I}$ сигнатуры τ по фильтру D* .

Пусть все свободные переменные формулы Φ содержатся в списке x_1, x_2, \dots, x_n , тогда справедлива следующая теорема Лося.

Теорема 3.3.1 (Лось). Пусть $(A_i)_{i \in I}$ – семейство алгебраических систем сигнатуры τ , D – **ультрафильтр** на множестве индексов I , а $\prod_{i \in I} A_i / \equiv_D$ – соответствующее **фильтрованное произведение**. Тогда для любых элементов $[g_1], [g_2], \dots, [g_n]$ из основного множества $\prod_{i \in I} A_i / \equiv_D$ системы $\prod_{i \in I} A_i / \equiv_D$ имеет место следующая эквивалентность

$$\begin{aligned} \prod_{i \in I} A_i / \equiv_D \models \Phi_{x_1, x_2, \dots, x_n}([g_1], [g_2], \dots, [g_n]) & \iff \\ \iff \{i \mid A_i \models \Phi_{x_1, x_2, \dots, x_n}(g_1(i), g_2(i), \dots, g_n(i))\} & \in D. \end{aligned}$$

Д о к а з а т е л ь с т в о. Доказательство будем вести индукцией по числу входящих в формулу Φ логических связок и кванторов.

(i) Пусть Φ – элементарная формула, т. е. имеет вид $p(t_1, \dots, t_m)$, где p – m -местный предикатный символ сигнатуры τ . Вместо записи $t_{j x_1, \dots, x_n}[a_1, \dots, a_n]$ будем использовать запись $t_j(a_1, \dots, a_n)$. Тогда выполняются равенства

$$\begin{aligned} t_j([g_1], \dots, [g_n]) &= [t_j(g_1, \dots, g_n)], \quad t_j(g_1, \dots, g_n)(i) = t_j(g_1(i), \dots, g_n(i)) \quad \text{и} \\ \Phi_{x_1, x_2, \dots, x_n}([g_1], [g_2], \dots, [g_n]) &= p(t_1([g_1], \dots, [g_n]), \dots, t_m([g_1], \dots, [g_n])). \end{aligned}$$

Доказательство в этом случае следует из следующих эквивалентностей

$$\begin{aligned}
 \prod_{i \in I} \mathcal{A}_i / \equiv_D \models \Phi_{x_1, x_2, \dots, x_n} [[g_1], [g_2], \dots, [g_n]] &\iff \\
 \prod_{i \in I} \mathcal{A}_i / \equiv_D \models p(t_1([g_1], \dots, [g_n]), \dots, t_m([g_1], \dots, [g_n])) &\iff \\
 \prod_{i \in I} \mathcal{A}_i / \equiv_D \models p([t_1(g_1, \dots, g_n)], \dots, [t_m(g_1, \dots, g_n)]) &\iff \\
 \{i \mid \mathcal{A}_i \models p(t_1(g_1, \dots, g_n)(i), \dots, t_m(g_1, \dots, g_n)(i))\} \in D &\iff \\
 \{i \mid \mathcal{A}_i \models p(t_1(g_1(i), \dots, g_n(i)), \dots, t_m(g_1(i), \dots, g_n(i)))\} \in D &\iff \\
 \iff \{i \mid \mathcal{A}_i \models \Phi_{x_1, x_2, \dots, x_n} [g_1(i), g_2(i), \dots, g_n(i)]\} \in D.
 \end{aligned}$$

(ii) Предположим, что указанная эквивалентность имеет место для формул Φ и Ψ и докажем, что тогда она выполняется и для формул

$$(\neg\Phi), \quad (\Phi \& \Psi), \quad (\Phi \vee \Psi), \quad (\Phi \rightarrow \Psi), \quad (\forall x)\Phi, \quad (\exists x)\Phi.$$

Так как D – **ультрафильтр**, то для любого подмножества U множества I выполняется эквивалентность

$$U \in D \iff (I \setminus U) \notin D$$

Кроме того, для любой формулы \mathcal{F} , все свободные переменные которой содержатся в списке x_1, x_2, \dots, x_n , и для любых элементов $[g_1], [g_2], \dots, [g_n]$ из основного множества $\prod_{i \in I} \mathcal{A}_i / \equiv_D$ системы $\prod_{i \in I} \mathcal{A}_i / \equiv_D$ выполняется равенство

$$\begin{aligned}
 \{i \mid \mathcal{A}_i \models (\neg\mathcal{F})_{x_1, x_2, \dots, x_n} [g_1(i), g_2(i), \dots, g_n(i)]\} = \\
 I \setminus \{i \mid \mathcal{A}_i \models \mathcal{F}_{x_1, x_2, \dots, x_n} [g_1(i), g_2(i), \dots, g_n(i)]\}.
 \end{aligned}$$

Поэтому справедлива эквивалентность

$$\begin{aligned}
 \{i \mid \mathcal{A}_i \models (\neg\mathcal{F})_{x_1, x_2, \dots, x_n} [g_1(i), g_2(i), \dots, g_n(i)]\} \in D &\iff \\
 \{i \mid \mathcal{A}_i \models \mathcal{F}_{x_1, x_2, \dots, x_n} [g_1(i), g_2(i), \dots, g_n(i)]\} \notin D,
 \end{aligned}$$

на основании которой получаем эквивалентности

$$\begin{aligned}
 \prod_{i \in I} \mathcal{A}_i / \equiv_D \models (\neg\Phi)_{x_1, x_2, \dots, x_n} [[g_1], [g_2], \dots, [g_n]] &\iff \\
 \iff \prod_{i \in I} \mathcal{A}_i / \equiv_D \not\models \Phi_{x_1, x_2, \dots, x_n} [[g_1], [g_2], \dots, [g_n]] &\iff \\
 \iff \{i \mid \mathcal{A}_i \models \Phi_{x_1, x_2, \dots, x_n} [g_1(i), g_2(i), \dots, g_n(i)]\} \notin D &\iff \\
 \iff \{i \mid \mathcal{A}_i \models (\neg\Phi)_{x_1, x_2, \dots, x_n} [g_1(i), g_2(i), \dots, g_n(i)]\} \in D.
 \end{aligned}$$

§3.3 Фильтрованные произведения

Для любого фильтра D и любых подмножеств U и V множества I справедлива эквивалентность

$$U \cap V \in D \iff U \in D \text{ и } V \in D.$$

Воспользовавшись этой эквивалентностью и равенством

$$\begin{aligned} \{i \mid \mathcal{A}_i \models \Phi_{x_1, x_2, \dots, x_n}[g_1(i), g_2(i), \dots, g_n(i)]\} \cap \\ \cap \{i \mid \mathcal{A}_i \models \Psi_{x_1, x_2, \dots, x_n}[g_1(i), g_2(i), \dots, g_n(i)]\} = \\ \{i \mid \mathcal{A}_i \models (\Phi \& \Psi)_{x_1, x_2, \dots, x_n}[g_1(i), g_2(i), \dots, g_n(i)]\}, \end{aligned}$$

получим эквивалентности

$$\begin{aligned} \prod_{i \in I} \mathcal{A}_i / \equiv_D \models (\Phi \& \Psi)_{x_1, x_2, \dots, x_n}[[g_1], [g_2], \dots, [g_n]] &\iff \\ \prod_{i \in I} \mathcal{A}_i / \equiv_D \models (\Phi_{x_1, x_2, \dots, x_n}[[g_1], [g_2], \dots, [g_n]] \& \Psi_{x_1, x_2, \dots, x_n}[[g_1], [g_2], \dots, [g_n]]) &\iff \\ \prod_{i \in I} \mathcal{A}_i / \equiv_D \models \Phi_{x_1, x_2, \dots, x_n}[[g_1], [g_2], \dots, [g_n]] \text{ и} & \\ \prod_{i \in I} \mathcal{A}_i / \equiv_D \models \Psi_{x_1, x_2, \dots, x_n}[[g_1], [g_2], \dots, [g_n]] &\iff \\ \iff \{i \mid \mathcal{A}_i \models \Phi_{x_1, x_2, \dots, x_n}[g_1(i), g_2(i), \dots, g_n(i)]\} \in D \text{ и} & \\ \{i \mid \mathcal{A}_i \models \Psi_{x_1, x_2, \dots, x_n}[g_1(i), g_2(i), \dots, g_n(i)]\} \in D &\iff \\ \iff \{i \mid \mathcal{A}_i \models \Phi_{x_1, x_2, \dots, x_n}[g_1(i), g_2(i), \dots, g_n(i)]\} \cap & \\ \{i \mid \mathcal{A}_i \models \Psi_{x_1, x_2, \dots, x_n}[g_1(i), g_2(i), \dots, g_n(i)]\} \in D &\iff \\ \iff \{i \mid \mathcal{A}_i \models (\Phi \& \Psi)_{x_1, x_2, \dots, x_n}[g_1(i), g_2(i), \dots, g_n(i)]\} \in D. & \end{aligned}$$

Для любого ультрафильтра D и любых подмножеств U и V множества I справедлива эквивалентность

$$U \cup V \in D \iff U \in D \text{ или } V \in D.$$

Воспользовавшись этой эквивалентностью и равенством

$$\begin{aligned} \{i \mid \mathcal{A}_i \models \Phi_{x_1, x_2, \dots, x_n}[g_1(i), g_2(i), \dots, g_n(i)]\} \cup \\ \{i \mid \mathcal{A}_i \models \Psi_{x_1, x_2, \dots, x_n}[g_1(i), g_2(i), \dots, g_n(i)]\} = \\ \{i \mid \mathcal{A}_i \models (\Phi \vee \Psi)_{x_1, x_2, \dots, x_n}[g_1(i), g_2(i), \dots, g_n(i)]\}, \end{aligned}$$

получим эквивалентности

$$\begin{aligned}
 \prod_{i \in I} \mathcal{A}_i / \equiv_D & \models (\Phi \vee \Psi)_{x_1, x_2, \dots, x_n} [[g_1], [g_2], \dots, [g_n]] \iff \\
 \prod_{i \in I} \mathcal{A}_i / \equiv_D & \models (\Phi_{x_1, x_2, \dots, x_n} [[g_1], [g_2], \dots, [g_n]] \vee \Psi_{x_1, x_2, \dots, x_n} [[g_1], [g_2], \dots, [g_n]]) \iff \\
 \prod_{i \in I} \mathcal{A}_i / \equiv_D & \models \Phi_{x_1, x_2, \dots, x_n} [[g_1], [g_2], \dots, [g_n]] \quad \text{или} \\
 \prod_{i \in I} \mathcal{A}_i / \equiv_D & \models \Psi_{x_1, x_2, \dots, x_n} [[g_1], [g_2], \dots, [g_n]] \iff \\
 \iff \{i \mid \mathcal{A}_i \models \Phi_{x_1, x_2, \dots, x_n} [g_1(i), g_2(i), \dots, g_n(i)]\} \in D & \text{ или} \\
 \{i \mid \mathcal{A}_i \models \Psi_{x_1, x_2, \dots, x_n} [g_1(i), g_2(i), \dots, g_n(i)]\} \in D & \iff \\
 \iff \{i \mid \mathcal{A}_i \models \Phi_{x_1, x_2, \dots, x_n} [g_1(i), g_2(i), \dots, g_n(i)]\} \cup & \\
 \{i \mid \mathcal{A}_i \models \Psi_{x_1, x_2, \dots, x_n} [g_1(i), g_2(i), \dots, g_n(i)]\} \in D & \iff \\
 \iff \{i \mid \mathcal{A}_i \models (\Phi \vee \Psi)_{x_1, x_2, \dots, x_n} [g_1(i), g_2(i), \dots, g_n(i)]\} \in D. &
 \end{aligned}$$

Для формулы $(\Phi \rightarrow \Psi)$ доказываемое утверждение легко получается из уже доказанного, если вспомнить, что она эквивалентна формуле $((\neg \Phi) \vee \Psi)$.

Рассмотрим формулу $(\exists x)\Phi$, где x – единственная свободная переменная формулы Φ . Мы будем, не оговаривая это особо, использовать равенства

$$((\exists x)\Phi)_{x_1, x_2, \dots, x_n} [a_1, a_2, \dots, a_n] \equiv (\exists x)(\Phi_{x_1, x_2, \dots, x_n} [a_1, a_2, \dots, a_n])$$

и

$$(\Phi_{x_1, x_2, \dots, x_n} [a_1, a_2, \dots, a_n])_x [a] \equiv \Phi_{x, x_1, x_2, \dots, x_n} [a, a_1, a_2, \dots, a_n],$$

где x, x_1, \dots, x_n – различные переменные, a, a_1, \dots, a_n – замкнутые термы. Пусть

$$\prod_{i \in I} \mathcal{A}_i / \equiv_D \models ((\exists x)\Phi)_{x_1, x_2, \dots, x_n} [[g_1], [g_2], \dots, [g_n]],$$

тогда при некотором $[g]$

$$\prod_{i \in I} \mathcal{A}_i / \equiv_D \models (\Phi_{x_1, x_2, \dots, x_n} [[g_1], [g_2], \dots, [g_n]])_x [[g]],$$

а значит,

$$\prod_{i \in I} \mathcal{A}_i / \equiv_D \models \Phi_{x, x_1, x_2, \dots, x_n} [[g], [g_1], [g_2], \dots, [g_n]].$$

По индуктивному предположению получаем

$$\{i \mid \mathcal{A}_i \models \Phi_{x, x_1, x_2, \dots, x_n} [g(i), g_1(i), g_2(i), \dots, g_n(i)]\} \in D.$$

Но

$$\begin{aligned}
 \{i \mid \mathcal{A}_i \models \Phi_{x, x_1, x_2, \dots, x_n} [g(i), g_1(i), g_2(i), \dots, g_n(i)]\} & \subseteq \\
 & \subseteq \{i \mid \mathcal{A}_i \models (\exists x)\Phi_{x_1, x_2, \dots, x_n} [g_1(i), g_2(i), \dots, g_n(i)]\},
 \end{aligned}$$

поэтому

$$\{i \mid \mathcal{A}_i \models (\exists x)\Phi_{x_1, x_2, \dots, x_n}[g_1(i), g_2(i), \dots, g_n(i)]\} \in D.$$

Для доказательства обратного утверждения предположим, что

$$\{i \mid \mathcal{A}_i \models (\exists x)\Phi_{x_1, x_2, \dots, x_n}[g_1(i), g_2(i), \dots, g_n(i)]\} \in D.$$

Пусть

$$I_1 = \{i \mid \mathcal{A}_i \models (\exists x)\Phi_{x_1, x_2, \dots, x_n}[g_1(i), g_2(i), \dots, g_n(i)]\}.$$

Тогда $I_1 \in D$ и при любом $i \in I_1$ найдется во множестве \mathcal{A}_i элемент h_i такой, что

$$\mathcal{A}_i \models \Phi_{x, x_1, x_2, \dots, x_n}[h_i, g_1(i), g_2(i), \dots, g_n(i)].$$

Строим функцию h из I в $\bigcup_{i \in I} \mathcal{A}_i$ такую, что при любом i из I $h(i) \in \mathcal{A}_i$ и при любом i из I_1 $h(i) = h_i$. Так как

$$I_1 \subseteq \{i \mid \mathcal{A}_i \models \Phi_{x, x_1, x_2, \dots, x_n}[h(i), g_1(i), g_2(i), \dots, g_n(i)]\},$$

то

$$\{i \mid \mathcal{A}_i \models \Phi_{x, x_1, x_2, \dots, x_n}[h(i), g_1(i), g_2(i), \dots, g_n(i)]\} \in D.$$

По индуктивному предположению получаем

$$\prod_{i \in I} \mathcal{A}_i / \equiv_D \models \Phi_{x, x_1, x_2, \dots, x_n}[[h], [g_1], [g_2], \dots, [g_n]],$$

а значит, и

$$\prod_{i \in I} \mathcal{A}_i / \equiv_D \models ((\exists x)\Phi)_{x_1, x_2, \dots, x_n}[[g_1], [g_2], \dots, [g_n]].$$

Для завершения доказательства теоремы осталось заметить, что формула $(\forall x)\Phi$ равносильна формуле $\neg((\exists x)\neg(\Phi))$. \square

Рассмотрим второй вариант доказательства локальной теоремы К. Геделя – А.И. Мальцева

Пусть множество замкнутых формул Γ языка L_τ является **локально совместным**, т. е. каждое его конечное подмножество совместно. Покажем, что **совместно** и все множество формул Γ .

Обозначим через I семейство всех конечных подмножеств множества формул Γ . Для каждого i из множества I пусть Φ_i – это конъюнкция всех формул из i , а \mathcal{A}_i – алгебраическая система, в которой истинны все формулы из i , а значит, и формула Φ_i .

Для произвольного t из I полагаем

$$I_t = \{i \mid i \in I \text{ \& } \mathcal{A}_i \models \Phi_t\}.$$

Докажем, что семейство $(I_t)_{t \in I}$ подмножеств множества I обладает следующим свойством: *пересечение любого конечного числа множеств этого семейства*

непусто. В самом деле пусть $I_{t_1}, I_{t_2}, \dots, I_{t_n}$ – элементы семейства, а $\Phi_{t_1}, \Phi_{t_2}, \dots, \Phi_{t_n}$ – соответствующие формулы. Обозначим через Φ конъюнкцию формул $\Phi_{t_1}, \Phi_{t_2}, \dots, \Phi_{t_n}$. По условию формула Φ *выполнима*. Пусть \mathcal{A}_{i_0} – соответствующая алгебраическая система. Тогда

$$i_0 \in I_{t_1} \cap I_{t_2} \cap \dots \cap I_{t_n}.$$

Тогда, как доказано в **Дополнении**, существует **ультрафильтр** D , содержащий все множества семейства $(I_t)_{t \in I}$. Рассмотрим ультрапроизведение

$$\prod_{i \in I} \mathcal{A}_i / \equiv_D.$$

Покажем, что все формулы из множества Γ истинны на этой системе. В самом деле, если Φ_t – произвольная формула из множества Γ , то

$$\{i \mid i \in I \ \& \ \mathcal{A}_i \models \Phi_t\} = I_t \in D.$$

Поэтому

$$\prod_{i \in I} \mathcal{A}_i / \equiv_D \models \Phi_t.$$

3.4. 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"*, 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, преобразовывали 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 гг.) метод ” $\varepsilon - \delta$ ” стал основным инструментом ”взятия пределов” в математическом анализе. Хотя Б. Больцано (1781 – 1848 гг.) на пятьдесят лет раньше предложил аналогичный метод, но 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 Лопиталья, 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, обоснование А. Робинсоном лейбницевского 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 сигнатура $\tau_{\mathbb{R}}$ включает в свое множество индивидных констант обозначения для каждого действительного числа, любой функции от произвольного числа действительных переменных и любого предиката, определенного на множестве действительных чисел.

Рассмотрим счетное семейство $(\mathcal{A}_i)_{i \in \mathbb{N}}$ алгебраических систем сигнатуры $\tau_{\mathbb{R}}$, каждая из которых – это поле действительных чисел \mathbb{R} со всеми определенными на нем функциями и предикатами.

Пусть F – *неглавный ультрафильтр* на множестве \mathbb{N} натуральных чисел.

Тогда \mathbb{R}^* – это просто фильтрованное произведение

$$\prod_{i \in \mathbb{N}} \mathcal{A}_i / F$$

(ультрастепень поля действительных чисел \mathbb{R}).

Ввиду достаточной сложности понятия фильтрованного произведения алгебраических систем, на наш взгляд, будет нелишним еще раз напомнить основные этапы построения фильтрованного произведения в рассматриваемом, по нашему мнению, более простом случае.

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 .

$$[f] + [g] \equiv [f + g], \quad [f] \cdot [g] \equiv [f \cdot g].$$

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

$$\bar{f}(n) \equiv \begin{cases} 1/f(n), & \text{если } f(n) \neq 0 \\ 1, & \text{в противном случае.} \end{cases}$$

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 $[g]$. Причем выполняются следующие свойства

IV. 4.1. $\alpha \not< \alpha$.

4.2. Если $\alpha < \beta$ и $\beta < \gamma$, то $\alpha < \gamma$.

4.3. Для любых α и β : 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 α через $n\alpha$ будем обозначать сумму n слагаемых, каждое из которых равно α .

Для действительных чисел выполняется **Аксиома Архимеда**: для любого положительного действительного числа α и любого действительного числа β 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 β 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 ε 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

$$f^*([(g^{(1)}(n))_{n \in N}], \dots, [(g^{(m)}(n))_{n \in N}]) \Leftrightarrow [(f(g^{(1)}(n)), \dots, f(g^{(m)}(n)))_{n \in N}].$$

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 $(\mathbb{R}^*)^m$:

$$p^*([(g^{(1)}(n))_{n \in N}], \dots, [(g^{(m)}(n))_{n \in N}]) = \text{И} \iff \{n \mid p(g^{(1)}(n), \dots, g^{(m)}(n)) = \text{И}\} \in F.$$

Предикат p^* называется *гиперрасширением* предиката p^* .

Для произвольной формулы Φ , 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 , $\&$ и \vee и кванторов \forall и \exists обозначим через Φ^* формулу, полученную из формулы Φ 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 $p^*(x_1, \dots, x_m)$.

Из доказанной выше теоремы Лося 3.6.3 следует

Принцип переноса Г. В. Лейбница Если все свободные переменные формулы Φ 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 $\Phi_{x_1, \dots, x_n}^*[\alpha_1, \dots, \alpha_n]$.

3.5. Исчисление предикатов

3.5.1. Логические аксиомы и правила вывода

Алфавит $\Sigma_{\text{ИП}_\tau}$ Исчисления Предикатов ИП_τ сигнатуры τ совпадает с **Алфавитом $\Sigma_{\text{ЛП}_\tau}$ Логики Предикатов ЛП_τ** сигнатуры τ .

Понятия **терма** и **формулы Исчисления Предикатов ИП_τ** сигнатуры τ совпадают с понятиями **терма** и **формулы Логики Предикатов ЛП_τ** сигнатуры τ , т. е. язык $L_{\text{ИП}_\tau}$ **Исчисления Предикатов ИП_τ** сигнатуры τ совпадает с языком $L_{\text{ЛП}_\tau}$ **Логики Предикатов ЛП_τ** сигнатуры τ . В дальнейшем язык $L_{\text{ИП}_\tau}$ **Исчисления Предикатов ИП_τ** сигнатуры τ мы будем обозначать через L_τ , а наряду с обозначением ИП_τ для **Исчисления Предикатов** сигнатуры τ будем использовать обозначение **ИП** в ситуациях, когда из контекста ясно, о какой сигнатуре идет речь.

Теперь мы приступаем к определению двух важнейших понятий **Исчисления Предикатов** - понятия **ВЫВОДА** и понятия **ВЫВОДИМОЙ ФОРМУЛЫ**. Эти понятия определяются аналогично тому, как это было сделано в случае **Исчисления Высказываний**.

Аксиомы Исчисления Предикатов

Зафиксируем произвольную сигнатуру τ . Все последующие определения будут относиться к **Исчислению Предикатов ИП_τ** этой сигнатуры τ , которое ради некоторой краткости будем называть просто **Исчислением Предикатов** и обозначать через **ИП** (без упоминания сигнатуры τ).

Для произвольных формул \mathcal{A} , \mathcal{B} и \mathcal{C} **Исчисления Предикатов** любая формула любого указанного ниже вида является **Логической Аксиомой Исчисления Предикатов**.

I $_{\rightarrow}$.

- I.1. $(\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{A}))$.
- I.2. $((\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})) \rightarrow ((\mathcal{A} \rightarrow \mathcal{B}) \rightarrow (\mathcal{A} \rightarrow \mathcal{C})))$.

II $_{\&}$.

- II.1. $((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{A})$.
- II.2. $((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{B})$.
- II.3. $((\mathcal{C} \rightarrow \mathcal{A}) \rightarrow ((\mathcal{C} \rightarrow \mathcal{B}) \rightarrow (\mathcal{C} \rightarrow (\mathcal{A} \& \mathcal{B}))))$.

III $_{\vee}$.

- III.1. $(\mathcal{A} \rightarrow (\mathcal{A} \vee \mathcal{B}))$.
- III.2. $(\mathcal{B} \rightarrow (\mathcal{A} \vee \mathcal{B}))$.
- III.3. $((\mathcal{A} \rightarrow \mathcal{C}) \rightarrow ((\mathcal{B} \rightarrow \mathcal{C}) \rightarrow ((\mathcal{A} \vee \mathcal{B}) \rightarrow \mathcal{C})))$.

IV $_{\neg}$.

- IV.1. $((\mathcal{A} \rightarrow (\neg \mathcal{B})) \rightarrow (\mathcal{B} \rightarrow (\neg \mathcal{A})))$.
- IV.2. $((\neg(\neg \mathcal{A})) \rightarrow \mathcal{A})$.

Для произвольной формулы \mathcal{A} **Исчисления Предикатов** и любого термина t допустимого для подстановки в формулу \mathcal{A} вместо свободных вхождений переменной x любая формула любого указанного ниже вида является **Логической Аксиомой Исчисления Предикатов**.

V $_{\forall}$.

- V.1. $((\forall x)\mathcal{A} \rightarrow \mathcal{A}_x[t])$.

VI $_{\exists}$.

- VI.1. $(\mathcal{A}_x[t] \rightarrow (\exists x)\mathcal{A})$.

В формуле $(\mathcal{A} \rightarrow \mathcal{B})$ подформула \mathcal{A} называется *антецедентом* или *посылкой*, а подформула \mathcal{B} – *консеквентом* или *заключением*. Поэтому аксиома I.1 носит название "Утверждение антецедента" или "Утверждение посылки". Аксиома I.2 называется "Самодистрибутивность импликации".

Правила Вывода Исчисления Предикатов

В **Исчислении Предикатов** используются три **Правила Вывода** – **Правило Отделения** (*Modus Ponens*), **Правило Введения** \forall и **Правило Введения** \exists .

Правило Отделения (кратко это правило будем обозначать через **MP**):

$$\frac{\mathcal{A}, (\mathcal{A} \rightarrow \mathcal{B})}{\mathcal{B}}.$$

Эта запись означает, что по правилу **MP** из формул \mathcal{A} и $(\mathcal{A} \rightarrow \mathcal{B})$ получается формула \mathcal{B} . При этом формулы \mathcal{A} и $(\mathcal{A} \rightarrow \mathcal{B})$ называются **посылками**.

правила **МР**, а формула \mathcal{B} – его **заключением** или непосредственным **следствием** формул \mathcal{A} и $(\mathcal{A} \rightarrow \mathcal{B})$ по правилу **МР**.

Правило Введения \forall :

$$\frac{(\mathcal{B} \rightarrow \mathcal{A})}{(\mathcal{B} \rightarrow (\forall x)\mathcal{A})},$$

при условии, что переменная x не входит свободно в формулу \mathcal{B} .

Эта запись означает, что по **Правилу Введения \forall** из формулы $(\mathcal{B} \rightarrow \mathcal{A})$ получается формула $(\mathcal{B} \rightarrow (\forall x)\mathcal{A})$. При этом формула $(\mathcal{B} \rightarrow \mathcal{A})$ называется **посылкой Правила Введения \forall** , а формула $(\mathcal{B} \rightarrow (\forall x)\mathcal{A})$ – его **заключением** или **непосредственным следствием** формулы $(\mathcal{B} \rightarrow \mathcal{A})$ по этому правилу.

Правило Введения \exists :

$$\frac{(\mathcal{A} \rightarrow \mathcal{B})}{((\exists x)\mathcal{A} \rightarrow \mathcal{B})},$$

при условии, что переменная x не входит свободно в формулу \mathcal{B} .

Эта запись означает, что по **Правилу Введения \exists** из формулы $(\mathcal{A} \rightarrow \mathcal{B})$ получается формула $((\exists x)\mathcal{A} \rightarrow \mathcal{B})$. При этом формула $(\mathcal{A} \rightarrow \mathcal{B})$ называется **посылкой Правила Введения \exists** , а формула $((\exists x)\mathcal{A} \rightarrow \mathcal{B})$ – его **заключением** или **непосредственным следствием** формулы $(\mathcal{A} \rightarrow \mathcal{B})$ по этому правилу.

Вывод и вывод из множества формул

Определение 3.5.1. *Выводом в Исчислении Предикатов называется любая конечная последовательность*

$$\mathcal{B}_1, \dots, \mathcal{B}_n$$

формул **Исчисления Предикатов**, удовлетворяющая следующему условию:
для любого i ($i = 1, \dots, n$)

либо

1) формула \mathcal{B}_i является **Логической Аксиомой Исчисления Предикатов**,

либо

2) найдутся числа j и k меньшие, чем i , такие, что формула \mathcal{B}_i получается из формул \mathcal{B}_j и \mathcal{B}_k по правилу **МР**,

либо

3) найдется число j меньшее, чем i , такое, что формула \mathcal{B}_i получается из формулы \mathcal{B}_j по правилу **Введения \forall** ,

либо

4) найдется число j меньшее, чем i , такое, что формула \mathcal{B}_i получается из формулы \mathcal{B}_j по правилу **Введения \exists** .

Определение 3.5.2. Формула B называется **выводимой в Исчислении Предикатов**, если существует **Вывод в Исчислении Предикатов**

$$B_1, \dots, B_n,$$

оканчивающийся этой формулой B .

Выражение $\vdash_{ИП} A$ служит сокращенной записью утверждения
”формула A выводима в Исчислении Предикатов”.

В дальнейшем для сокращения индекс *ИП* будем опускать, т. е. вместо $\vdash_{ИП} A$ будем писать просто $\vdash A$.

Доказательство следующей теоремы для **Исчисления Предикатов** дословно повторяет доказательство аналогичной теоремы для **Исчисления Высказываний**.

Теорема 3.5.1. Для любой формулы A формула $(A \rightarrow A)$ выводима в **Исчислении Предикатов**.

Доказательство. Чтобы доказать, что формула $(A \rightarrow A)$ **выводима в Исчислении Предикатов**, 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**. □

Напомним, что если $\alpha_1, \dots, \alpha_n$ – попарно различные буквы (символы) произвольного алфавита Σ , а X, Z_1, \dots, Z_n – слова, то через $X_{\alpha_1, \dots, \alpha_n} [Z_1, \dots, Z_n]$ мы обозначаем *результат одновременной замены всех вхождений букв $\alpha_1, \dots, \alpha_n$ в слово X соответственно на слова Z_1, \dots, Z_n* .

Слово $X_{\alpha_1, \dots, \alpha_n} [Z_1, \dots, Z_n]$ называется также *результатом подстановки в слово X слов Z_1, \dots, Z_n вместо букв $\alpha_1, \dots, \alpha_n$ соответственно*.

Пусть A – формула **Исчисления Высказываний**, все пропозициональные переменные которой содержатся среди A_1, \dots, A_n , а Φ_1, \dots, Φ_n – произвольные формулы **Исчисления Предикатов**. Индукцией по построению формул нетрудно доказать, что $A_{A_1, \dots, A_n} [\Phi_1, \dots, \Phi_n]$ – формула **Исчисления Предикатов**. Она называется *формулой, полученной из формулы **Исчисления Высказываний** A заменой пропозициональных переменных A_1, \dots, A_n на произвольные формулы **Исчисления Предикатов** Φ_1, \dots, Φ_n* .

В дальнейшем будет полезна следующая теорема.

Теорема 3.5.2. Если \mathcal{A} – тождественно истинная формула **Логике Высказываний**, все пропозициональные переменные которой содержатся среди A_1, \dots, A_n , а Φ_1, \dots, Φ_n – произвольные формулы **Исчисления Предикатов**, то формула $\mathcal{A}_{A_1, \dots, A_n}[\Phi_1, \dots, \Phi_n]$ выводима в **Исчислении Предикатов**.

Доказательство. Если \mathcal{A} – тождественно истинная формула **Логике Высказываний**, то она выводима в **Исчислении Высказываний**. Пусть последовательность формул **Исчисления Высказываний** B_1, B_2, \dots, B_m является **выводом** формулы \mathcal{A} . Предположим, что все пропозициональные переменные этих формул содержатся среди A_1, \dots, A_p .

С целью упрощения обозначений для произвольной формулы \mathcal{B} **Логике Высказываний** обозначим через \mathcal{B}^* формулу $\mathcal{B}_{A_1, \dots, A_p}[\Phi_1, \dots, \Phi_p]$.

Легко проверить, что последовательность формул $\mathcal{B}_1^*, \mathcal{B}_2^*, \dots, \mathcal{B}_m^*$ является **выводом в Исчислении Предикатов** формулы \mathcal{A}^* , т. е. формулы $\mathcal{A}_{A_1, \dots, A_n}[\Phi_1, \dots, \Phi_n]$. \square

Установление выводимости даже достаточно простых формул – процесс весьма трудоемкий. С целью облегчения изучения отношения выводимости $\vdash \mathcal{A}$, как и в случае **Исчисления Высказываний**, введем и изучим более общее понятие, чем понятие **Вывода** – понятие **Вывод из множества гипотез**.

Пусть Γ – произвольное множество формул. Формулы из множества Γ будем называть **гипотезами**. Смысл такого названия прояснится позже.

Определение 3.5.3. **Выводом в Исчислении Предикатов из множества формул Γ** называется любая конечная последовательность

$$B_1, \dots, B_n$$

формул **Исчисления Предикатов**, удовлетворяющая следующему условию:

для любого i ($i = 1, \dots, n$)

либо

0) $B_i \in \Gamma$ (формула B_i является **гипотезой**),

либо

1) формула B_i является **Логической Аксиомой Исчисления Предикатов**,

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 **MP**,

либо

3) найдется число j меньшее, чем i , такое, что формула B_i получается из формулы B_j по правилу **Введения \forall** ,

либо

4) найдется число j меньшее, чем i , такое, что формула B_i получается из формулы B_j по правилу **Введения \exists** .

Определение 3.5.4. Формула B называется **выводимой в Исчислении Предикатов из множества формул Γ** , если существует **Вывод в Исчислении Предикатов из множества формул Γ**

$$B_1, \dots, B_n,$$

оканчивающийся формулой B .

Выражение $\Gamma \vdash_{\text{ИП}} A$ служит сокращенной записью утверждения "**формула A выводима в Исчислении Предикатов из множества формул Γ** ". И вновь индекс *ИВ* не будем писать.

Несколько "туманное" понятие доказательства мы заменяем точным математическим понятием "**вывод в Исчислении Предикатов из множества формул Γ** ". При этом сами выводы – это просто конечные последовательности формул с определенными свойствами. Такой подход открывает возможность изучать сами выводы и их свойства, в частности, можно пытаться доказывать отсутствие (невозможность существования, невозможность построения) выводов с некоторыми заранее указанными свойствами, а значит, устанавливать невыводимость определенных формул.

Если Γ и Δ – два произвольных множества формул, то запись

$$\Gamma \vdash \Delta$$

означает, что **любая формула из множества Δ выводима в Исчислении Предикатов из множества формул Γ** .

Теорема 3.5.3. Если $\Gamma \vdash A$ и $\Gamma \subset \Gamma_1$, то $\Gamma_1 \vdash A$.

Если $\Gamma_1 \vdash A$, то найдется **конечное** подмножество Γ множества Γ_1 такое, что $\Gamma \vdash A$.

Д о к а з а т е л ь с т в о. Если $\Gamma \subset \Gamma_1$, то любой **вывод из множества формул Γ** будет и **выводом из множества формул Γ_1** .

Если $\Gamma_1 \vdash A$ и B_1, \dots, B_n – **вывод формулы A из множества формул Γ_1** , то в качестве Γ можно взять $\Gamma_1 \cap \{B_1, \dots, B_n\}$. \square

Лемма 3.5.1. Если $\Gamma_1 \vdash B$ и $\Gamma_2 \cup \{B\} \vdash A$, то $\Gamma_1 \cup \Gamma_2 \vdash A$.

Д о к а з а т е л ь с т в о. Пусть $\mathcal{D}_0: B_1, B_2, \dots, B_n = B$ – **вывод формулы B из множества формул Γ_1** .

По произвольному выводу $\mathcal{D}: A_1, A_2, \dots, A_m = A$ формулы A из множества формул $\Gamma_2 \cup \{B\}$ построим вывод $\mathcal{D}^*: A_1^*, A_2^*, \dots, A_p^* = A$ формулы A из множества формул $\Gamma_1 \cup \Gamma_2$:

для произвольного i ($i = 1, \dots, n$) заменим в выводе \mathcal{D} вхождение формулы A_i некоторой последовательностью формул с соответствующими комментариями по следующему правилу

если

0) $\mathcal{A}_i \in \Gamma_2 \cup \{\mathcal{B}\}$, то в случае $\mathcal{A}_i \in \Gamma_2$ вхождение формулы \mathcal{A}_i не меняется, а в случае $\mathcal{A}_i \in \{\mathcal{B}\}$, т. е. $\mathcal{A}_i = \{\mathcal{B}\}$, заменяем вхождение формулы \mathcal{A}_i на последовательность формул $\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_n = \mathcal{B} = \mathcal{A}_i$, являющуюся выводом формулы $\mathcal{B} = \mathcal{A}_i$ из множества формул Γ_1 , с соответствующим комментарием,

если

1) формула \mathcal{A}_i является **Логической Аксиомой Исчисления Предикатов**, то вхождение формулы \mathcal{A}_i и соответствующий ей комментарий не меняются,

если

2) найдутся числа j и k меньшие, чем i , такие, что формула \mathcal{A}_i получается из формул \mathcal{A}_j и \mathcal{A}_k по правилу **МР**, то вхождение формулы \mathcal{A}_i не меняется, а в соответствующем ей комментарии меняются лишь номера формул, из которых получается формула \mathcal{A}_i ,

если

3) найдется число j меньшее, чем i , такое, что формула \mathcal{A}_i получается из формулы \mathcal{A}_j по правилу **Введения** \forall , то вхождение формулы \mathcal{A}_i не меняется, а в соответствующем ей комментарии меняется лишь номер формулы, из которой получается формула \mathcal{A}_i ,

если

4) найдется число j меньшее, чем i , такое, что формула \mathcal{A}_i получается из формулы \mathcal{A}_j по правилу **Введения** \exists , то вхождение формулы \mathcal{A}_i не меняется, а в соответствующем ей комментарии меняется лишь номер формулы, из которой получается формула \mathcal{A}_i . \square

Теорема 3.5.4. Если $\Gamma_1 \vdash \Delta$ и $\Gamma_2 \cup \Delta \vdash \mathcal{A}$, то $\Gamma_1 \cup \Gamma_2 \vdash \mathcal{A}$.

Доказательство. В силу предыдущей теоремы можно считать, что множество Δ конечное, поэтому доказательство легко получается из предыдущей леммы индукцией по числу формул в множестве Δ . \square

Замечание. В дальнейшем по сложившейся традиции вместо записи

$$\Gamma_1 \cup \Gamma_2 \vdash \mathcal{A}$$

будем использовать запись

$$\Gamma_1, \Gamma_2 \vdash \mathcal{A},$$

а вместо записи

$$\Gamma_1, \{\mathcal{B}\} \vdash \mathcal{A} -$$

запись $\Gamma_1, \mathcal{B} \vdash \mathcal{A}$.

По мере необходимости будем доказывать вспомогательные теоремы, которые будут способствовать изучению отношения выводимости $\Gamma \vdash \mathcal{A}$.

Теорема 3.5.5. Для любого множества формул Γ и любых формул \mathcal{A} , \mathcal{B} и \mathcal{C} имеют место эквивалентности:

$$\begin{aligned} \Gamma \vdash (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})) & \text{ тогда и только тогда, когда } \Gamma \vdash (\mathcal{B} \rightarrow (\mathcal{A} \rightarrow \mathcal{C})), \\ \Gamma \vdash (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})) & \text{ тогда и только тогда, когда } \Gamma \vdash ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{C}). \end{aligned}$$

Замечание. Первую эквивалентность мы будем называть ”перестановкой посылок”, а вторую – ”объединением-разъединением посылок”.

Д о к а з а т е л ь с т в о. Непосредственная проверка показывает, что следующие формулы **Логике Высказываний** являются тождественно истинными

$$\begin{aligned} ((A_1 \rightarrow (A_2 \rightarrow A_3)) \rightarrow (A_2 \rightarrow (A_1 \rightarrow A_3))), \\ ((A_1 \rightarrow (A_2 \rightarrow A_3)) \rightarrow ((A_1 \& A_2) \rightarrow A_3)), \\ (((A_1 \& A_2) \rightarrow A_3) \rightarrow (A_1 \rightarrow (A_2 \rightarrow A_3))). \end{aligned}$$

Поэтому по теореме 3.5.2 для любых формул \mathcal{A} , \mathcal{B} и \mathcal{C} **Исчисления Предикатов** в нем выводимы следующие формулы

$$\begin{aligned} ((\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})) \rightarrow (\mathcal{B} \rightarrow (\mathcal{A} \rightarrow \mathcal{C}))), \\ ((\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})) \rightarrow ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{C})), \\ (((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{C}) \rightarrow (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C}))). \end{aligned}$$

Если $\Gamma \vdash (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C}))$, то в силу

$$\vdash ((\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})) \rightarrow (\mathcal{B} \rightarrow (\mathcal{A} \rightarrow \mathcal{C})))$$

получаем $\Gamma \vdash (\mathcal{B} \rightarrow (\mathcal{A} \rightarrow \mathcal{C}))$.

Если $\Gamma \vdash (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C}))$, то в силу

$$\vdash ((\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})) \rightarrow ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{C}))$$

получаем

$$\Gamma \vdash ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{C}).$$

Обратно, если $\Gamma \vdash ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{C})$, то в силу

$$\vdash (((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{C}) \rightarrow (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})))$$

получаем

$$\Gamma \vdash (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})).$$

□

3.5.2. Теорема дедукции

В этом параграфе мы докажем теорему, которая значительно облегчает изучение отношения $\Gamma \vdash \mathcal{A}$. Эта теорема аналогична **Теореме Дедукции**, доказанной выше для **Исчисления Высказываний**, и называется **Теорема Дедукции** для **Исчисления Предикатов**.

Теорема Дедукции. Если $\Gamma, \mathcal{A} \vdash \mathcal{B}$ и существует вывод D формулы \mathcal{B} из множества формул $\Gamma \cup \{\mathcal{A}\}$, в котором **Правило Введения** \forall и **Правило Введения** \exists не применяются по переменным, входящим свободно в формулу \mathcal{A} , то $\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B})$.

Обратно, если $\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B})$, то $\Gamma, \mathcal{A} \vdash \mathcal{B}$.

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 $D: \mathcal{B}_1, \dots, \mathcal{B}_n$ – вывод формулы \mathcal{B} из множества формул $\Gamma \cup \{\mathcal{A}\}$, в котором **Правило Введения** \forall и **Правило Введения** \exists не применяются по переменным, входящим свободно в формулу \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 четыре 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 3.5.3 и 3.5.4 получаем

$$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B}_i).$$

Если же $\mathcal{B}_i \in \{\mathcal{A}\}$, то $\mathcal{B}_i = \mathcal{A}$.

Тогда по теореме 3.5.1

$$\vdash (\mathcal{A} \rightarrow \mathcal{B}_i).$$

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 3.5.3 и 3.5.4 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 **MP**.

Тогда

$$\mathcal{B}_k \equiv (\mathcal{B}_j \rightarrow \mathcal{B}_i).$$

По индуктивному предположению имеем

$$\begin{aligned} \Gamma &\vdash (\mathcal{A} \rightarrow \mathcal{B}_j), \\ \Gamma &\vdash (\mathcal{A} \rightarrow \mathcal{B}_k), \end{aligned}$$

т. е.

$$\Gamma \vdash (\mathcal{A} \rightarrow (\mathcal{B}_j \rightarrow \mathcal{B}_i)).$$

Так как

$$\begin{aligned} &\vdash ((\mathcal{A} \rightarrow (\mathcal{B}_j \rightarrow \mathcal{B}_i)) \rightarrow ((\mathcal{A} \rightarrow \mathcal{B}_j)) \rightarrow (\mathcal{A} \rightarrow \mathcal{B}_i)) \\ &\quad \text{то} \\ &(\mathcal{A} \rightarrow (\mathcal{B}_j \rightarrow \mathcal{B}_i)), (\mathcal{A} \rightarrow \mathcal{B}_j) \vdash (\mathcal{A} \rightarrow \mathcal{B}_i)). \end{aligned}$$

Поэтому по теореме 3.5.4 получаем

$$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B}_i).$$

3) Найдется число j меньшее, чем i , такое, что формула \mathcal{B}_i получается из формулы \mathcal{B}_j по правилу **Введения** \forall ,

Тогда

$$\mathcal{B}_j \equiv (\mathcal{E} \rightarrow \mathcal{C}), \quad \mathcal{B}_i \equiv (\mathcal{E} \rightarrow (\forall x)\mathcal{C})$$

и переменная x не входит свободно в формулу \mathcal{E} .

По индуктивному предположению имеем

$$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B}_j),$$

т. е.

$$\Gamma \vdash (\mathcal{A} \rightarrow (\mathcal{E} \rightarrow \mathcal{C})).$$

По теореме 3.5.5 получаем

$$\Gamma \vdash ((\mathcal{A} \& \mathcal{E}) \rightarrow \mathcal{C}).$$

По предположению переменная x не входит свободно в формулы \mathcal{A} и \mathcal{E} . Применив **Правило Введения** \forall , получим

$$\Gamma \vdash ((\mathcal{A} \& (\mathcal{E}) \rightarrow (\forall x)\mathcal{C}).$$

По теореме 3.5.5 получаем

$$\Gamma \vdash (\mathcal{A} \rightarrow (\mathcal{E} \rightarrow (\forall x)\mathcal{C})),$$

т. е.

$$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B}_i).$$

4) Найдется число j меньшее, чем i , такое, что формула \mathcal{B}_i получается из формулы \mathcal{B}_j по правилу **Введения** \exists .

Тогда

$$\mathcal{B}_j = (\mathcal{C} \rightarrow \mathcal{E}), \quad \mathcal{B}_i = ((\exists x)\mathcal{C} \rightarrow \mathcal{E}),$$

и переменная x не входит свободно в формулу \mathcal{E} .

По индуктивному предположению имеем

$$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B}_j),$$

т. е.

$$\Gamma \vdash (\mathcal{A} \rightarrow (\mathcal{C} \rightarrow \mathcal{E})).$$

По теореме 3.5.5 получаем

$$\Gamma \vdash (\mathcal{C} \rightarrow (\mathcal{A} \rightarrow \mathcal{E})).$$

По предположению переменная x не входит свободно в формулы \mathcal{A} и \mathcal{E} . Применив **Правило Введения** \exists , получим

$$\Gamma \vdash ((\exists x)\mathcal{C} \rightarrow (\mathcal{A} \rightarrow \mathcal{E})).$$

По теореме 3.5.5 получаем

$$\Gamma \vdash (\mathcal{A} \rightarrow ((\exists x)\mathcal{C} \rightarrow \mathcal{E})),$$

т. е.

$$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B}_i).$$

При $i = n$ получаем

$$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B}).$$

Для доказательства второй части теоремы предположим, что

$$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B}).$$

Так как

$$\mathcal{A} \vdash \mathcal{A}$$

и

$$\mathcal{A}, (\mathcal{A} \rightarrow \mathcal{B}) \vdash \mathcal{B},$$

то по теореме 3.5.4 получаем

$$\Gamma, \mathcal{A} \vdash \mathcal{B}.$$

Это завершает доказательство теоремы. □

Следствие 3.5.5.1. Если $\Gamma, \mathcal{A} \vdash \mathcal{B}$ и существует вывод D формулы \mathcal{B} из множества формул $\Gamma \cup \{\mathcal{A}\}$, в котором применяется лишь **Правило Отделения МР**, то $\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B})$.

Теорема 3.5.6. Для любых формул \mathcal{A} и \mathcal{B}

$$\vdash (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow (\mathcal{A} \& \mathcal{B}))).$$

Д о к а з а т е л ь с т в о. Доказательство следует из теоремы 3.5.2, если воспользоваться тождественно истинной формулой **Логика Выводимости**

$$(\mathcal{A}_1 \rightarrow (\mathcal{A}_2 \rightarrow (\mathcal{A}_1 \& \mathcal{A}_2))).$$

□

Теорема 3.5.7. Для любых формул \mathcal{A} и \mathcal{B} и любого множества формул Γ имеет место эквивалентность:

$$\Gamma \vdash \mathcal{A} \quad \text{и} \quad \Gamma \vdash \mathcal{B}$$

тогда и только тогда, когда

$$\Gamma \vdash (\mathcal{A} \& \mathcal{B}).$$

Д о к а з а т е л ь с т в о. По предыдущей теореме

$$\vdash (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow (\mathcal{A} \& \mathcal{B}))),$$

кроме того,

$$\mathcal{A}, \mathcal{B}, (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow (\mathcal{A} \& \mathcal{B}))) \vdash (\mathcal{A} \& \mathcal{B}).$$

Откуда по теореме 3.5.4 получаем

$$\mathcal{A}, \mathcal{B} \vdash (\mathcal{A} \& \mathcal{B}).$$

Если

$$\Gamma \vdash \mathcal{A} \quad \text{и} \quad \Gamma \vdash \mathcal{B},$$

то применив Теорему 3.5.7, получим

$$\Gamma \vdash (\mathcal{A} \& \mathcal{B}).$$

Для доказательства обратного утверждения предположим, что

$$\Gamma \vdash (\mathcal{A} \& \mathcal{B}).$$

Используя **логические аксиомы** II.1 и II.2 и **Теорему Дедукции** (ее вторую часть), получаем

$$(\mathcal{A} \& \mathcal{B}) \vdash \mathcal{A} \quad \text{и} \quad (\mathcal{A} \& \mathcal{B}) \vdash \mathcal{B},$$

поэтому, применив теорему 3.5.4, получим

$$\Gamma \vdash \mathcal{A} \quad \text{и} \quad \Gamma \vdash \mathcal{B}.$$

□

Теорема 3.5.8. Для любой формулы \mathcal{A}

$$\vdash (\mathcal{A} \rightarrow (\neg(\neg\mathcal{A}))).$$

Доказательство. Доказательство следует из теоремы 3.5.2, если воспользоваться тождественно истинной формулой **Логика Высказываний**

$$(\mathcal{A}_1 \rightarrow (\neg(\neg\mathcal{A}_1))).$$

□

Для любых двух формул \mathcal{A} и \mathcal{B} запись $\mathcal{A} \leftrightarrow \mathcal{B}$ будет служить сокращенным обозначением формулы $((\mathcal{A} \rightarrow \mathcal{B}) \& (\mathcal{B} \rightarrow \mathcal{A}))$.

Следствие 3.5.8.1. Для любой формулы \mathcal{A} и любого множества формул Γ имеем

- 1) $\mathcal{A} \vdash (\neg(\neg\mathcal{A}))$,
- 2) $(\neg(\neg\mathcal{A})) \vdash \mathcal{A}$,
- 3) $\Gamma \vdash \mathcal{A} \iff \Gamma \vdash (\neg(\neg\mathcal{A}))$,
- 4) $\vdash (\mathcal{A} \leftrightarrow (\neg(\neg\mathcal{A})))$.

Доказательство. 1) В силу предыдущей теоремы 3.5.8

$$\vdash (\mathcal{A} \rightarrow (\neg(\neg\mathcal{A}))),$$

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 3.5.4 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 3.5.7 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 3.5.9. Для любых формул \mathcal{A} и \mathcal{B}

$$\begin{aligned} 1) \vdash (\mathcal{A} \rightarrow ((\neg \mathcal{A}) \rightarrow \mathcal{B})), \quad 2) \vdash ((\neg \mathcal{A}) \rightarrow (\mathcal{A} \rightarrow \mathcal{B})), \\ 3) \mathcal{A}, (\neg \mathcal{A}) \vdash \mathcal{B}, \\ 4) \vdash ((\mathcal{A} \& (\neg \mathcal{A})) \rightarrow \mathcal{B}), \quad 5) (\mathcal{A} \& (\neg \mathcal{A})) \vdash \mathcal{B}. \end{aligned}$$

Д о к а з а т е л ь с т в о. Доказательство пунктов 1) и 2) следует из теоремы 3.5.2, если воспользоваться тождественно истинными формулами **Логики Высказываний**

$$(\mathcal{A}_1 \rightarrow ((\neg \mathcal{A}_1) \rightarrow \mathcal{A}_2)) \quad \text{и} \quad ((\neg \mathcal{A}_1) \rightarrow (\mathcal{A}_1 \rightarrow \mathcal{A}_2))$$

Пункт 3) легко следует из 1).

Доказательство пункта 4) следует из теоремы 3.5.2, если воспользоваться тождественно истинной формулой **Логики Высказываний**

$$((\mathcal{A}_1 \& (\neg \mathcal{A}_1)) \rightarrow \mathcal{A}_2).$$

Пункт 5) легко следует из 4). □

Определение 3.5.5. Множество формул Γ называется **противоречивым**, если найдется такая формула \mathcal{A} , что

$$\Gamma \vdash \mathcal{A} \quad \text{и} \quad \Gamma \vdash (\neg \mathcal{A}),$$

в противном случае множество формул Γ называется **непротиворечивым**.

Теорема 3.5.10. Если Γ – противоречивое множество формул, то для любой формулы \mathcal{B}

$$\Gamma \vdash \mathcal{B}.$$

Д о к а з а т е л ь с т в о. Если Γ – противоречивое множество формул, то найдется такая формула \mathcal{A} , что

$$\Gamma \vdash \mathcal{A} \quad \text{и} \quad \Gamma \vdash (\neg \mathcal{A}).$$

Пусть \mathcal{B} – произвольная формула. По предыдущей теореме 3.5.9

$$\mathcal{A}, (\neg \mathcal{A}) \vdash \mathcal{B}.$$

Поэтому по теореме 3.5.4

$$\Gamma \vdash \mathcal{B}.$$

□

Теорема 3.5.11. *Множество формул Γ языка L_{II} 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 Γ_1 множества формул Γ языка L_{II} является **противоречивым**, то возьмем такую формулу \mathcal{A} , что

$$\Gamma_1 \vdash \mathcal{A} \quad \text{и} \quad \Gamma_1 \vdash (\neg \mathcal{A}),$$

но тогда

$$\Gamma \vdash \mathcal{A} \quad \text{и} \quad \Gamma \vdash (\neg \mathcal{A}),$$

т. е. и само множество формул Γ является **противоречивым**.

Если **противоречивым** является само множество формул Γ языка L_{II} , то возьмем такую формулу \mathcal{A} , что

$$\Gamma \vdash \mathcal{A} \quad \text{и} \quad \Gamma \vdash (\neg \mathcal{A}).$$

Пусть \mathcal{D} – вывод из множества формул Γ формулы \mathcal{A} , а \mathcal{D}_1 – вывод из множества формул Γ формулы $(\neg \mathcal{A})$.

Если Γ_1 – это множество всех формул из множества Γ , входящих в \mathcal{D} или в \mathcal{D}_1 , то, очевидно,

$$\Gamma_1 \vdash \mathcal{A} \quad \text{и} \quad \Gamma_1 \vdash (\neg \mathcal{A}).$$

Остается заметить, что Γ_1 – конечное множество формул. □

Теорема 3.5.12. *Для любых формул \mathcal{A} , \mathcal{B} и \mathcal{C}*

$$(\mathcal{A} \rightarrow \mathcal{B}), (\mathcal{B} \rightarrow \mathcal{C}) \vdash (\mathcal{A} \rightarrow \mathcal{C}).$$

Д о к а з а т е л ь с т в о. Покажем, что для любых формул \mathcal{A} , \mathcal{B} и \mathcal{C}

$$\vdash ((\mathcal{A} \rightarrow \mathcal{B}) \rightarrow ((\mathcal{B} \rightarrow \mathcal{C}) \rightarrow (\mathcal{A} \rightarrow \mathcal{C}))),$$

и затем два раза применим вторую часть **Теоремы Дедукции**.

Доказательство следует из теоремы 3.5.2, если воспользоваться тождественно истинной формулой **Логика Высказываний**

$$((A_1 \rightarrow A_2) \rightarrow ((A_2 \rightarrow A_3) \rightarrow (A_1 \rightarrow A_3))).$$

□

Следствие 3.5.12.1. *Для любых формул \mathcal{A} , \mathcal{B} , \mathcal{C} и любого множества формул Γ : если*

$$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B}) \quad \text{и} \quad \Gamma \vdash (\mathcal{B} \rightarrow \mathcal{C}),$$

то

$$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{C}).$$

Д о к а з а т е л ь с т в о. Для доказательства достаточно воспользоваться только что доказанной теоремой 3.5.12 и теоремой 3.5.4. \square

Теорема 3.5.13. *Для любых формул \mathcal{A} , \mathcal{B} и \mathcal{C}*

$$(\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})) \vdash (\mathcal{B} \rightarrow (\mathcal{A} \rightarrow \mathcal{C})).$$

Д о к а з а т е л ь с т в о. Доказательство следует из теоремы 3.5.2, если воспользоваться тождественно истинной формулой **Логики Высказываний**

$$((A_1 \rightarrow (A_2 \rightarrow A_3)) \rightarrow (A_2 \rightarrow (A_1 \rightarrow A_3))).$$

\square

Следствие 3.5.13.1. *Для любых формул \mathcal{A} , \mathcal{B} и \mathcal{C} и любого множества формул Γ : если*

$$\Gamma \vdash (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})),$$

то

$$\Gamma \vdash (\mathcal{B} \rightarrow (\mathcal{A} \rightarrow \mathcal{C})).$$

Д о к а з а т е л ь с т в о. следует из предыдущей теоремы 3.5.13 и теоремы 3.5.4. \square

Следствие 3.5.13.2. *Для любых формул \mathcal{A} , \mathcal{B} , \mathcal{C} и любого множества формул Γ : если*

$$\Gamma \vdash (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})),$$

то

$$\Gamma \vdash ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{C}).$$

Д о к а з а т е л ь с т в о. Из теоремы 3.5.2, воспользовавшись тождественно истинной формулой **Логики Высказываний**

$$((A_1 \rightarrow (A_2 \rightarrow A_3)) \rightarrow ((A_1 \& A_2) \rightarrow A_3)),$$

получаем, что для любых формул \mathcal{A} , \mathcal{B} и \mathcal{C}

$$\vdash ((\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})) \rightarrow ((\mathcal{A} \& \mathcal{A}) \rightarrow \mathcal{C})).$$

Поэтому если

$$\Gamma \vdash (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})),$$

то

$$\Gamma \vdash ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{C}).$$

\square

Теорема 3.5.14. Для любых формул \mathcal{A} и \mathcal{B}

1. $\vdash (((\neg \mathcal{B}) \rightarrow (\neg \mathcal{A})) \rightarrow (\mathcal{A} \rightarrow \mathcal{B})),$
2. $\vdash ((\mathcal{A} \rightarrow \mathcal{B}) \rightarrow ((\neg \mathcal{B}) \rightarrow (\neg \mathcal{A}))),$
3. $((\neg \mathcal{B}) \rightarrow (\neg \mathcal{A})) \vdash (\mathcal{A} \rightarrow \mathcal{B}),$
4. $(\mathcal{A} \rightarrow \mathcal{B}) \vdash ((\neg \mathcal{B}) \rightarrow (\neg \mathcal{A})),$
5. $\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B})$ тогда и только тогда, когда $\Gamma \vdash ((\neg \mathcal{B}) \rightarrow (\neg \mathcal{A})).$
6. Для любых замкнутых формул \mathcal{A} и \mathcal{B}
 $\Gamma, \mathcal{A} \vdash \mathcal{B}$ тогда и только тогда, когда $\Gamma, (\neg \mathcal{B}) \vdash (\neg \mathcal{A}).$

Доказательство. Доказательство пунктов 1) и 2) следует из теоремы 3.5.2, если воспользоваться тождественно истинными формулами **Логике Высказываний**

$$\begin{aligned} & (((\neg A_2) \rightarrow (\neg A_1)) \rightarrow (A_1 \rightarrow A_2)), \\ & ((A_1 \rightarrow A_2) \rightarrow ((\neg A_2) \rightarrow (\neg A_1))). \end{aligned}$$

Доказательство пунктов 3), 4) и 5) следует из пунктов 1) и 2).

Используя **Теорему Дедукции**, из пункта 5) легко получаем 6). \square

Теорема 3.5.15. Для любых формул \mathcal{A} и \mathcal{B}

- 1) $\vdash (\mathcal{A} \rightarrow ((\neg \mathcal{B}) \rightarrow (\neg(\mathcal{A} \rightarrow \mathcal{B})))),$
- 2) $\mathcal{A}, (\neg \mathcal{B}) \vdash (\neg(\mathcal{A} \rightarrow \mathcal{B})).$

Доказательство. Доказательство пункта 1) следует из теоремы 3.5.2, если воспользоваться тождественно истинной формулой **Логике Высказываний**

$$((A_1) \rightarrow ((\neg A_2) \rightarrow \neg(A_1 \rightarrow A_2))).$$

Пункт 2) легко следует из 1). \square

Теорема 3.5.16. Для любых формул \mathcal{A} и \mathcal{B}

- 1) $\vdash ((\mathcal{A} \rightarrow \mathcal{B}) \rightarrow (((\neg \mathcal{A}) \rightarrow \mathcal{B}) \rightarrow \mathcal{B})),$
- 2) $(\mathcal{A} \rightarrow \mathcal{B}), ((\neg \mathcal{A}) \rightarrow \mathcal{B}) \vdash \mathcal{B}.$
- 3) Если \mathcal{A} – замкнутая формула, $\Gamma, \mathcal{A} \vdash \mathcal{B}$ и $\Gamma, (\neg \mathcal{A}) \vdash \mathcal{B}$, то $\Gamma \vdash \mathcal{B}.$

Доказательство. Доказательство пункта 1) следует из теоремы 3.5.2, если воспользоваться тождественно истинной формулой **Логике Высказываний** $((A_1 \rightarrow A_2) \rightarrow (((\neg A_1) \rightarrow A_2) \rightarrow A_2)).$

Пункт 2) легко следует из 1).

Если $\Gamma, \mathcal{A} \vdash \mathcal{B}$ и $\Gamma, (\neg \mathcal{A}) \vdash \mathcal{B}$ и \mathcal{A} – замкнутая формула, то по **Теореме Дедукции**

$$\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B})$$

и

$$\Gamma \vdash ((\neg \mathcal{A}) \rightarrow \mathcal{B}).$$

И остается воспользоваться теоремой 3.5.4. \square

Теорема 3.5.17 (Закон исключенного третьего). Для любой формулы \mathcal{A}

$$\vdash (\mathcal{A} \vee (\neg \mathcal{A})).$$

Доказательство. Доказательство следует из теоремы 3.5.2, если воспользоваться тождественно истинной формулой **Логика Высказываний**

$$(A_1 \vee (\neg A_1)).$$

□

Теорема 3.5.18. Для любого множества формул Γ , произвольной формулы \mathcal{A} и индивидуальной переменной v справедлива эквивалентность

$$\Gamma \vdash \mathcal{A} \text{ тогда и только тогда, когда } \Gamma \vdash (\forall v)\mathcal{A}.$$

Доказательство. Пусть \mathcal{B} – произвольная замкнутая формула, выводимая из Γ . Тогда последовательно получаем $\Gamma \vdash (\mathcal{B} \rightarrow \mathcal{A})$, $\Gamma \vdash (\mathcal{B} \rightarrow (\forall v)\mathcal{A})$ и $\Gamma \vdash (\forall v)\mathcal{A}$.

Для доказательства обратного утверждения предположим, что

$$\Gamma \vdash (\forall v)\mathcal{A}$$

и, воспользовавшись логической аксиомой $((\forall v)\mathcal{A} \rightarrow \mathcal{A})$, получим, что $\Gamma \vdash \mathcal{A}$. □

Индукцией по n получаем следующее следствие, которое будем называть **Правилом Обобщения**.

Следствие 3.5.18.1. Если v_1, \dots, v_n – индивидуальные переменные и $\Gamma \vdash \mathcal{A}$, то

$$\Gamma \vdash (\forall v_1) \dots (\forall v_n)\mathcal{A}.$$

Конечно, справедливо и обратное утверждение.

Следствие 3.5.18.2. Если v_1, \dots, v_n – индивидуальные переменные и

$$\Gamma \vdash (\forall v_1) \dots (\forall v_n)\mathcal{A},$$

то $\Gamma \vdash \mathcal{A}$.

Следующее следствие будем называть **Правилом Замыкания**.

Следствие 3.5.18.3. Если $\Gamma \vdash \mathcal{A}$, то $\Gamma \vdash \forall \mathcal{A}$, где $\forall \mathcal{A}$ – \forall -замыкание формулы \mathcal{A} .

Конечно, справедливо и обратное утверждение.

Следствие 3.5.18.4. Если $\Gamma \vdash \forall \mathcal{A}$, то $\Gamma \vdash \mathcal{A}$.

Следующая теорема будет называться **Правилом Подстановки**.

Теорема 3.5.19. *Если v_1, \dots, v_n – индивидные переменные, t_1, \dots, t_n – термы, допустимые для подстановки в формулу \mathcal{A} вместо свободных вхождений переменных v_1, \dots, v_n и $\Gamma \vdash \mathcal{A}$, то $\Gamma \vdash \mathcal{A}_{v_1, \dots, v_n}[t_1, \dots, t_n]$.*

Д о к а з а т е л ь с т в о. Проведем индукцию по n . При $n = 1$ из $\Gamma \vdash \mathcal{A}$ в силу предыдущей теоремы получаем $\Gamma \vdash (\forall v_1)\mathcal{A}$. Что вместе с логической аксиомой $((\forall v_1)\mathcal{A} \rightarrow \mathcal{A}_{v_1}[t_1])$ дает $\Gamma \vdash \mathcal{A}_{v_1}[t_1]$.

Предположим, что утверждение доказано для n . Докажем его для $n + 1$.

Пусть v_1, \dots, v_{n+1} – индивидные переменные, t_1, \dots, t_{n+1} – термы, допустимые для подстановки в формулу \mathcal{A} вместо свободных вхождений переменных v_1, \dots, v_{n+1} . Выберем индивидную переменную y , не входящую ни в термы t_1, \dots, t_{n+1} , ни в формулу \mathcal{A} и отличную от переменных v_1, \dots, v_{n+1} . Тогда выполняется равенство

$$((\mathcal{A}_{v_{n+1}}[y])_{v_1, \dots, v_n}[t_1, \dots, t_n])_y[t_{n+1}] \equiv (\mathcal{A}_{v_1, \dots, v_n, v_{n+1}}[t_1, \dots, t_n, n+1]).$$

Используя это равенство, последовательно получаем

$$\begin{aligned} \Gamma \vdash \mathcal{A}_{v_{n+1}}[y], \quad \Gamma \vdash (\mathcal{A}_{v_{n+1}}[y])_{v_1, \dots, v_n}[t_1, \dots, t_n], \\ \Gamma \vdash ((\mathcal{A}_{v_{n+1}}[y])_{v_1, \dots, v_n}[t_1, \dots, t_n])_y[t_{n+1}], \quad \Gamma \vdash \mathcal{A}_{v_1, \dots, v_n, v_{n+1}}[t_1, \dots, t_n, n+1]. \end{aligned}$$

□

Пусть v_1, \dots, v_n – попарно различные переменные. Индукцией по n легко установить, что для любой формулы \mathcal{A}

$$\vdash (\mathcal{A} \rightarrow (\exists v_1) \dots (\exists v_n)\mathcal{A}), \quad \vdash ((\forall v_1) \dots (\forall v_n)\mathcal{A} \rightarrow \mathcal{A}).$$

Используя это замечание, получаем следствие предыдущей теоремы.

Следствие 3.5.19.1. *Если v_1, \dots, v_n – индивидные переменные, t_1, \dots, t_n – термы, допустимые для подстановки в формулу \mathcal{A} вместо свободных вхождений переменных v_1, \dots, v_n , то*

$$\begin{aligned} \vdash (\mathcal{A}_{v_1, \dots, v_n}[t_1, \dots, t_n] \rightarrow (\exists v_1) \dots (\exists v_n)\mathcal{A}), \\ \vdash ((\forall v_1) \dots (\forall v_n)\mathcal{A} \rightarrow \mathcal{A}_{v_1, \dots, v_n}[t_1, \dots, t_n]). \end{aligned}$$

Напомним, что формула $(\mathcal{A} \longleftrightarrow \mathcal{B})$ служит сокращением для формулы $((\mathcal{A} \rightarrow \mathcal{B}) \& (\mathcal{B} \rightarrow \mathcal{A}))$. Поэтому в силу теоремы 3.5.7 для установления выводимости $\Gamma \vdash (\mathcal{A} \longleftrightarrow \mathcal{B})$ необходимо и достаточно установить, что $\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B})$ и $\Gamma \vdash (\mathcal{B} \rightarrow \mathcal{A})$.

Теорема 3.5.20. Если $\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B})$, то

$$\begin{aligned} \Gamma \vdash ((\exists x)\mathcal{A} \rightarrow (\exists x)\mathcal{B}) \text{ и} \\ \Gamma \vdash ((\forall x)\mathcal{A} \rightarrow (\forall x)\mathcal{B}). \end{aligned}$$

Если $\Gamma \vdash (\mathcal{A} \longleftrightarrow \mathcal{B})$, то

$$\begin{aligned} \Gamma \vdash ((\exists x)\mathcal{A} \longleftrightarrow (\exists x)\mathcal{B}) \text{ и} \\ \Gamma \vdash ((\forall x)\mathcal{A} \longleftrightarrow (\forall x)\mathcal{B}). \end{aligned}$$

Д о к а з а т е л ь с т в о. Если $\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B})$, то используя $\vdash (\mathcal{B} \rightarrow (\exists x)\mathcal{B})$, по **Правилу Транзитивности** получаем $\Gamma \vdash (\mathcal{A} \rightarrow (\exists x)\mathcal{B})$, а значит, и $\Gamma \vdash ((\exists x)\mathcal{A} \rightarrow (\exists x)\mathcal{B})$.

Если $\Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B})$, то, используя $\vdash ((\forall x)\mathcal{A} \rightarrow \mathcal{A})$, по **Правилу Транзитивности** получаем $\Gamma \vdash ((\forall x)\mathcal{A} \rightarrow \mathcal{B})$, а значит, и $\Gamma \vdash ((\forall x)\mathcal{A} \rightarrow (\forall x)\mathcal{B})$.

Доказательство второй части теоремы сразу следует из первой ее части. \square

Теорема 3.5.21. Для произвольных формул \mathcal{A} и \mathcal{B}

$$\begin{aligned} \vdash ((\forall x)(\mathcal{A} \& \mathcal{B}) \longleftrightarrow ((\forall x)\mathcal{A} \& (\forall x)\mathcal{B})), \\ \vdash ((\exists x)(\mathcal{A} \vee \mathcal{B}) \longleftrightarrow ((\exists x)\mathcal{A} \vee (\exists x)\mathcal{B})). \end{aligned}$$

Д о к а з а т е л ь с т в о. Так как

$$\vdash ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{A}) \quad \text{и} \quad \vdash ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{B}),$$

то

$$\vdash ((\forall x)(\mathcal{A} \& \mathcal{B}) \rightarrow (\forall x)\mathcal{A}) \quad \text{и} \quad \vdash ((\forall x)(\mathcal{A} \& \mathcal{B}) \rightarrow (\forall x)\mathcal{B}),$$

а значит,

$$\vdash ((\forall x)(\mathcal{A} \& \mathcal{B}) \rightarrow (\forall x)\mathcal{A} \& (\forall x)\mathcal{B}).$$

С другой стороны,

$$\vdash (((\forall x)\mathcal{A} \& (\forall x)\mathcal{B}) \rightarrow (\forall x)\mathcal{A}), \quad \vdash (((\forall x)\mathcal{A} \& (\forall x)\mathcal{B}) \rightarrow (\forall x)\mathcal{B}).$$

Но

$$((\forall x)\mathcal{A} \rightarrow \mathcal{A}), \quad ((\forall x)\mathcal{B} \rightarrow \mathcal{B}).$$

Поэтому

$$\vdash (((\forall x)(\mathcal{A} \& (\forall x)\mathcal{B}) \rightarrow (\mathcal{A} \& \mathcal{B})).$$

Значит,

$$\vdash (((\forall x)\mathcal{A} \& (\forall x)\mathcal{B}) \rightarrow (\forall x)(\mathcal{A} \& \mathcal{B})).$$

Поэтому

$$\vdash ((\forall x)(\mathcal{A} \& \mathcal{B}) \longleftrightarrow ((\forall x)\mathcal{A} \& (\forall x)\mathcal{B})).$$

Доказательство

$$\vdash (\exists x)(\mathcal{A} \vee \mathcal{B}) \longleftrightarrow ((\exists x)\mathcal{A} \vee (\exists x)\mathcal{B}).$$

проведем по аналогичной схеме. Так как

$$\vdash (\mathcal{A} \rightarrow (\exists x)\mathcal{A}), \quad \vdash ((\exists x)\mathcal{A} \rightarrow ((\exists x)\mathcal{A} \vee (\exists x)\mathcal{B})),$$

то

$$\vdash (\mathcal{A} \rightarrow ((\exists x)\mathcal{A} \vee (\exists x)\mathcal{B})).$$

Аналогично устанавливаем, что

$$\vdash (\mathcal{B} \rightarrow ((\exists x)\mathcal{A} \vee (\exists x)\mathcal{B})).$$

Поэтому

$$\vdash ((\mathcal{A} \vee \mathcal{B}) \rightarrow ((\exists x)\mathcal{A} \vee (\exists x)\mathcal{B})).$$

Значит,

$$\vdash ((\exists x)(\mathcal{A} \vee \mathcal{B}) \rightarrow ((\exists x)\mathcal{A} \vee (\exists x)\mathcal{B})).$$

С другой стороны, так как

$$\vdash (\mathcal{A} \rightarrow (\mathcal{A} \vee \mathcal{B})), \quad \vdash (\mathcal{B} \rightarrow (\mathcal{A} \vee \mathcal{B})),$$

то

$$\vdash ((\exists x)\mathcal{A} \rightarrow (\exists x)(\mathcal{A} \vee \mathcal{B})), \quad \vdash ((\exists x)\mathcal{B} \rightarrow (\exists x)(\mathcal{A} \vee \mathcal{B})),$$

поэтому

$$\vdash (((\exists x)\mathcal{A} \vee (\exists x)\mathcal{B}) \rightarrow (\exists x)(\mathcal{A} \vee \mathcal{B})).$$

□

Теорема 3.5.22. Для произвольной формулы \mathcal{A}

$$\vdash (\neg(\forall x)\mathcal{A} \longleftrightarrow (\exists x)\neg\mathcal{A}), \quad \vdash (\neg(\exists x)\mathcal{A} \longleftrightarrow (\forall x)\neg\mathcal{A}).$$

Доказательство. Доказательство первой эквивалентности получается из следующих двух цепочек выводимых формул

$$\begin{aligned} \vdash ((\forall x)\mathcal{A} \rightarrow \mathcal{A}), \quad \vdash (\neg\mathcal{A} \rightarrow \neg(\forall x)\mathcal{A}), \quad \vdash ((\exists x)\neg\mathcal{A} \rightarrow \neg(\forall x)\mathcal{A}); \\ \vdash (\neg\mathcal{A} \rightarrow (\exists x)\neg\mathcal{A}), \quad \vdash (\neg(\exists x)\neg\mathcal{A} \rightarrow \mathcal{A}), \\ \vdash (\neg(\exists x)\neg\mathcal{A} \rightarrow (\forall x)\mathcal{A}), \quad \vdash (\neg(\forall x)\mathcal{A} \rightarrow (\exists x)\neg\mathcal{A}). \end{aligned}$$

Вторая эквивалентность легко получается из первой.

□

Теорема 3.5.23. Если переменная x не входит свободно в формулу \mathcal{A} , то для произвольной формулы \mathcal{B}

$$\begin{aligned} &\vdash (\exists x)(\mathcal{A} \& \mathcal{B}) \longleftrightarrow (\mathcal{A} \& (\exists x)\mathcal{B}), \quad \vdash (\forall x)(\mathcal{A} \vee \mathcal{B}) \longleftrightarrow (\mathcal{A} \vee (\forall x)\mathcal{B}), \\ &\vdash (\exists x)(\mathcal{A} \rightarrow \mathcal{B}) \longleftrightarrow (\mathcal{A} \rightarrow (\exists x)\mathcal{B}), \quad \vdash (\forall x)(\mathcal{A} \rightarrow \mathcal{B}) \longleftrightarrow (\mathcal{A} \rightarrow (\forall x)\mathcal{B}), \\ &\vdash (\exists x)(\mathcal{B} \rightarrow \mathcal{A}) \longleftrightarrow ((\forall x)\mathcal{B} \rightarrow \mathcal{A}), \quad \vdash (\forall x)(\mathcal{B} \rightarrow \mathcal{A}) \longleftrightarrow ((\exists x)\mathcal{B} \rightarrow \mathcal{A}). \end{aligned}$$

Д о к а з а т е л ь с т в о. Так как

$$\vdash ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{A}), \quad \vdash ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{B}), \quad \vdash (\mathcal{B}) \rightarrow (\exists x)\mathcal{B},$$

то

$$\vdash ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{A}), \quad \vdash ((\mathcal{A} \& \mathcal{B}) \rightarrow (\exists x)\mathcal{B}).$$

Значит,

$$\vdash ((\mathcal{A} \& \mathcal{B}) \rightarrow (\mathcal{A} \& (\exists x)\mathcal{B})),$$

поэтому

$$\vdash ((\exists x)(\mathcal{A} \& \mathcal{B}) \rightarrow (\mathcal{A} \& (\exists x)\mathcal{B})).$$

Для установления обратной импликации поступаем следующим образом

$$\vdash ((\mathcal{A} \& \mathcal{B}) \rightarrow (\exists x)(\mathcal{A} \& \mathcal{B})).$$

Значит,

$$\begin{aligned} &\vdash (\mathcal{B} \rightarrow (\mathcal{A} \rightarrow (\exists x)(\mathcal{A} \& \mathcal{B}))), \\ &\vdash ((\exists x)\mathcal{B} \rightarrow (\mathcal{A} \rightarrow (\exists x)(\mathcal{A} \& \mathcal{B}))), \\ &\vdash ((\mathcal{A} \& (\exists x)\mathcal{B}) \rightarrow (\exists x)(\mathcal{A} \& \mathcal{B})). \end{aligned}$$

Докажем, что при сделанных предположениях

$$\vdash (\forall x)(\mathcal{A} \vee \mathcal{B}) \longleftrightarrow (\mathcal{A} \vee (\forall x)\mathcal{B}).$$

Так как

$$\vdash (\mathcal{A} \rightarrow (\mathcal{A} \vee \mathcal{B})), \quad \vdash ((\forall x)\mathcal{B} \rightarrow \mathcal{B}), \quad \vdash (\mathcal{B} \rightarrow (\mathcal{A} \vee \mathcal{B})),$$

то

$$\vdash ((\mathcal{A} \vee (\forall x)\mathcal{B}) \rightarrow (\mathcal{A} \vee \mathcal{B})),$$

значит,

$$\vdash ((\mathcal{A} \vee (\forall x)\mathcal{B}) \rightarrow (\forall x)(\mathcal{A} \vee \mathcal{B})).$$

Остается доказать, что

$$\vdash ((\forall x)(\mathcal{A} \vee \mathcal{B}) \rightarrow (\mathcal{A} \vee (\forall x)\mathcal{B})).$$

Так как формула **Логики Высказываний**

$$((A_1 \vee A_2) \rightarrow (\neg A_1 \rightarrow A_2))$$

тождественно истинна, то по теореме 3.5.2

$$\vdash ((\mathcal{A} \vee \mathcal{B}) \rightarrow (\neg \mathcal{A} \rightarrow \mathcal{B})).$$

Что вместе с

$$\vdash ((\forall x)(\mathcal{A} \vee \mathcal{B}) \rightarrow (\mathcal{A} \vee \mathcal{B}))$$

дает

$$\vdash ((\forall x)(\mathcal{A} \vee \mathcal{B}) \rightarrow (\neg \mathcal{A} \rightarrow \mathcal{B})).$$

Откуда получаем

$$\begin{aligned} &\vdash (((\forall x)(\mathcal{A} \vee \mathcal{B}) \& (\neg \mathcal{A})) \rightarrow \mathcal{B}), \\ &\vdash (((\forall x)(\mathcal{A} \vee \mathcal{B}) \& (\neg \mathcal{A})) \rightarrow (\forall x)\mathcal{B}), \\ &\vdash ((\forall x)(\mathcal{A} \vee \mathcal{B}) \rightarrow ((\neg \mathcal{A}) \rightarrow (\forall x)\mathcal{B})), \\ &\vdash ((\forall x)(\mathcal{A} \vee \mathcal{B}) \rightarrow (\mathcal{A} \vee (\forall x)\mathcal{B})). \end{aligned}$$

Для доказательства эквивалентностей

$$\vdash ((\exists x)(\mathcal{A} \rightarrow \mathcal{B}) \longleftrightarrow (\mathcal{A} \rightarrow (\exists x)\mathcal{B})), \quad \vdash ((\forall x)(\mathcal{A} \rightarrow \mathcal{B}) \longleftrightarrow (\mathcal{A} \rightarrow (\forall x)\mathcal{B}))$$

достаточно заметить, что $\vdash ((\mathcal{A} \rightarrow \mathcal{B}) \longleftrightarrow (\neg \mathcal{A} \vee \mathcal{B}))$, а, значит,

$$\vdash ((\exists x)(\mathcal{A} \rightarrow \mathcal{B}) \longleftrightarrow (\exists x)(\neg \mathcal{A} \vee \mathcal{B})), \quad \vdash ((\forall x)(\mathcal{A} \rightarrow \mathcal{B}) \longleftrightarrow (\forall x)(\neg \mathcal{A} \vee \mathcal{B}))$$

и воспользоваться уже установленными эквивалентностями. \square

Индукцией по построению формул из доказанных утверждений легко получается следующая теорема, носящая название **Теорема эквивалентности**.

Теорема 3.5.24. Если формула \mathcal{A}^* получается из формулы \mathcal{A} заменой некоторых вхождений подформулы $\mathcal{B}_1, \dots, \mathcal{B}_n$ соответственно на $\mathcal{B}_1^*, \dots, \mathcal{B}_n^*$ и $\Gamma \vdash (\mathcal{B}_1 \longleftrightarrow \mathcal{B}_1^*), \dots, \Gamma \vdash (\mathcal{B}_n \longleftrightarrow \mathcal{B}_n^*)$, то $\Gamma \vdash (\mathcal{A} \longleftrightarrow \mathcal{A}^*)$.

Рассмотрим вопрос о **переименовании связанных переменных**. Формула \mathcal{A}^* называется **вариантом** формулы \mathcal{A} , если она может быть получена из формулы \mathcal{A} с помощью конечного числа операций замены типа: *заменить подформулу вида $(Qx)\mathcal{B}$ на $(Qy)\mathcal{B}_x[y]$ при условии, что переменная y не входит свободно в формулу \mathcal{B} , где Q – это \exists или \forall* . Говорят также, что формула \mathcal{A}^* получена из формулы \mathcal{A} **переименованием связанных переменных**.

Теорема 3.5.25. Если формула \mathcal{A}^* является вариантом формулы \mathcal{A} , т. е. получена из нее переименованием связанных переменных, то $\vdash \mathcal{A} \longleftrightarrow \mathcal{A}^*$.

Доказательство. В силу **теоремы эквивалентности** достаточно доказать, что

$$(Qx)\mathcal{B} \longleftrightarrow (Qy)\mathcal{B}_x[y].$$

А это следует из следующей цепочки выводимостей

$$\begin{aligned} \vdash (\mathcal{B}_x[y] \rightarrow (\exists x)\mathcal{B}), \quad \vdash ((\exists y)\mathcal{B}_x[y] \rightarrow (\exists x)\mathcal{B}), \\ \vdash ((\mathcal{B}_x[y])_y[x] \rightarrow (\exists y)\mathcal{B}_x[y]), \quad \vdash ((\exists x)\mathcal{B} \rightarrow (\exists y)\mathcal{B}_x[y]), \\ \vdash ((\exists x)\mathcal{B} \longleftrightarrow (\exists y)\mathcal{B}_x[y]), \\ \vdash ((\forall x)\mathcal{B} \rightarrow \mathcal{B}_x[y]), \quad \vdash ((\forall x)\mathcal{B} \rightarrow (\forall y)\mathcal{B}_x[y]), \\ \vdash ((\forall y)\mathcal{B}_x[y]) \rightarrow (\mathcal{B}_x[y])_y[x]), \quad \vdash ((\forall y)\mathcal{B}_x[y]) \rightarrow (\forall x)\mathcal{B}), \\ \vdash ((\forall x)\mathcal{B} \longleftrightarrow (\forall y)\mathcal{B}_x[y]). \end{aligned}$$

□

3.5.3. Теорема К. Геделя о полноте

Основная цель этого параграфа – доказать следующую **Теорему Адекватности**.

Теорема Адекватности. Для любой формулы \mathcal{A} языка $L_{\text{ИП}}$ и для любого множества формул Γ этого языка имеет место следующая эквивалентность: формула \mathcal{A} является **логическим следствием** множества формул Γ тогда и только тогда, когда формула \mathcal{A} **выводима** из этого множества формул Γ .

Как следствие мы получим **Теорему К. Геделя о полноте** для **Исчисления Предикатов**.

Теорема К. Геделя. Для любой формулы \mathcal{A} языка $L_{\text{ИП}}$ имеет место следующая эквивалентность:

\mathcal{A} является **тождественно истинной** формулой **Логики Предикатов** тогда и только тогда, когда она выводима в **Исчислении Предикатов**.

Доказательство второй части **Теоремы Адекватности**

если формула \mathcal{A} **выводима** из множества формул Γ , то формула \mathcal{A} является **логическим следствием** этого множества формул Γ

достаточно просто провести, например, *индукцией по длине вывода*. Проверка всех деталей оставляется читателю в качестве несложного, но весьма полезного упражнения.

Для доказательства первой части **Теоремы Адекватности**

если формула \mathcal{A} является **логическим следствием** множества формул Γ , то формула \mathcal{A} **выводима** из этого множества формул Γ

необходимо проделать определенную подготовительную работу.

Докажем вспомогательную теорему.

Теорема 3.5.26. Если для множества формул Γ и замкнутых формул \mathcal{A} и \mathcal{B} выполнены условия

$$\Gamma, (\neg\mathcal{A}) \vdash \mathcal{B} \quad \text{и} \quad \Gamma, (\neg\mathcal{A}) \vdash (\neg\mathcal{B}),$$

то

$$\Gamma \vdash \mathcal{A}.$$

Д о к а з а т е л ь с т в о. Если

$$\Gamma, (\neg\mathcal{A}) \vdash \mathcal{B} \quad \text{и} \quad \Gamma, (\neg\mathcal{A}) \vdash (\neg\mathcal{B}),$$

то по теореме 3.5.10 для любой формулы \mathcal{C} имеем

$$\Gamma, (\neg\mathcal{A}) \vdash (\neg\mathcal{C}).$$

Пусть \mathcal{C} – замкнутая формула, тогда в силу пункта 6) теоремы 3.5.14

$$\Gamma, \mathcal{C} \vdash \mathcal{A}.$$

Взяв в качестве формулы \mathcal{C} любую такую замкнутую формулу, что

$$\Gamma \vdash \mathcal{C},$$

например, в качестве такой формулы \mathcal{C} можно взять любую логическую аксиому, являющуюся замкнутой формулой, получим по теореме 3.5.4

$$\Gamma \vdash \mathcal{A}.$$

□

Покажем, что **Теорема Адекватности** эквивалентна следующей **Теореме Непротиворечивости**

Теорема Непротиворечивости. Множество формул T языка $L_{\text{ИП}}$ **непротиворечиво** тогда и только тогда, когда оно **совместно**.

Д о к а з а т е л ь с т в о. Покажем, что **Теорема Адекватности** влечет **Теорему Непротиворечивости**.

Предположим, что справедлива **Теорема Адекватности**.

Покажем, что справедлива **Теорема Непротиворечивости**.

Пусть T – **совместное** множество формул и φ – интерпретация, в которой истинны все формулы из T . Если бы множество формул T было **противоречивым**, то для любой замкнутой формулы \mathcal{A} из T была бы выводима как сама формула \mathcal{A} , так и ее отрицание $(\neg\mathcal{A})$. Тогда обе эти формулы были бы логическим следствием множества формул T , а, значит, формула \mathcal{A} и ее отрицание $(\neg\mathcal{A})$ были бы истинны в интерпретации φ , что невозможно. Значит, множество формул T **непротиворечиво**.

Обратно предположим, что множество формул T **непротиворечиво**. Покажем, что оно **совместно**. В противном случае любая формула B была бы **логическим следствием** множества формул T , а, значит, по **Теореме Адекватности выводима** из множества формул T . Но это противоречит предположению о непротиворечивости множества формул T .

Покажем, что **Теорема Непротиворечивости** влечет **Теорему Адекватности**.

Предположим, что справедлива **Теорема Непротиворечивости**.

Покажем, что справедлива **Теорема Адекватности**.

Если формула A **выводима** из множества формул Γ , то *индукцией по длине вывода* нетрудно доказать, что формула A является **логическим следствием** множества формул Γ .

Пусть формула A является **логическим следствием** множества формул Γ .

Предположим, что формула A **невыводима** из множества формул Γ . Тогда по теореме 3.5.26 множество формул $\Gamma \cup \{\neg A\}$ **непротиворечиво**. Значит, по **Теореме Непротиворечивости** оно **совместно**. Пусть φ – интерпретация, в которой истинны все формулы из множества $\Gamma \cup \{\neg A\}$. Значит, формула A ложна в этой интерпретации. Но, по предположению, формула A является **логическим следствием** множества формул Γ . А так как все формулы из множества Γ истинны в интерпретации φ , то и формула A истинна в этой интерпретации. Полученное противоречие завершает доказательство теоремы. \square

Определение 3.5.6. Язык L^* называется **расширением** языка L , если его алфавит является расширением алфавита языка L .

Если языки L^* и L – языки первого порядка, то, учитывая ранее сделанное соглашение относительно применения логических символов в языках первого порядка, ясно, что для того чтобы язык первого порядка L^* был расширением языка первого порядка L , необходимо и достаточно, чтобы каждый нелогический символ из алфавита L являлся символом алфавита языка L^* .

Определение 3.5.7. Любое множество T формул произвольного языка первого порядка L , замкнутое относительно правил вывода **Исчисления Предикатов**, будем называть **теорией** первого порядка, а L – ее языком.

Если Γ – произвольное множество формул языка первого порядка L , то через $T[\Gamma]$ будем обозначать множество всех формул языка L , выводимых из Γ . При этом Γ будет называться множеством *нелогических аксиом* теории $T[\Gamma]$. Утверждения "формула A выводима (доказуема) в теории $T[\Gamma]$ " и "формула A выводима (доказуема) из множества формул Γ " будем считать обозначающими одно и то же.

Определение 3.5.8. Теория первого порядка T^* называется **расширением** теории первого порядка T , если ее язык $L(T^*)$ является расширением языка $L(T)$ теории T и для любой формулы F языка $L(T)$ из ее выводимости в теории T следует выводимость в теории T^* .

Заметим, что для того чтобы любая теорема теории T была доказуема в теории T^* , необходимо и достаточно, чтобы это было верно для нелогических аксиом теории T .

Определение 3.5.9. Расширение T^* теории T называется **консервативным расширением**, если для любой формулы F языка $L(T)$ из ее выводимости в теории T^* следует выводимость в исходной теории T .

Таким образом, теория T^* является консервативным расширением теории T тогда и только тогда, когда для их языков выполнено включение $L(T) \subseteq L(T^*)$ и для любой формулы F языка $L(T)$ имеет место эквивалентность:

$$\vdash_T F \iff \vdash_{T^*} F.$$

Пусть язык $L(T^+)$ теории T^+ получается из языка L теории T добавлением новых индивидуальных констант без изменения множества нелогических аксиом.

Заметим, множество логических аксиом теории T^+ является расширением множества логических аксиом теории T .

Покажем, что теория T^+ является консервативным расширением теории T . Это будет следовать из следующей более сильной теоремы, носящей название **Теорема о константах**.

Теорема 3.5.27. Если \mathcal{A} – произвольная формула теории T , v_1, \dots, v_n – попарно различные индивидуальные переменные, а c_1, \dots, c_n – попарно различные новые константы теории T^+ , то имеет место эквивалентность

$$\vdash_T \mathcal{A} \iff \vdash_{T^+} \mathcal{A}_{v_1, \dots, v_n}[c_1, \dots, c_n].$$

Доказательство. Если $\vdash_T \mathcal{A}$, то $\vdash_{T^+} \mathcal{A}$. Тогда по **Правилу подстановки** $\vdash_{T^+} \mathcal{A}_{v_1, \dots, v_n}[c_1, \dots, c_n]$.

Пусть теперь $\vdash_{T^+} \mathcal{A}_{v_1, \dots, v_n}[c_1, \dots, c_n]$ и $\mathcal{B}_1, \dots, \mathcal{B}_k = \mathcal{A}_{v_1, \dots, v_n}[c_1, \dots, c_n]$ – вывод формулы $\mathcal{A}_{v_1, \dots, v_n}[c_1, \dots, c_n]$ в теории T^+ .

Пусть c_1, \dots, c_m – все новые константы теории T^+ , встречающиеся в этом выводе.

Выберем m переменных y_1, \dots, y_m , не встречающихся в формулах $\mathcal{B}_1, \dots, \mathcal{B}_k$.

Для произвольной формулы \mathcal{B} обозначим через \mathcal{B}^* формулу

$$\mathcal{B}_{c_1, \dots, c_m}[y_1, \dots, y_m].$$

Непосредственная проверка показывает, что $\mathcal{B}_1^*, \dots, \mathcal{B}_k^*$ – **вывод** формулы

$$(\mathcal{A}_{v_1, \dots, v_n}[c_1, \dots, c_n])_{c_1, \dots, c_m}[y_1, \dots, y_m] \equiv \mathcal{A}_{v_1, \dots, v_n}[y_1, \dots, y_n]$$

в теории T .

По **Правилу подстановки** в теории T выводима формула

$$(\mathcal{A}_{v_1, \dots, v_n}[y_1, \dots, y_n])_{y_1, \dots, y_n}[v_1, \dots, v_n] = \mathcal{A}.$$

□

Покажем, как можно использовать теорему дедукции в сочетании с теоремой о константах.

Пусть T – некоторая теория языка $L(T)$, а \mathcal{A} и \mathcal{B} – формулы этого языка, все свободные переменные которых содержатся в списке v_1, \dots, v_n . Добавим к алфавиту языка $L(T)$ новые константные символы c_1, \dots, c_n , получим теорию T^+ языка $L(T^+)$. Тогда по **Теореме о константах**

$$\vdash (\mathcal{A} \rightarrow \mathcal{B}) \iff \vdash_{T^+} (\mathcal{A}_{v_1, \dots, v_n}[c_1, \dots, c_n] \rightarrow \mathcal{B}_{v_1, \dots, v_n}[c_1, \dots, c_n]),$$

а последнее по **Теореме Дедукции** равносильно

$$\vdash_{T^+[\mathcal{A}_{v_1, \dots, v_n}[c_1, \dots, c_n]]} \mathcal{B}_{v_1, \dots, v_n}[c_1, \dots, c_n].$$

Что нередко установить бывает проще.

Определение 3.5.10. Теории T^* и T называются **эквивалентными**, если каждая из них является расширением другой.

Ясно, что для эквивалентности теорий T^* и T необходимо и достаточно, чтобы их языки совпадали $L(T) = L(T^*)$ и для любой формулы F в языке этих теорий имела бы место эквивалентность:

$$\vdash_T F \iff \vdash_{T^*} F.$$

Теорема редукции. Для любого множества формул Γ и любой формулы F в языке теории T имеет место эквивалентность:

$$\vdash_{T[\Gamma]} F \iff \text{в } \Gamma \text{ существуют такие различные формулы } F_1, \dots, F_n, \text{ что } \vdash_T (\forall F_1 \rightarrow (\forall F_2 \rightarrow (\dots \rightarrow (\forall F_n \rightarrow F) \dots))),$$

где $\forall F_i$ – \forall -замыкание формулы $\forall F_i$.

Д о к а з а т е л ь с т в о. Если $\vdash_{T[\Gamma]} F$, то пусть \mathcal{D} – вывод формулы F в теории $T[\Gamma]$, а F_1, F_2, \dots, F_n – все различные формулы из Γ , входящие в \mathcal{D} . Тогда $\vdash_{T[F_1, \dots, F_n]} F$. Так как при любом i ($1 \leq i \leq n$) $\vdash_{T[\forall F_1, \dots, \forall F_n]} \forall F_i$, то $\vdash_{T[\forall F_1, \dots, \forall F_n]} F$. Так как каждая формула $\forall F_i$ замкнутая, то по следствию **Теоремы Дедукции** получаем, что

$$\vdash_T (\forall F_1 \rightarrow (\forall F_2 \rightarrow (\dots \rightarrow (\forall F_n \rightarrow F) \dots))).$$

Предположим, что в Γ найдутся такие различные формулы F_1, \dots, F_n , что $\vdash_T (\forall F_1 \rightarrow (\forall F_2 \rightarrow (\dots \rightarrow (\forall F_n \rightarrow F) \dots)))$.

Так как при любом i ($i = 1, \dots, n$) $\vdash_{T[\Gamma]} F_i$, то по теореме замыкания $\vdash_{T[\Gamma]} \forall F_i$. Из $\vdash_T (\forall F_1 \rightarrow (\forall F_2 \rightarrow (\dots \rightarrow (\forall F_n \rightarrow F) \dots)))$ применяя n раз правило отделения, получаем $\vdash_{T[\Gamma]} F$. □

Определение 3.5.11. Множество формул Γ языка L_{II} **Исчисления Предикатов** называется **полным**, если оно непротиворечиво и для любой замкнутой формулы \mathcal{A} языка L_{II}

$$\Gamma \vdash \mathcal{A} \quad \text{либо} \quad \Gamma \vdash (\neg \mathcal{A}).$$

Теорема 3.5.28. Для любого непротиворечивого множества формул Γ языка L_{II} **Исчисления Предикатов** существует такое **полное** множество формул Γ^* этого языка L_{II} , что

$$\Gamma \subseteq \Gamma^*.$$

Доказательство. Дадим два варианта доказательства. В первом варианте доказательства будем считать, что сигнатура τ *счетная*. Тогда счетными будут и алфавит языка L_τ **Исчисления Предикатов**, и множество всех замкнутых формул **Исчисления Предикатов** этой сигнатуры.

Пусть последовательность $(\Phi_n)_{n \in \mathbb{N}}$ дает *пересчет* всех замкнутых формул сигнатуры τ .

Определим последовательность $(\Gamma_n)_{n \in \mathbb{N}}$ множеств формул.

Полагаем

$$\Gamma_1 \equiv \Gamma.$$

Если множество Γ_n уже определено, то полагаем

$$\Gamma_{n+1} \equiv \begin{cases} \Gamma_n \cup \{\Phi_n\}, & \text{если } \Gamma_n \vdash \Phi_n \\ \Gamma_n \cup \{(\neg \Phi_n)\}, & \text{если } \Gamma_n \not\vdash \Phi_n. \end{cases}$$

Индукцией по n докажем, что каждое из множеств формул Γ_n является *непротиворечивым*.

Так как $\Gamma_1 \equiv \Gamma$, то множество формул Γ_1 является непротиворечивым по условию теоремы.

Предположим, что уже доказана непротиворечивость множества формул Γ_n . Докажем непротиворечивость множества формул Γ_{n+1} .

Если $\Gamma_n \vdash \Phi_n$, то $\Gamma_{n+1} = \Gamma_n \cup \{\Phi_n\}$.

Если бы множество формул Γ_{n+1} оказалось противоречивым, для любой формулы \mathcal{A} мы имели бы $\Gamma_{n+1} \vdash \mathcal{A}$, т. е. $\Gamma_n \cup \{\Phi_n\} \vdash \mathcal{A}$. Но $\Gamma_n \vdash \Phi_n$, поэтому по теореме 3.5.4 получаем $\Gamma_n \vdash \mathcal{A}$, что противоречит предположению о непротиворечивости множества формул Γ_n .

Если $\Gamma_n \not\vdash \Phi_n$, то $\Gamma_{n+1} = \Gamma_n \cup \{(\neg \Phi_n)\}$.

Если бы множество формул Γ_{n+1} оказалось противоречивым, то для любой замкнутой формулы \mathcal{A} мы имели бы $\Gamma_{n+1} \vdash \mathcal{A}$ и $\Gamma_{n+1} \vdash (\neg \mathcal{A})$, т. е. $\Gamma_n \cup \{(\neg \Phi_n)\} \vdash \mathcal{A}$ и $\Gamma_n \cup \{(\neg \Phi_n)\} \vdash (\neg \mathcal{A})$. Отсюда по теореме 3.5.26 получаем $\Gamma_n \vdash \Phi_n$. Но последнее противоречит предположению $\Gamma_n \not\vdash \Phi_n$. Значит, и в этом случае множество формул Γ_{n+1} является непротиворечивым.

Тем самым доказано, что *при любом n множество формул Γ_n является непротиворечивым.*

Полагаем

$$\Gamma^* \Rightarrow \bigcup_{n=1}^{\infty} \Gamma_n.$$

Покажем, что Γ^* – **полное множество формул** и

$$\Gamma \subseteq \Gamma^*.$$

Последнее очевидно, так как

$$\Gamma = \Gamma_1 \subseteq \Gamma^*.$$

Если бы множество формул Γ^* было противоречиво, то нашлось бы **конечное противоречивое** 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 непротиворечивости множества формул Γ_n .

Значит, Γ^* – **непротиворечивое** множество формул.

Пусть \mathcal{A} – произвольная замкнутая 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 Γ^* – **полное** множество формул языка L_τ такое, что $\Gamma \subseteq \Gamma^*$.

В случае произвольной сигнатуры τ возможно аналогичное доказательство, однако при этом вместо достаточно простой индукции по n необходимо использовать *трансфинитную индукцию*. Мы не будем рассматривать этот вариант доказательства, а приведем доказательство с использованием **Леммы Тейхмюллера – Тьюки**.

Напомним, что 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} .

В первой главе было показано, что следующее утверждение эквивалентно **Аксиоме выбора**.

Лемма Тейхмюллера – Тьюки. *Каждое семейство подмножеств \mathcal{X} множества E , имеющее конечный характер, обладает **максимальным элементом**.*

Рассмотрим следующее семейство подмножеств \mathcal{X} множества F_τ всех формул языка L_τ

$$T \in \mathcal{X} \iff T \cup \Gamma \text{ — непротиворечиво.}$$

Из определения семейства подмножеств \mathcal{X} сразу следует, что оно имеет *конечный характер*. По **Лемме Тейхмюллера – Тьюки** в семействе подмножеств \mathcal{X} имеется **максимальный элемент** T^* . Покажем, что множество $\Gamma^* = \Gamma \cup T^*$ является **полным**.

Из определения семейства подмножеств \mathcal{X} сразу следует, что множество Γ^* является **непротиворечивым**.

Докажем **полноту** множества Γ^* .

Пусть \mathcal{A} – произвольная *замкнутая формула*.

Если множество $\Gamma^* \cup \{(\neg \mathcal{A})\}$ **противоречиво**, то по теореме 3.5.26 $\Gamma^* \vdash \mathcal{A}$.

Если же множество $\Gamma^* \cup \{(\neg \mathcal{A})\}$, т. е. множество $\Gamma \cup T^* \cup \{(\neg \mathcal{A})\}$, непротиворечиво, то в силу максимальной T^* получаем $(\neg \mathcal{A}) \in T^*$. Значит, $\Gamma^* \vdash (\neg \mathcal{A})$.

Итак, Γ^* – **полное расширение** непротиворечивого множества формул Γ . \square

На первый взгляд кажется, что второй вариант доказательства ”проще” первого, однако это обманчивое впечатление – во втором варианте вся идейная трудность доказательства перенесена в доказательство эквивалентности **Леммы Тейхмюллера – Тьюки Аксиоме Выбора**.

Кроме свойства **полноты** теории для доказательства **Теоремы Непротиворечивости** нам понадобится еще одно свойство множеств формул Σ языка первого порядка L_τ сигнатуры τ – **свойство Генкина**.

Определение 3.5.12. Множество формул Σ языка первого порядка L_τ сигнатуры τ обладает **свойством Генкина**, если для любой формулы F с одной свободной переменной v из того, что $\Sigma \vdash (\exists v)F$, следует, что найдется такой замкнутый терм t , что $\Sigma \vdash F_v[t]$.

Теорема 3.5.29. Для любого непротиворечивого множества формул Γ языка L_τ сигнатуры τ можно построить непротиворечивое множество формул Γ^+ языка L_{τ^+} сигнатуры τ^+ такое, что $\Gamma \subseteq \Gamma^+$, сигнатура τ^+ получается из сигнатуры τ добавлением новых индивидуальных констант и для множества формул Γ^+ выполнено **свойство Генкина**.

Доказательство. Доказательство проведем лишь в случае счетной сигнатуры. Общий случай рассматривается по аналогичной схеме.

Рассмотрим сигнатуру τ^+ , полученную из сигнатуры τ добавлением счетного множества $\{c_1, c_2, \dots, c_m, \dots\}$ новых индивидуальных констант.

Непротиворечивое множество формул Γ языка L_τ сигнатуры τ мы рассматриваем как множество формул языка L_{τ^+} расширенной сигнатуры τ^+ . Покажем, что множество формул Γ **непротиворечиво** и в **Исчислении Предикатов ИП** $_{\tau^+}$ расширенной сигнатуры τ^+ .

Предположим, что множество формул Γ **противоречиво** в **Исчислении Предикатов** $\mathbf{ИП}_{\tau+}$ расширенной сигнатуры τ^+ .

Тогда из множества формул Γ в **Исчислении Предикатов** $\mathbf{ИП}_{\tau+}$ расширенной сигнатуры τ^+ выводима любая формула.

Пусть \mathcal{A} – произвольная замкнутая формула языка L_{τ} исходной сигнатуры τ и $\mathcal{B}_1, \dots, \mathcal{B}_n$ – **вывод из множества формул** Γ формулы $(\mathcal{A} \& \neg \mathcal{A})$ в **Исчислении Предикатов** $\mathbf{ИП}_{\tau+}$ расширенной сигнатуры τ^+ .

Предположим, что все новые индивидные константы, встречающиеся в формулах вывода $\mathcal{B}_1, \dots, \mathcal{B}_n$, содержатся в списке c_1, c_2, \dots, c_m , а все переменные, встречающиеся в формулах вывода $\mathcal{B}_1, \dots, \mathcal{B}_n$, содержатся в списке x_1, x_2, \dots, x_p .

Для произвольной формулы \mathcal{B} языка $L_{\tau+}$ расширенной сигнатуры τ^+ обозначим через \mathcal{B}^+ формулу $\mathcal{B}_{c_1, c_2, \dots, c_m}[x_{p+1}, x_{p+2}, \dots, x_{p+m}]$.

Нетрудно проверить, что последовательность формул $\mathcal{B}_1^+, \dots, \mathcal{B}_n^+$ – **вывод из множества формул** Γ формулы $(\mathcal{A} \& \neg \mathcal{A})$ в **Исчислении Предикатов** $\mathbf{ИП}_{\tau}$ исходной сигнатуры τ . Однако это *противоречит предположению о непротиворечивости множества формул Γ в языке L_{τ} исходной сигнатуры τ .*

Значит, множество формул Γ **непротиворечиво** в **Исчислении Предикатов** $\mathbf{ИП}_{\tau+}$ расширенной сигнатуры τ^+ .

Так как сигнатура τ по предположению *счетная*, то счетными будут сигнатура τ^+ , алфавит языка $L_{\tau+}$ **Исчисления Предикатов** этой сигнатуры и множество $F_{\tau+}$ всех формул **Исчисления Предикатов** этой расширенной сигнатуры τ^+ .

Занумеруем $(F_n)_{n \in \mathbb{N}}$ все формулы языка $L_{\tau+}$, содержащие в точности одну свободную переменную. Для каждой формулы F_n через v_n будем обозначать ее единственную свободную переменную.

Индукцией по n построим последовательность $d_1, d_2, \dots, d_n, \dots$ из новых констант $\{c_1, c_2, \dots, c_m, \dots\}$ и непротиворечивые множества формул Γ_n .

Полагаем $\Gamma_0 = \Gamma$.

Пусть d_1 – это любая новая константа c_i , не входящая в формулу F_1 . Полагаем $\Gamma_1 = \Gamma \cup \{((\exists v_1)F_1 \rightarrow (F_1)_{v_1}[d_1])\}$.

Предположим, что уже построены начальный отрезок d_1, d_2, \dots, d_n последовательности из новых констант и множества формул Γ_n , причем

$$\Gamma_n = \Gamma_{n-1} \cup \{((\exists v_n)F_n \rightarrow (F_n)_{v_n}[d_n])\}.$$

Пусть d_{n+1} – это любая новая константа c_i , отличная от уже определенных констант d_1, d_2, \dots, d_n и не входящая в формулы F_1, F_2, \dots, F_n и F_{n+1} .

Полагаем

$$\Gamma_{n+1} = \Gamma_n \cup \{((\exists v_{n+1})F_{n+1} \rightarrow (F_{n+1})_{v_{n+1}}[d_{n+1}])\}.$$

Индукцией по n докажем **непротиворечивость** множеств формул Γ_n .

При $n = 0$ непротиворечивость множества формул Γ_0 следует из равенства $\Gamma_0 = \Gamma$.

Предположим, уже установлена непротиворечивость множества формул Γ_n . Докажем непротиворечивость множества формул Γ_{n+1} .

Предположим противное, т. е. что множество формул Γ_{n+1} противоречиво. Тогда из него выводима любая формула. Пусть \mathcal{A} — *доказуемая замкнутая* формула, например, логическая аксиома. Тогда из Γ_{n+1} выводима, в частности, формула $(\neg \mathcal{A})$. По **Теореме Дедукции** из Γ_n выводима формула

$$(((\exists v_{n+1})F_{n+1} \rightarrow (F_{n+1})_{v_{n+1}}[d_{n+1}]) \rightarrow (\neg \mathcal{A})),$$

а значит, и формула

$$(\mathcal{A}) \rightarrow (\neg((\exists v_{n+1})F_{n+1} \rightarrow (F_{n+1})_{v_{n+1}}[d_{n+1}])).$$

В силу доказуемости формулы \mathcal{A} получаем выводимость из Γ_n формулы

$$(\neg((\exists v_{n+1})F_{n+1} \rightarrow (F_{n+1})_{v_{n+1}}[d_{n+1}])).$$

Тождественно истинная формула **Логики Высказываний**

$$(\neg(A_1 \rightarrow A_2) \rightarrow (A_1 \& \neg A_2))$$

в силу теоремы 3.5.2 влечет для любых формул \mathcal{B} и \mathcal{C} **Исчисления Предикатов** выводимость в нем формулы

$$(\neg(\mathcal{B} \rightarrow \mathcal{C}) \rightarrow (\mathcal{B} \& (\neg \mathcal{C}))).$$

Значит, из Γ_n **выводима** формула

$$((\exists v_{n+1})F_{n+1} \& (\neg(F_{n+1})_{v_{n+1}}[d_{n+1}])).$$

Поэтому из Γ_n **выводима** каждая из формул

$$((\exists v_{n+1})F_{n+1} \quad \text{и} \quad (\neg(F_{n+1})_{v_{n+1}}[d_{n+1}])).$$

Пусть $\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_m$ — **вывод из** Γ_n формулы $(\neg(F_{n+1})_{v_{n+1}}[d_{n+1}])$ и переменная y не встречается в этом выводе.

Для произвольной формулы \mathcal{B} обозначим через \mathcal{B}^* формулу $\mathcal{B}_{d_{n+1}}[y]$.

Нетрудно проверить, что $\mathcal{B}_1^*, \mathcal{B}_2^*, \dots, \mathcal{B}_m^*$ — **вывод из** Γ_n формулы

$$(\neg(F_{n+1})_{v_{n+1}}[y])).$$

В силу **Правила Обобщения** тогда из Γ_n выводима формула

$$(\forall y)(\neg(F_{n+1})_{v_{n+1}}[y])).$$

С другой стороны, доказуемы формулы

$$\begin{aligned} ((\forall y)(\neg(F_{n+1})_{v_{n+1}}[y]) \rightarrow (\neg(F_{n+1})_{v_{n+1}}[v_{n+1}])), \\ ((F_{n+1})_{v_{n+1}}[v_{n+1}] \rightarrow \neg(\forall y)(\neg(F_{n+1})_{v_{n+1}}[y])), \\ ((\exists v_{n+1})(F_{n+1})_{v_{n+1}}[v_{n+1}] \rightarrow \neg(\forall y)(\neg(F_{n+1})_{v_{n+1}}[y])), \end{aligned}$$

т. е. формула

$$((\exists v_{n+1})F_{n+1} \rightarrow \neg(\forall y)(\neg(F_{n+1})_{v_{n+1}}[y])).$$

Но из Γ_n выводима формула $((\exists v_{n+1})F_{n+1})$, поэтому из Γ_n выводима формула $\neg(\forall y)(\neg(F_{n+1})_{v_{n+1}}[y])$. Последнее вместе с выводимостью из Γ_n формулы $(\forall y)(\neg(F_{n+1})_{v_{n+1}}[y])$ означает **противоречивость** множества формул Γ_n . Что противоречит индуктивному предположению.

Можно было бы провести рассуждение и по несколько иной схеме.

Пусть \mathcal{A} – *доказуемая замкнутая* формула, не содержащая новых констант.

Из выводимости из Γ_n формулы

$$(((\exists v_{n+1})F_{n+1} \rightarrow (F_{n+1})_{v_{n+1}}[d_{n+1}]) \rightarrow (\neg\mathcal{A})),$$

по **Теореме о константах** следует выводимость из Γ_n формулы

$$(((\exists v_{n+1})F_{n+1} \rightarrow F_{n+1}) \rightarrow (\neg\mathcal{A})).$$

Тогда по **Правилу Введения** \exists получаем выводимость формулы

$$((\exists v_{n+1})((\exists v_{n+1})F_{n+1} \rightarrow F_{n+1}) \rightarrow (\neg\mathcal{A})).$$

Так как выводимы формулы

$$\begin{aligned} &(((\exists v_{n+1})F_{n+1} \rightarrow (\exists v_{n+1})F_{n+1}) \rightarrow (\exists v_{n+1})((\exists v_{n+1})F_{n+1} \rightarrow F_{n+1})) \quad \text{и} \\ &((\exists v_{n+1})F_{n+1} \rightarrow (\exists v_{n+1})F_{n+1}), \end{aligned}$$

то из Γ_n **выводима** формула $(\neg\mathcal{A})$. Что вместе с выводимостью из Γ_n формулы \mathcal{A} *противоречит предположению о непротиворечивости* множества формул Γ_n .

Полагаем

$$\Gamma^+ \equiv \bigcup_{n=1}^{\infty} \Gamma_n.$$

Покажем, что Γ^+ – **непротиворечивое множество формул, обладающее свойством Генкина** и

$$\Gamma \subseteq \Gamma^+.$$

Последнее очевидно. Для доказательства **непротиворечивости** множества формул Γ^+ рассмотрим произвольное его конечное подмножество T . Так как при любом k $\Gamma_k \subseteq \Gamma_{k+1}$, то найдется такое n , что $T \subseteq \Gamma_n$. Так как выше уже доказано, что Γ_n **непротиворечиво**, то T **непротиворечиво**, поэтому **непротиворечиво** и Γ^+ .

Докажем, что **множество формул Γ^+ обладает свойством Генкина**.

Пусть F – произвольная формула с одной свободной переменной v . Найдется такое n , что F – это F_n , а v – это v_n . Тогда

$$((\exists v_n)F \rightarrow F_{v_n}[d_n]) \in \Gamma_n \subseteq \Gamma^+$$

т. е.

$$((\exists v)F \rightarrow F_v[d_n]) \in \Gamma_n \subseteq \Gamma^+.$$

Если $\Gamma^+ \vdash (\exists v)F$, то $\Gamma^+ \vdash F_v[d_n]$. \square

После проделанной подготовки мы можем доказать **Теорему Адекватности**, которая, как это было показано выше, эквивалентна **Теореме Непротиворечивости**. Напомним формулировку последней.

Теорема 3.5.30. *Множество формул Γ языка L_τ является совместным, тогда и только тогда, когда оно является непротиворечивым.*

Доказательство. Выше уже отмечалось, что если множество формул Γ языка L_τ является **совместным**, то, очевидно, оно является **непротиворечивым**.

Обратно, предположим, что множество Γ **непротиворечиво**.

Докажем, что тогда оно **совместно**.

Применив две предыдущие теоремы, мы получим *полное, обладающее свойством Генкина* множество формул $\bar{\Gamma} = (\Gamma^+)^*$ языка первого порядка L_{τ^+} сигнатуры τ^+ , полученной из сигнатуры τ добавлением новых индивидуальных констант такое, что $\Gamma \subseteq \bar{\Gamma}$. То, что множество формул $\bar{\Gamma} = (\Gamma^+)^*$ является **полным**, очевидно.

Заметим, что при переходе от множества формул Γ^+ к множеству формул $(\Gamma^+)^*$ сигнатура τ^+ не меняется.

Докажем, что **множество формул $(\Gamma^+)^*$ обладает свойством Генкина**.

Пусть F – произвольная формула с одной свободной переменной v сигнатуры τ^+ .

Найдется такое n , что F – это F_n , а v – это v_n . Тогда

$$((\exists v_n)F \rightarrow F_{v_n}[d_n]) \in \Gamma_n \subseteq \Gamma^+ \subseteq (\Gamma^+)^*.$$

Значит,

$$((\exists v)F \rightarrow F_v[d_n]) \in (\Gamma^+)^*.$$

Если $(\Gamma^+)^* \vdash (\exists v)F$, то $(\Gamma^+)^* \vdash F_v[d_n]$.

Покажем, что множество формул $\bar{\Gamma}$ является **совместным**. Отсюда, конечно, сразу будет следовать совместность и множества формул Γ .

Построим интерпретацию φ такую, что $\varphi(\bar{\Gamma}) = \text{И}$.

Для языка первого порядка L_{τ^+} сигнатуры τ^+ , используя **полное, обладающее свойством Генкина** множество формул $\bar{\Gamma}$, построим **естественную структуру \mathcal{A}_{τ^+}** – алгебраическую систему сигнатуры τ^+ , **основным множеством A** которой будет **множество \mathcal{T}_{τ^+} всех замкнутых термов** языка L_{τ^+} .

Построим **естественную интерпретацию φ** языка L_{τ^+} в алгебраической системе \mathcal{A}_{τ^+} .

Каждой индивидуальной константе c сигнатуры τ^+ сопоставим терм c – элемент основного множества A естественной структуры \mathcal{A}_{τ^+} .

Каждому n -местному функциональному символу f сигнатуры τ^+ сопоставим n -местную алгебраическую операцию $f^{\mathcal{A}_{\tau^+}}$ на основном множестве A естественной структуры \mathcal{A}_{τ^+} , полагая для произвольных элементов t_1, \dots, t_n множества A , т. е. термов языка L_{τ^+} ,

$$f^{\mathcal{A}_{\tau^+}}(t_1, \dots, t_n) = f(t_1, \dots, t_n).$$

Каждому n -местному предикатному символу p сигнатуры τ^+ сопоставим n -местный предикат $p^{\mathcal{A}_{\tau^+}}$ на основном множестве A естественной структуры \mathcal{A}_{τ^+} , полагая для произвольных элементов t_1, \dots, t_n множества A , т. е. замкнутых термов языка L_{τ^+} ,

$$p^{\mathcal{A}_{\tau^+}}(t_1, \dots, t_n) = \text{И} \iff \bar{\Gamma} \vdash p(t_1, \dots, t_n).$$

Для каждого индивида $t \in A$, т. е. замкнутого терма t сигнатуры τ^+ , его *именем* будет он сам t . Тогда сигнатура $\tau^+(A)$, полученная из сигнатуры τ^+ добавлением к множеству S индивидуальных констант сигнатуры τ^+ множества \bar{A} всех *имен индивидов* из A , будет совпадать с исходной сигнатурой τ^+ , а язык $L_{\tau^+(A)}$ – с исходным языком L_{τ^+} .

Для каждого замкнутого терма t языка L_{τ^+} обычным образом индукцией по построению терма t определяем индивид $\mathcal{A}(t)$ из A , который *будет соответствовать терму t* или являться *значением терма t* в интерпретации.

Нетрудно понять, что в рассматриваемом случае $\mathcal{A}(t)$ – это t , но это разные t – первое t – это терм t языка L_{τ^+} , а второе t – это элемент t основного множества A естественной структуры \mathcal{A}_{τ^+} языка L_{τ^+} .

Обычным способом для каждой замкнутой (т. е. не содержащей свободных переменных) формулы Φ языка $L_{\tau^+(A)}$ определяем ее *истинностное значение* $\varphi(\Phi)$ в системе \mathcal{A}_{τ^+} индукцией по построению формулы Φ (т. е. сопоставим Φ значение **И** или **Л**).

Условимся писать:

$$\begin{aligned} \mathcal{A}_{\tau^+} \models \Phi, & \text{ если } \varphi(\Phi) = \text{И}, \\ \mathcal{A}_{\tau^+} \not\models \Phi, & \text{ если } \varphi(\Phi) = \text{Л}. \end{aligned}$$

(i) Если Φ – атомная формула вида $p(t_1, \dots, t_n)$, где p – n -местный предикатный символ сигнатуры τ^+ , а t_1, \dots, t_n – замкнутые термы сигнатуры $\tau^+(A)$, то полагаем

$$\mathcal{A}_{\tau^+} \models \Phi \iff p^{\mathcal{A}_{\tau^+}}(\mathcal{A}_{\tau^+}(t_1), \dots, \mathcal{A}_{\tau^+}(t_n)) = \text{И},$$

т. е.

$$\mathcal{A}_{\tau^+} \models \Phi \iff \bar{\Gamma} \vdash p(t_1, \dots, t_n).$$

(ii) Теперь, если Φ и Ψ – замкнутые формулы, то полагаем

$$\begin{aligned} \mathcal{A}_{\tau^+} \models (\neg\Phi) &\iff \mathcal{A}_{\tau^+} \not\models \Phi, \\ \mathcal{A}_{\tau^+} \models (\Phi \vee \Psi) &\iff \mathcal{A}_{\tau^+} \models \Phi \text{ или } \mathcal{A}_{\tau^+} \models \Psi, \\ \mathcal{A}_{\tau^+} \models (\Phi \&\Psi) &\iff \mathcal{A}_{\tau^+} \models \Phi \text{ и } \mathcal{A}_{\tau^+} \models \Psi, \\ \mathcal{A}_{\tau^+} \not\models (\Phi \rightarrow \Psi) &\iff \mathcal{A}_{\tau^+} \models \Phi \text{ и } \mathcal{A}_{\tau^+} \not\models \Psi. \end{aligned}$$

(iii) Если Φ – формула, не содержащая свободных переменных, отличных от x , то полагаем

$$\begin{aligned} \mathcal{A}_{\tau^+} \models (\exists x)\Phi &\iff \\ \mathcal{A}_{\tau^+} \models \Phi_x[t] &\text{ для имени } t \text{ некоторого индивида } t \text{ из } A, \text{ т. е. терма } t, \end{aligned}$$

$$\begin{aligned} \mathcal{A}_{\tau^+} \models (\forall x)\Phi &\iff \\ \mathcal{A}_{\tau^+} \models \Phi_x[t] &\text{ для имени } t \text{ любого индивида } t \text{ из } A, \text{ т. е. терма } t. \end{aligned}$$

Напомним, что $\bar{\Gamma}$ – **полное** множество формул, поэтому для любой замкнутой формулы Φ

$$\bar{\Gamma} \vdash \Phi \text{ или } \bar{\Gamma} \vdash (\neg\Phi),$$

но не то и другое одновременно, в частности, это верно и для произвольной атомной формулы вида $p(t_1, \dots, t_n)$, где p – n -местный предикатный символ сигнатуры τ^+ . Поэтому интерпретация φ определена корректно.

Индукцией по построению формул (либо по их длине, либо по числу входящих в них логических связок и кванторов) докажем, что для произвольной замкнутой формулы Φ имеет место эквивалентность:

$$\bar{\Gamma} \vdash \Phi \iff \varphi(\Phi) = \text{И}.$$

(i) Для элементарных формул Φ указанная эквивалентность имеет место по определению интерпретации φ .

(ii) Предположим, что указанная эквивалентность имеет место для формул Φ и Ψ , и докажем, что тогда она выполняется и для формул

$$(\neg\Phi), \quad (\Phi \&\Psi), \quad (\Phi \vee \Psi), \quad (\Phi \rightarrow \Psi), \quad (\forall x)\Phi, \quad (\exists x)\Phi.$$

Так как

$$\bar{\Gamma} \vdash \neg\Phi \iff \bar{\Gamma} \not\vdash \Phi$$

и

$$\varphi(\Phi) = \text{Л} \iff \varphi(\neg\Phi) = \text{И},$$

то

$$\bar{\Gamma} \vdash \neg\Phi \iff \varphi(\neg\Phi) = \text{И}.$$

По теореме 3.5.7

$$\bar{\Gamma} \vdash (\Phi \& \Psi) \iff \bar{\Gamma} \vdash \Phi \text{ и } \bar{\Gamma} \vdash \Psi.$$

Кроме того, по определению интерпретации φ

$$\varphi(\Phi) = \text{И} \text{ и } \varphi(\Psi) = \text{И} \iff \varphi(\Phi \& \Psi) = \text{И}.$$

Значит,

$$\bar{\Gamma} \vdash (\Phi \& \Psi) \iff \varphi(\Phi \& \Psi) = \text{И}.$$

Покажем, что для **полного** множества формул $\bar{\Gamma}$ и произвольных *замкнутых* формул Φ и Ψ имеет место эквивалентность

$$\bar{\Gamma} \vdash (\Phi \vee \Psi) \iff \bar{\Gamma} \vdash \Phi \text{ или } \bar{\Gamma} \vdash \Psi$$

В самом деле, если

$$\bar{\Gamma} \vdash \Phi \text{ или } \bar{\Gamma} \vdash \Psi,$$

то, используя аксиому III.1 или III.2, получаем

$$\bar{\Gamma} \vdash (\Phi \vee \Psi).$$

Обратно, предположим, что

$$\bar{\Gamma} \vdash (\Phi \vee \Psi).$$

Покажем, что тогда

$$\bar{\Gamma} \vdash \Phi \text{ или } \bar{\Gamma} \vdash \Psi.$$

Предположим противное, т. е. что

$$\bar{\Gamma} \not\vdash \Phi \text{ и } \bar{\Gamma} \not\vdash \Psi.$$

Так как $\bar{\Gamma}$ – **полное** множество формул, то тогда

$$\bar{\Gamma} \vdash (\neg\Phi) \text{ и } \bar{\Gamma} \vdash (\neg\Psi),$$

а значит,

$$\bar{\Gamma} \vdash (\neg\Phi) \& (\neg\Psi).$$

Тождественно истинная формула **Логики Высказываний**

$$((\neg A_1 \& \neg A_2) \rightarrow \neg(A_1 \vee A_2))$$

по теореме 3.5.2 дает выводимость в **Исчислении Предикатов** формулы

$$((\neg\Phi \& \neg\Psi) \rightarrow \neg(\Phi \vee \Psi)).$$

Значит,

$$\bar{\Gamma} \vdash \neg(\Phi \vee \Psi).$$

Что в силу **непротиворечивости** множества формул $\bar{\Gamma}$ противоречит сделанному выше предположению

$$\bar{\Gamma} \vdash (\Phi \vee \Psi).$$

В итоге получаем

$$\bar{\Gamma} \vdash (\Phi \vee \Psi) \iff \bar{\Gamma} \vdash \Phi \text{ или } \bar{\Gamma} \vdash \Psi$$

и

$$\varphi(\Phi) = \text{И} \text{ или } \varphi(\Psi) = \text{И} \iff \varphi(\Phi \vee \Psi) = \text{И},$$

поэтому

$$\bar{\Gamma} \vdash (\Phi \vee \Psi) \iff \varphi(\Phi \vee \Psi) = \text{И}.$$

Доказательство эквивалентности

$$\bar{\Gamma} \vdash (\Phi \rightarrow \Psi) \iff \varphi(\Phi \rightarrow \Psi) = \text{И}$$

проводится по той же схеме с использованием полноты и непротиворечивости множества формул $\bar{\Gamma}$.

Тождественно истинные формулы **Логики Высказываний**

$$((A_1 \rightarrow A_2) \rightarrow (\neg A_1 \vee A_2))$$

и

$$((\neg A_1 \vee A_2) \rightarrow (A_1 \rightarrow A_2))$$

по теореме 3.5.2 дает выводимость в **Исчислении Предикатов** формул

$$((\Phi \rightarrow \Psi) \rightarrow (\neg \Phi \vee \Psi)),$$

$$((\neg \Phi \vee \Psi) \rightarrow (\Phi \rightarrow \Psi)).$$

Поэтому

$$\bar{\Gamma} \vdash ((\Phi \rightarrow \Psi)$$

тогда и только тогда, когда

$$\bar{\Gamma} \vdash (\neg \Phi \vee \Psi).$$

Как уже было показано выше, последнее выполнено тогда и только тогда, когда

$$\bar{\Gamma} \not\vdash \Phi \text{ или } \bar{\Gamma} \vdash \Psi).$$

По индуктивному предположению это выполнено тогда и только тогда, когда

$$\varphi(\Phi) = \text{Л} \text{ или } \varphi(\Psi) = \text{И}.$$

А последнее эквивалентно равенству

$$\varphi((\Phi \rightarrow \Psi)) = \text{И}.$$

Остается рассмотреть формулы вида $(\exists x)\Phi$ и $(\forall x)\Phi$. Именно при их рассмотрении нам понадобится **свойство Генкина**.

Если Φ – формула, не содержащая свободных переменных, отличных от x , то по определению

$$\begin{aligned} \mathcal{A}_{\tau+} \models (\exists x)\Phi &\iff \\ \mathcal{A}_{\tau+} \models \Phi_x[t] &\text{ для имени } t \text{ некоторого индивида } t \text{ из } A, \text{ т. е. терма } t. \end{aligned}$$

Покажем, что имеет место эквивалентность:

$$\bar{\Gamma} \vdash (\exists x)\Phi \iff \varphi((\exists x)\Phi) = \text{И}.$$

Если

$$\bar{\Gamma} \vdash (\exists x)\Phi,$$

то в силу **свойства Генкина** найдется такой замкнутый терм t , что

$$\bar{\Gamma} \vdash \Phi_x[t].$$

По индуктивному предположению тогда $\varphi(\Phi_x[t]) = \text{И}$, поэтому и

$$\varphi((\exists x)\Phi) = \text{И}.$$

Если же $\varphi((\exists x)\Phi) = \text{И}$, то найдется такой замкнутый терм t , что

$$\varphi(\Phi_x[t]) = \text{И}.$$

По индуктивному предположению тогда

$$\bar{\Gamma} \vdash \Phi_x[t].$$

Так как

$$\vdash (\Phi_x[t] \rightarrow (\exists x)\Phi),$$

то

$$\bar{\Gamma} \vdash (\exists x)\Phi.$$

Тем самым доказано, что

$$\bar{\Gamma} \vdash (\exists x)\Phi \iff \varphi((\exists x)\Phi) = \text{И}.$$

По той же схеме доказывается, что

$$\bar{\Gamma} \vdash (\forall x)\Phi \iff \varphi((\forall x)\Phi) = \text{И}.$$

В итоге доказано, что для произвольной замкнутой формулы Φ имеет место эквивалентность:

$$\bar{\Gamma} \vdash \Phi \iff \varphi(\Phi) = \text{И}.$$

Если Φ – произвольная формула из множества $\bar{\Gamma}$, то, очевидно, $\bar{\Gamma} \vdash \Phi$, значит, $\bar{\Gamma} \vdash \forall\Phi$, где $\forall\Phi$ – \forall -замыкание формулы Φ .

Поэтому $\varphi(\forall\Phi) = \text{И}$.

Значит, $\varphi(\bar{\Gamma}) = \text{И}$, поэтому множество формул $\bar{\Gamma}$ **является совместным**. □

Важным следствием и уточнением **Теоремы Непротиворечивости** является следующая теорема, носящая название **Теорема Левенгейма – Сколема**.

Теорема 3.5.31. *Если счетное множество формул Γ является **совместным**, то существует интерпретация со счетным основным множеством, в которой все формулы из Γ истинны.*

Доказательство. Пусть Γ – счетное множество формул языка L_τ . Обозначим через τ_1 сигнатуру, включающую в себя лишь те символы сигнатуры L_τ , которые входят в формулы из Γ .

Из счетности множества формул Γ следует, что сигнатура τ_1 конечная или счетная, т. е. не более чем счетная. Поэтому можно считать, что Γ – счетное множество формул языка L_{τ_1} не более чем счетной сигнатуры τ_1 . Чтобы не усложнять обозначения, будем вместо τ_1 писать просто τ .

Если Γ – **совместное** множество формул, то оно **непротиворечиво**.

Проанализируем в этом случае доказательство **Теоремы Непротиворечивости**.

Сигнатура τ^+ получается из сигнатуры τ добавлением *счетного* множества символов индивидуальных констант, поэтому τ^+ – **счетная** сигнатура.

Значит, **счетным** будет и множество \mathcal{T}_{τ^+} всех **замкнутых термов** языка L_{τ^+} . А это множество \mathcal{T}_{τ^+} и является **основным множеством** A построенной в ходе доказательства **Теоремы Непротиворечивости** интерпретации I , в которой истинны все формулы из множества Γ . \square

В качестве непосредственного следствия получаем следующее утверждение.

Следствие. *Если счетное множество формул Γ является **совместным**, то существует интерпретация с множеством натуральных чисел в качестве основного множества, в которой все формулы из Γ истинны.*

Другими словами: *если счетное множество формул Γ выполнимо, то оно выполнимо на множестве натуральных чисел.*

Если счетное множество формул Γ языка L_τ сигнатуры τ является **совместным**, то по теореме Левенгейма – Сколема существует интерпретация I со счетным основным множеством A , в которой все формулы из Γ истинны.

Построим интерпретацию I_N языка L_τ сигнатуры τ с множеством N натуральных чисел в качестве основного множества.

Пусть φ – биективное отображение множества натуральных чисел N на множество A .

Для произвольных n -местного функционального символа f и n -местного предикатного символа p сигнатуры τ и произвольных натуральных чисел m_1, \dots, m_n полагаем:

$$I_N(f)(m_1, \dots, m_n) = \varphi^{-1}(I(f)(\varphi(m_1), \dots, \varphi(m_n)));$$

$$I_N(p)(m_1, \dots, m_n) = I(p)(\varphi(m_1), \dots, \varphi(m_n)).$$

Индукцией по построению формул легко доказывается, что для произвольной формулы Φ языка L_τ сигнатуры τ , все свободные переменные которой содержатся в списке x_1, \dots, x_n , и произвольных натуральных чисел m_1, \dots, m_n выполняется равенство

$$I_N(\Phi_{x_1, \dots, x_n}[m_1, \dots, m_n]) = I(\Phi_{x_1, \dots, x_n}[\varphi(m_1), \dots, \varphi(m_n)]).$$

Это доказательство может быть без труда проведено читателем в качестве полезного упражнения.

Рассмотренные выше **Исчисление Высказываний** и **Исчисление Предикатов** являются важными частными случаями общего понятия **формальной** или **аксиоматической теории**.

Формальная или **аксиоматическая теория** \mathcal{T} считается заданной, если выполнены следующие условия:

1) задано некоторое множество $\Sigma_{\mathcal{T}}$ символов - символов теории \mathcal{T} , которые образуют **алфавит теории** \mathcal{T} . Конечные последовательности символов алфавита теории \mathcal{T} , т. е. слова в этом алфавите, называются *выражениями теории* \mathcal{T} . Множество всех слов в алфавите $\Sigma_{\mathcal{T}}$ обозначается через $\Sigma_{\mathcal{T}}^*$.

2) определено подмножество $\mathcal{F}_{\mathcal{T}}$ множества $\Sigma_{\mathcal{T}}^*$ всех выражений теории \mathcal{T} , элементы которого называются **формулами теории** \mathcal{T} .

Если существует алгоритм, позволяющий по произвольному выражению в алфавите теории \mathcal{T} определить, является ли оно формулой этой теории, то говорят, что \mathcal{T} – **теория с эффективным понятием формулы**.

Если выполнены условия 1) и 2), то говорят, что задан язык $\mathcal{L}_{\mathcal{T}}$ теории \mathcal{T} .

3) выделено некоторое множество формул, называемых **аксиомами теории** \mathcal{T} .

Если существует алгоритм, позволяющий по произвольному выражению в алфавите теории \mathcal{T} определить, является ли оно аксиомой этой теории, то говорят, что \mathcal{T} – **теория с эффективным понятием аксиомы**.

4) определено конечное множество R_1, \dots, R_m отношений между формулами теории \mathcal{T} , называемых **правилами вывода**.

Если каждое отношение R_j является n_j -местным и для любого j существует алгоритм, позволяющий по любой формуле F и любым n_j формулам F_1, \dots, F_{n_j} определить, находится ли формула F в отношении R_j с формулами F_1, \dots, F_{n_j} (если "да", то формула F называется *непосредственным следствием* данных n_j формул F_1, \dots, F_{n_j} по правилу R_j), то говорят, что \mathcal{T} – **теория с эффективными правилами вывода**.

Правило вывода R_j часто записывается в виде

$$\frac{F_1, \dots, F_{n_j}}{F} (R_j).$$

Теория \mathcal{T} называется **теорией первого порядка**, если:

1) языком $\mathcal{L}_{\mathcal{T}}$ теории \mathcal{T} является язык \mathcal{L}_τ первого порядка некоторой сигнатуры τ ;

2) аксиомами теории \mathcal{T} являются *логические аксиомы* в языке $\mathcal{L}_{\mathcal{T}}$ и *некоторые другие формулы этого языка, называемые нелогическими аксиомами*;

3) правилами вывода являются введенные выше **Правило Отделения** MP , **Правило Введения** \exists и **Правило Введения** \forall .

Тем самым для задания теории первого порядка достаточно указать ее *нелогические аксиомы*, все остальное дано по определению теории. Заметим, что *логические аксиомы и правила вывода определены, как только выбран язык первого порядка, точнее, его сигнатура, они не зависят от нелогических аксиом*.

Выводом в теории \mathcal{T} называется любая конечная последовательность F_1, \dots, F_n формул языка $\mathcal{L}_{\mathcal{T}}$ этой теории такая, что при любом i либо формула F_i является логической аксиомой, либо формула F_i является нелогической аксиомой, либо формула F_i является непосредственным следствием некоторых предыдущих формул этой последовательности по одному из правил вывода.

Формула F называется **выводимой в теории \mathcal{T}** или **теоремой** этой теории, если существует вывод в этой теории, оканчивающийся формулой F . Такой вывод называется **выводом формулы F** .

Запись $\vdash_{\mathcal{T}} F$ служит сокращенной записью утверждения "формула F является теоремой теории \mathcal{T} ".

Для исследования отношения выводимости $\vdash_{\mathcal{T}} F$ полезны так называемые **вспомогательные правила вывода**.

Вспомогательное правило вывода \mathcal{R} теории \mathcal{T} – это любое выражение вида

$$\frac{\vdash_{\mathcal{T}} F_1, \dots, \vdash_{\mathcal{T}} F_n}{\vdash_{\mathcal{T}} F} \quad (\mathcal{R})$$

такое, что для любых формул F_1, \dots, F_n и F теории \mathcal{T} из выводимости в теории \mathcal{T} формул F_1, \dots, F_n следует выводимость формулы F в этой теории.

Рассмотрим примеры вспомогательных правил вывода, справедливость которых установлена выше.

Правило перестановки посылок

$$\frac{\vdash_{\mathcal{T}} (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C}))}{\vdash_{\mathcal{T}} (\mathcal{B} \rightarrow (\mathcal{A} \rightarrow \mathcal{C}))}.$$

Правило объединения посылок

$$\frac{\vdash_{\mathcal{T}} (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C}))}{\vdash_{\mathcal{T}} ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{C})}.$$

Правило разъединения посылок

$$\frac{\vdash_{\mathcal{T}} ((\mathcal{A} \& \mathcal{B}) \rightarrow \mathcal{C})}{\vdash_{\mathcal{T}} (\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C}))}.$$

Правило транзитивности

$$\frac{\vdash_{\mathcal{T}} (\mathcal{A} \rightarrow \mathcal{B}), \vdash_{\mathcal{T}} (\mathcal{B} \rightarrow \mathcal{C})}{\vdash_{\mathcal{T}} (\mathcal{A} \rightarrow \mathcal{C})}.$$

Четыре однотипных правила можно объединить в одно

Правило антисимметричности

$$\frac{\vdash_{\mathcal{T}} (\mathcal{A} \rightarrow \mathcal{B})}{\vdash_{\mathcal{T}} ((\neg \mathcal{B}) \rightarrow (\neg \mathcal{A}))}, \quad \frac{\vdash_{\mathcal{T}} (\mathcal{A} \rightarrow (\neg \mathcal{B}))}{\vdash_{\mathcal{T}} (\mathcal{B} \rightarrow (\neg \mathcal{A}))},$$

$$\frac{\vdash_{\mathcal{T}} ((\neg \mathcal{A}) \rightarrow \mathcal{B})}{\vdash_{\mathcal{T}} ((\neg \mathcal{B}) \rightarrow \mathcal{A})}, \quad \frac{\vdash_{\mathcal{T}} ((\neg \mathcal{A}) \rightarrow (\neg \mathcal{B}))}{\vdash_{\mathcal{T}} (\mathcal{B} \rightarrow \mathcal{A})}.$$

Правило обобщения

$$\frac{\vdash_{\mathcal{T}} \mathcal{A}}{\vdash_{\mathcal{T}} (\forall x)\mathcal{A}}.$$

с равенством

3.6. Логика первого порядка с равенством

В этом параграфе рассматриваются некоторые вопросы для **Логики предикатов с равенством** произвольной сигнатуры

$$\tau = \langle C, F, P, \theta, \varphi \rangle,$$

во множестве P предикатных символов которой выделен 2-местный предикатный символ, обозначаемый через $=$.

По сигнатуре $\tau = \langle C, F, P, \theta, \varphi \rangle$ обычным образом строится язык первого порядка L_{τ} . Напомним, что его алфавит Σ_{τ} языка L_{τ} является объединением следующих пяти множеств символов: V , Σ_1 , Σ_2 , Σ_3 , C , F и P , где

(i) $V = \{x_1, x_2, \dots\}$ – счетное множество **предметных (индивидуальных) переменных**. Каждый элемент x_i множества V называется **индивидуальной (предметной) переменной**.

(ii) $\Sigma_1 = \{\neg, \vee, \&, \rightarrow\}$ – множество 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 связками**, причем \neg – одноместной связкой, а \vee , $\&$ и \rightarrow – двуместными связками.

(iii) множество Σ_2 состоит из двух символов \exists и \forall , называемых соответственно **квантором существования** и **квантором общности**.

(iv) множество Σ_3 состоит из двух технических символов: $($ – **левая скобка** и $)$ – **правая скобка**.

Понятия **терма** и **формулы** определяются обычным образом как и в случае произвольной сигнатуры. Однако формулу $= (t_1, t_2)$ будем записывать в более привычном виде $t_1 = t_2$.

Понятие **интерпретации** для **Логики предикатов с равенством** отличается от аналогичного понятия для **Логики предикатов** произвольной сигнатуры введением лишь одного дополнительного условия – **выделенный 2-местный предикатный символ $=$ интерпретируется как обычное равенство**

на основном множестве интерпретации. Чтобы подчеркнуть, что для рассматриваемой интерпретации I это условие выполнено, будем называть I **нормальной интерпретацией**.

Таким образом, задание **нормальной интерпретации I Логике предикатов с равенством** сигнатуры τ включает в себя

- (i) задание непустого множества A , называемого **основным множеством** (универсумом или носителем) интерпретации I ;
- (ii) задание отображения γ_1 множества C индивидуальных констант сигнатуры τ во множество A ;
- (iii) задание отображения γ_2 множества F функциональных символов сигнатуры τ во множество алгебраических операций на множестве A , причем если $f \in F$, то $\gamma_2(f)$ – это $\theta(f)$ -местная алгебраическая операция на A ;
- (iv) задание отображения γ_3 множества P предикатных символов во множество предикатов, определенных на A , такое, что если $p \in P$, то $\gamma_3(p)$ – это $\varphi(p)$ -местный предикат на A и $\gamma_3(=)$ – это **обычное равенство** на A .

Как и в случае произвольной сигнатуры, для каждого индивида $a \in A$ мы выбираем новую константу \bar{a} , называемую **именем** индивида a . При этом придерживаемся соглашения: если $\bar{a} = \bar{b}$, то $a = b$, т. е. **для разных индивидов выбираются разные имена**.

Обозначим через $\tau(A)$ сигнатуру, полученную из сигнатуры τ добавлением к множеству C индивидуальных констант сигнатуры τ множества \bar{A} всех **имен индивидов** из A .

Язык $L_{\tau(A)}$ первого порядка сигнатуры $\tau(A)$ будем обозначать через $L_\tau(A)$ или просто через $L(A)$ и говорить, что он *получен из языка L добавлением всех имен индивидов из A* .

Для каждого, не содержащего переменных терма t языка $L(A)$, как и в случае произвольной интерпретации, определяется индивид $I(t)$ из A , который называется *соответствующим терму t в нормальной интерпретации I* .

Для каждой замкнутой формулы Φ языка $L(A)$ по той же схеме что и в случае произвольной интерпретации определяется **истинностное значение** $I(\Phi)$ формулы Φ в нормальной интерпретации I .

Единственное отличие от общего случая состоит в том, что для атомной формулы вида $=(t_1, t_2)$ полагаем

$$I(=(t_1, t_2)) = \text{И} \iff I(t_1) \text{ совпадает с } I(t_2).$$

Пусть Φ – произвольная формула языка L , а v_1, \dots, v_n – все ее свободные переменные. Если $\bar{a}_1, \dots, \bar{a}_n$ – имена произвольных индивидов a_1, \dots, a_n из A , то формулу

$$\Phi_{v_1, \dots, v_n}[\bar{a}_1, \dots, \bar{a}_n]$$

называем **A -частным случаем** формулы Φ .

Определение 3.6.1. Произвольная формула Φ языка L называется **истинной** в нормальной интерпретации I , если для любого \mathcal{A} -частного случая Φ' формулы Φ $I(\Phi') = \mathbb{I}$.

Если формула Φ содержит лишь свободные переменные v_1, \dots, v_n (в алфавитном порядке) ($n \geq 0$), то \forall -замыканием формулы Φ назовем формулу вида $(\forall v_1) \dots (\forall v_n) \Phi$.

\forall -замыкание формулы Φ обозначим через $\forall \Phi$.

Ясно, что $\forall \Phi$ – замкнутая формула, и если Φ – замкнутая формула, то $\forall \Phi$ – это просто Φ .

Нетрудно понять, что формула Φ языка L **истинна** в нормальной интерпретации I тогда и только тогда, когда $I(\forall \Phi) = \mathbb{I}$.

Пусть Γ – произвольное множество формул языка L . Если I – нормальная интерпретация языка L первого порядка с равенством, в которой истинны все формулы из множества Γ , то I называется **нормальной моделью** для Γ .

Обычным образом определяется понятие **логического следствия**.

Определение 3.6.2. Формула Φ языка L первого порядка с равенством называется **логическим следствием** множества формул Γ , если Φ истинна в каждой нормальной модели для Γ , т. е. для любой нормальной интерпретации I языка L из того, что все формулы множества Γ истинны в нормальной интерпретации I следует, что в I истинна и формула Φ .

Запись $\Gamma \models_n \Phi$ будет служить сокращением для утверждения ”формула Φ является **логическим следствием** множества формул Γ ”.

Напомним, что для произвольной интерпретации I и любой замкнутой формулы \mathcal{A} языка L_τ истинностное значение $I(\mathcal{A})$ мы называем **истинностным значением** формулы \mathcal{A} в интерпретации I . Если при этом $I(\mathcal{A}) = \mathbb{I}$, то говорим, что формула \mathcal{A} **истинна в интерпретации I** , а если $I(\mathcal{A}) = \mathbb{L}$, то говорим, что формула \mathcal{A} **ложна в интерпретации I** .

Определение 3.6.3. Формула \mathcal{A} языка L_τ первого порядка с равенством называется **выполнимой**, если существует нормальная интерпретация, в которой эта формула истинна.

Определение 3.6.4. Множество формул Γ языка L_τ первого порядка с равенством называется **совместным**, если существует **нормальная интерпретация**, в которой все формулы из этого множества истинны.

Замечание. Для произвольного множества формул Γ языка L_τ и для любой нормальной интерпретации I запись

$$I(\Gamma) = \mathbb{I}$$

служит сокращением для утверждения ”все формулы множества Γ истинны в нормальной интерпретации I ”.

Определение 3.6.5. Формула A языка L_τ первого порядка с равенством называется **тождественно истинной**, если она истинна в любой нормальной интерпретации этого языка.

Для углубленного изучения понятия совместности множества формул языка первого порядка с равенством и отношения логического следствия нам будут полезны их финитные аналоги.

Определение 3.6.6. Множество формул Γ языка L_τ первого порядка с равенством называется **локально совместным**, если любое его **конечное подмножество** совместно, т. е. имеет нормальную модель.

Определение 3.6.7. Формула A языка L_τ называется **локальным логическим следствием** множества формул Γ этого языка L_τ , если она является логическим следствием некоторого **конечного подмножества** Γ_0 множества Γ .

Замечание. В этом параграфе запись $\Gamma \models_{fin} A$ будет служить сокращением для утверждения "формула A является локальным логическим следствием множества формул Γ ."

Определение 3.6.8. Множество формул Γ языка L_τ назовем **локально полным**, если оно локально совместно и для любой замкнутой формулы A языка L_τ либо $\Gamma \models_{fin} A$, либо $\Gamma \models_{fin} (\neg A)$.

Замечание. Если Γ – локально совместное множество формул, то не существует такой замкнутой формулы A , что $\Gamma \models_{fin} A$ и $\Gamma \models_{fin} (\neg A)$. В самом деле, предположим, что существует такая замкнутая формула A , что $\Gamma \models_{fin} A$ и $\Gamma \models_{fin} (\neg A)$. В соответствии с определением найдутся такие конечные подмножества Γ_1 и Γ_2 множества Γ , 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 Γ .

Теорема 3.6.1. Для любого локально совместного множества формул Γ языка L_τ **Логики Предикатов с равенством** существует такое локально полное множество формул Γ^* языка L_τ , что

$$\Gamma \subseteq \Gamma^*.$$

Доказательство. Дадим два варианта доказательства. В первом варианте доказательства будем считать, что сигнатура τ **счетная**. Тогда счетными будут и алфавит языка L_τ **Логики Предикатов с равенством**, и множество F_τ всех замкнутых формул **Логики Предикатов с равенством** этой сигнатуры.

Пусть $F_\tau = (\Phi_n)_{n \in \mathbb{N}}$.

Определим последовательность $(\Gamma_n)_{n \in \mathbb{N}}$ множеств формул.

Полагаем

$$\Gamma_1 \Rightarrow \Gamma.$$

Если множество Γ_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 Γ_n является **локально совместным**.

Так как $\Gamma_1 \Rightarrow \Gamma$, то множество формул Γ_1 является **локально совместным** по условию теоремы.

Предположим, что уже доказана локальная совместность множества формул Γ_n . Докажем локальную совместность множества формул Γ_{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 Γ' – конечное подмножество множества Γ_n . Пусть Γ'' – такое конечное подмножество множества Γ_n , что $\Gamma'' \models \Phi_n$. Для конечного подмножества $\Gamma' \cup \Gamma''$ локально совместного множества формул Γ_n существует нормальная интерпретация I такая, что

$$I(\Gamma' \cup \Gamma'') = \mathbb{I}.$$

Тогда $I(\Phi_n) = \mathbb{I}$ и $I(\Gamma' \cup \{\Phi_n\}) = \mathbb{I}$. Значит, множество $\Gamma' \cup \{\Phi_n\}$ совместно, поэтому в рассматриваемом случае множество Γ_{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 Γ_{n+1} не является локально совместным, то найдется такое конечное подмножество Γ' множества Γ_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 $\Gamma_n \not\models_{fin} \Phi_n$. Значит, и в этом случае множество формул Γ_{n+1} является локально совместным.

Тем самым доказано, что *при любом n множество формул Γ_n является локально совместным*.

Полагаем

$$\Gamma^* \Rightarrow \bigcup_{n=1}^{\infty} \Gamma_n.$$

Покажем, что Γ^* – **локально полное множество формул** и

$$\Gamma \subseteq \Gamma^*.$$

Последнее очевидно, так как

$$\Gamma = \Gamma_1 \subseteq \Gamma^*.$$

Если бы множество формул $\bar{\Gamma}$ 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 Γ_n .

Значит, Γ^* – **локально совместное** множество формул.

Пусть \mathcal{A} – произвольная замкнутая формула. Тогда найдется такое число n , что $\mathcal{A} \equiv \Phi_n$.

Если $\Gamma_n \models_{fin} \Phi_n$, то $\Gamma^* \models_{fin} \Phi_n$, а, значит, $\Gamma^* \models_{fin} \mathcal{A}$.

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. $\Gamma^* \models_{fin} (\neg \mathcal{A})$.

Итак доказано, что Γ^* – **локально полное** множество формул языка L_τ такое, что $\Gamma \subseteq \Gamma^*$.

В случае произвольной сигнатуры τ возможно аналогичное доказательство, однако при этом вместо достаточно простой индукции по n необходимо использовать *трансфинитную индукцию*. Мы не будем рассматривать этот вариант доказательства, а приведем доказательство с использованием **Леммы Тейхмюллера – Тьюки**.

Напомним, что 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} .

Как уже отмечалось выше следующее утверждение, эквивалентно **Аксиоме выбора**.

Лемма Тейхмюллера – Тьюки.

*Каждое семейство подмножеств \mathcal{X} множества E , имеющее конечный характер, обладает **максимальным элементом**.*

Рассмотрим следующее семейство подмножеств \mathcal{X} множества F_τ всех формул языка L_τ

$$T \in \mathcal{X} \iff T \cup \Gamma \text{ — локально совместно.}$$

Из определения семейства подмножеств \mathcal{X} сразу следует, что оно имеет *конечный характер*. По **Лемме Тейхмюллера – Тьюки** в семействе подмножеств \mathcal{X} имеется **максимальный элемент** T^* . Покажем, что множество $\Gamma^* = \Gamma \cup T^*$ является **локально полным**.

Из определения семейства подмножеств \mathcal{X} сразу следует, что множество Γ^* является **локально совместным**.

Докажем **полноту** множества Γ^* .

Пусть \mathcal{A} – произвольная замкнутая формула.

Если множество $\Gamma^* \cup \{(\neg \mathcal{A})\}$ не является **локально совместным**, то

$$\Gamma^* \vdash_{fin} \mathcal{A}.$$

Если же множество $\Gamma^* \cup \{(\neg \mathcal{A})\}$, т. е. множество $\Gamma \cup T^* \cup \{(\neg \mathcal{A})\}$, является **локально совместным**, то в силу максимальности T^* получаем $(\neg \mathcal{A}) \in T^*$. Значит, $\Gamma^* \vdash_{fin} (\neg \mathcal{A})$.

Итак, Γ^* – **локально полное расширение** локально совместного множества формул Γ . \square

На первый взгляд кажется, что второй вариант доказательства ”проще” первого, однако это обманчивое впечатление – во втором варианте вся идейная трудность доказательства перенесена в доказательство эквивалентности **Леммы Тейхмюллера – Тьюки Аксиоме Выбора**.

Для множества формул Σ языка L_τ первого порядка с равенством сигнатуры τ выполнено **свойство Генкина**, если для любой формулы F с одной свободной переменной v из того, что $\Sigma \models_{fin} (\exists v)F$, следует, что найдется такой замкнутый терм t , что $\Sigma \models_{fin} F_v[t]$.

Теорема 3.6.2. Для любого локально совместного множества формул Γ языка L_τ первого порядка с равенством сигнатуры τ можно построить локально совместное множество формул Γ^+ языка L_{τ^+} первого порядка с равенством сигнатуры τ^+ такое, что $\Gamma \subseteq \Gamma^+$, сигнатура τ^+ получается из сигнатуры τ добавлением новых индивидных констант и для множества формул Γ^+ выполнено свойство Генкина.

До к а з а т е л ь с т в о. Доказательство проведем лишь в случае счетной сигнатуры. Общий случай рассматривается по аналогичной схеме.

Рассмотрим сигнатуру τ^+ , полученную из сигнатуры τ добавлением *счетного* множества $\{c_1, c_2, \dots, c_m, \dots\}$ новых индивидных констант.

Заметим, что любую нормальную интерпретацию языка L_τ сигнатуры τ можно продолжить до нормальной интерпретации языка L_{τ^+} сигнатуры τ^+ , определив лишь ее значения для новых индивидных констант $\{c_1, c_2, \dots, c_m, \dots\}$, а любую нормальную интерпретацию языка L_{τ^+} сигнатуры τ^+ можно сузить до нормальной интерпретации языка L_τ сигнатуры τ , ”игнорируя” ее значения для новых индивидных констант $\{c_1, c_2, \dots, c_m, \dots\}$.

Локально совместное множество формул Γ языка L_τ сигнатуры τ мы рассматриваем как локально совместное множество формул языка L_{τ^+} сигнатуры τ^+ .

Так как сигнатура τ по предположению *счетная*, то счетными будут сигнатура τ^+ , алфавит языка L_{τ^+} **Логики Предикатов** этой сигнатуры и множество F_{τ^+} всех формул **Логики Предикатов** этой сигнатуры τ^+ .

Занумеруем $(F_n)_{n \in \mathbb{N}}$ все формулы языка L_{τ^+} , содержащие в точности одну свободную переменную. Для каждой формулы F_n через v_n будем обозначать ее единственную свободную переменную.

Индукцией по n построим последовательность $d_1, d_2, \dots, d_n, \dots$ из новых констант $\{c_1, c_2, \dots, c_m, \dots\}$ и локально совместные множества формул Γ_n .

Пусть d_1 – это любая новая константа c_i , не входящая в формулу F_1 . Полагаем

$$\Gamma_1 = \Gamma \cup \{((\exists v_1)F \rightarrow F_{v_1}[d_1])\}.$$

Докажем локальную совместность множества формул Γ_1 . Пусть Γ_0 – произвольное конечное подмножество множества Γ . Существует нормальная интерпретация I с основным множеством A языка $L_{\tau+}$, в которой все формулы из множества Γ_0 истинны. Заметим, что если мы изменим значения интерпретации I на некоторых новых константах c_i , то в новой нормальной интерпретации I' значения всех формул языка L_{τ} не изменятся, в частности, все формулы из множества Γ_0 будут истинны.

Если $I((\exists v_1)F_1) = \text{И}$ и a – такой элемент из основного множества A , что $I(F_{1,v_1}[\bar{a}]) = \text{И}$, то изменим значение $I(d_1)$, определив новое значение равенством $I'(d_1) = a$. Тогда

$$I'((\exists v_1)F_1 \rightarrow F_{1,v_1}[d_1]) = \text{И}.$$

Если же $I((\exists v_1)F_1) = \text{Л}$, то

$$I((\exists v_1)F_1 \rightarrow F_{1,v_1}[d_1]) = \text{И}.$$

Так как в формулы множества Γ_0 не входят новые константы, то для любой формулы F из Γ_0 получаем $I(F) = I'(F) = \text{И}$.

Значит, $\Gamma_0 \cup \{((\exists v_1)F \rightarrow F_{v_1}[d_1])\}$ **совместно**, поэтому

$$\Gamma_1 = \Gamma \cup \{((\exists v_1)F \rightarrow F_{v_1}[d_1])\}$$

локально совместно.

Пусть уже построены начальный отрезок d_1, d_2, \dots, d_n последовательности из новых констант и локально совместное множество формул Γ_n , причем

$$\Gamma_n = \Gamma_{n-1} \cup \{((\exists v_n)F \rightarrow F_{v_n}[d_n])\}.$$

Пусть d_{n+1} – это любая новая константа c_i , отличная от уже определенных констант d_1, d_2, \dots, d_n и не входящая в формулы F_1, F_2, \dots, F_n и F_{n+1} . Полагаем

$$\Gamma_{n+1} = \Gamma_n \cup \{((\exists v_{n+1})F \rightarrow F_{v_{n+1}}[d_{n+1}])\}.$$

Докажем **локальную совместность** множества формул Γ_{n+1} .

Пусть Γ_0 – произвольное конечное подмножество множества Γ_n . Существует нормальная интерпретация I с основным множеством A языка $L_{\tau+}$, в которой все формулы из множества Γ_0 истинны. Заметим, что константа d_{n+1} не входит в формулы из множества Γ_n , поэтому если для интерпретации I изменить лишь значение $I(d_{n+1})$, то для полученной новой нормальной интерпретации I' для любой формулы F из Γ_n получаем $I(F) = I'(F)$. Поэтому, в частности, все формулы из множества Γ_0 будут истинны в нормальной интерпретации I' .

Если $I((\exists v_{n+1})F_{n+1}) = \mathbb{I}$ и a – такой элемент из основного множества A , что $I(F_{n+1, v_{n+1}}[\bar{a}]) = \mathbb{I}$, то изменим значение $I(d_{n+1})$, определив новое значение равенством $I'(d_{n+1}) = a$. Тогда

$$I'((\exists v_{n+1})F_{n+1} \rightarrow F_{n+1, v_{n+1}}[d_{n+1}]) = \mathbb{I}.$$

Если же $I((\exists v_{n+1})F_{n+1}) = \mathbb{L}$, то

$$I((\exists v_{n+1})F_{n+1} \rightarrow F_{n+1, v_{n+1}}[d_{n+1}]) = \mathbb{I}.$$

Так как в формулы множества Γ_0 не входит новая константа d_{n+1} , то для любой формулы F из Γ_0 получаем $I'(F) = I(F) = \mathbb{I}$.

Значит, $\Gamma_0 \cup \{((\exists v_{n+1})F \rightarrow F_{v_{n+1}}[d_{n+1}])\}$ **совместно**, поэтому

$$\Gamma_{n+1} = \Gamma_n \cup \{((\exists v_{n+1})F \rightarrow F_{v_{n+1}}[d_{n+1}])\}$$

локально совместно.

Полагаем

$$\Gamma^+ \Leftarrow \bigcup_{n=1}^{\infty} \Gamma_n.$$

Покажем, что Γ^+ – **локально совместное множество формул, обладающее свойством Генкина** и

$$\Gamma \subseteq \Gamma^+.$$

Последнее очевидно. Для доказательства **локальной совместности** множества формул Γ^+ рассмотрим произвольное его *конечное* подмножество Γ_0 . Так как при любом k $\Gamma_k \subseteq \Gamma_{k+1}$, то найдется такое n , что $\Gamma_0 \subseteq \Gamma_n$. Так как выше уже доказано, что Γ_n **локально совместно**, то Γ_0 совместно, поэтому Γ^+ **локально совместно**.

Докажем, что множество формул Γ^+ обладает **свойством Генкина**.

Пусть F – произвольная формула с одной свободной переменной v . Найдется такое n , что F – это F_n , а v – это v_n . Тогда

$$((\exists v_n)F \rightarrow F_{v_n}[d_n]) \in \Gamma_n \subseteq \Gamma^+,$$

т. е.

$$((\exists v)F \rightarrow F_v[d_n]) \in \Gamma_n \subseteq \Gamma^+.$$

Если $\Gamma^+ \models_{fin} (\exists v)F$, то найдется такое конечное подмножество Γ_0 множества Γ^+ , что $\Gamma_0 \models (\exists v)F$. Но тогда

$$\Gamma_0 \cup \{((\exists v)F \rightarrow F_v[d_n])\} \models F_v[d_n],$$

значит, $\Gamma^+ \models_{fin} F_v[d_n]$. □

Замечание. Построенное множество формул Γ^+ обладает следующим важным для дальнейшего свойством: если F – произвольная формула с одной свободной переменной v , то найдется такая константа c , что

$$((\exists v)F \rightarrow F_v[c]) \in \Gamma^+.$$

Поэтому, если T – любое множество формул той же сигнатуры, что и Γ^+ , причем $\Gamma^+ \subseteq T$, то

$$((\exists v)F \rightarrow F_v[c]) \in T.$$

В частности, для T выполнено свойство Генкина.

Теорема компактности или локальная теорема К. Геделя – А.И. Мальцева для Логике Предикатов с равенством. Множество замкнутых формул Γ языка L_τ первого порядка с равенством является **совместным**, тогда и только тогда, когда оно является **локально совместным**.

Доказательство. Если множество формул Γ языка L_τ первого порядка с равенством является **совместным**, то, очевидно, является совместным и любое его подмножество. В частности, является совместным и любое конечное подмножество множества формул Γ . Значит, Γ **локально совместно**.

Обратно, предположим, что множество Γ **локально совместно**, т. е. любое его конечное подмножество является совместным. Докажем, что тогда совместно и все множество Γ .

Мы дадим два доказательства этого важного факта, чтобы продемонстрировать некоторые общие методы математической логики, работающие и в более сложных ситуациях.

Первое доказательство.

Применив две предыдущие теоремы, мы получим **локально полное, обладающее свойством Генкина** множество формул

$$\bar{\Gamma} = (\Gamma^+)^*$$

языка первого порядка L_{τ^+} сигнатуры τ^+ , полученной из сигнатуры τ добавлением новых индивидуальных констант такое, что $\Gamma \subseteq \bar{\Gamma}$.

Покажем, что множество формул $\bar{\Gamma}$ является **совместным**. Отсюда, конечно, сразу будет следовать **совместность и множества формул Γ** .

Построим **нормальную интерпретацию** I такую, что $I(\bar{\Gamma}) = \text{И}$.

Для языка первого порядка L_{τ^+} сигнатуры τ^+ , используя **локально полное, обладающее свойством Генкина** множество формул $\bar{\Gamma}$, построим **естественную структуру** \mathcal{A}_{τ^+} – алгебраическую систему сигнатуры τ^+ , основным множеством A которой будет множество \mathcal{T}_{τ^+} всех замкнутых термов языка L_{τ^+} .

Каждой **индивидуальной константе** c сигнатуры τ^+ сопоставим **терм** c – элемент основного множества A естественной структуры \mathcal{A}_{τ^+} .

Каждому n -местному **функциональному символу** f сигнатуры τ^+ сопоставим n -местную *алгебраическую операцию* $f^{A_{\tau^+}}$ на основном множестве A естественной структуры A_{τ^+} , полагая для произвольных элементов t_1, \dots, t_n множества A , т. е. термов языка L_{τ^+} ,

$$f^{A_{\tau^+}}(t_1, \dots, t_n) \equiv f(t_1, \dots, t_n).$$

Каждому n -местному **предикатному символу** p сигнатуры τ^+ сопоставим n -местный *предикат* $p^{A_{\tau^+}}$ на основном множестве A естественной структуры A_{τ^+} , полагая для произвольных элементов t_1, \dots, t_n множества A , т. е. термов языка L_{τ^+} ,

$$p^{A_{\tau^+}}(t_1, \dots, t_n) = \text{И} \iff \bar{\Gamma} \models_{fin} p(t_1, \dots, t_n).$$

Для каждого индивида $t \in A$, т. е. терма t сигнатуры τ^+ , его *именем* будет он сам t . Тогда сигнатура $\tau^+(A)$, полученная из сигнатуры τ^+ добавлением к множеству C индивидных констант сигнатуры τ^+ множества \bar{A} всех *имен индивидов* из A , будет совпадать с исходной сигнатурой τ^+ , а язык $L_{\tau^+(A)}$ – с исходным языком L_{τ^+} .

Для каждого свободного от переменных терма t языка L_{τ^+} обычным образом индукцией по построению терма t определяем индивид $\mathcal{A}(t)$ из A , который *будет соответствовать терму* t .

Нетрудно понять, что в рассматриваемом случае $\mathcal{A}(t)$ – это t , но это разные t – первое t – это терм t языка L_{τ^+} , а второе t – это элемент t основного множества A естественной структуры A_{τ^+} языка L_{τ^+} .

Обычным способом для каждой замкнутой (т. е. не содержащей свободных переменных) формулы Φ языка $L_{\tau^+(A)}$ определяем ее *истинностное значение* $I(\Phi)$ в системе A_{τ^+} индукцией по построению формулы Φ (т. е. сопоставим Φ значение И или Л).

Условимся писать:

$$\begin{aligned} \mathcal{A}_{\tau^+} \models \Phi, & \text{ если } I(\Phi) = \text{И}, \\ \mathcal{A}_{\tau^+} \not\models \Phi, & \text{ если } I(\Phi) = \text{Л}. \end{aligned}$$

(i) Если Φ – атомная формула вида $p(t_1, \dots, t_n)$, где p – n -местный предикатный символ сигнатуры τ^+ , а t_1, \dots, t_n – свободные от переменных термы сигнатуры $\tau^+(A)$, то полагаем

$$\mathcal{A}_{\tau^+} \models \Phi \iff p^{A_{\tau^+}}(\mathcal{A}_{\tau^+}(t_1), \dots, \mathcal{A}_{\tau^+}(t_n)) = \text{И},$$

т. е.

$$\mathcal{A}_{\tau^+} \models \Phi \iff \bar{\Gamma} \models_{fin} p(t_1, \dots, t_n).$$

(ii) Теперь если Φ и Ψ – замкнутые формулы, то полагаем

$$\begin{aligned} \mathcal{A}_{\tau^+} \models (\neg \Phi) & \iff \mathcal{A}_{\tau^+} \not\models \Phi, \\ \mathcal{A}_{\tau^+} \models (\Phi \vee \Psi) & \iff \mathcal{A}_{\tau^+} \models \Phi \text{ или } \mathcal{A}_{\tau^+} \models \Psi, \\ \mathcal{A}_{\tau^+} \models (\Phi \& \Psi) & \iff \mathcal{A}_{\tau^+} \models \Phi \text{ и } \mathcal{A}_{\tau^+} \models \Psi, \\ \mathcal{A}_{\tau^+} \models (\Phi \rightarrow \Psi) & \iff \mathcal{A}_{\tau^+} \models \Phi \text{ и } \mathcal{A}_{\tau^+} \models \Psi. \end{aligned}$$

(iii) Если Φ – формула, не содержащая свободных переменных, отличных от x , то полагаем

$$\begin{aligned} \mathcal{A}_{\tau^+} \models (\exists x)\Phi &\iff \\ \mathcal{A}_{\tau^+} \models \Phi_x[t] &\text{ для имени } t \text{ некоторого индивида } t \text{ из } A, \text{ т. е. терма } t, \end{aligned}$$

$$\begin{aligned} \mathcal{A}_{\tau^+} \models (\forall x)\Phi &\iff \\ \mathcal{A}_{\tau^+} \models \Phi_x[t] &\text{ для имени } t \text{ любого индивида } t \text{ из } A, \text{ т. е. терма } t. \end{aligned}$$

Напомним, что $\bar{\Gamma}$ – **локально полное множество формул**, поэтому для любой замкнутой формулы Φ

$$\bar{\Gamma} \models_{fin} \Phi \quad \text{или} \quad \bar{\Gamma} \models_{fin} \neg\Phi,$$

но не то и другое одновременно, в частности, это верно и для произвольной атомной формулы вида $p(t_1, \dots, t_n)$, где p – n -местный предикатный символ сигнатуры τ^+ . Поэтому интерпретация I определена корректно.

Индукцией по построению формул (либо по их длине, либо по числу входящих в них логических связок и кванторов) докажем, что для произвольной формулы Φ имеет место эквивалентность:

$$\bar{\Gamma} \models_{fin} \Phi \iff I(\Phi) = \text{И}.$$

(i) Для элементарных формул Φ указанная эквивалентность имеет место по определению интерпретации I .

(ii) Предположим, что указанная эквивалентность имеет место для формул Φ и Ψ и докажем, что тогда она выполняется и для формул

$$(\neg\Phi), \quad (\Phi \& \Psi), \quad (\Phi \vee \Psi), \quad (\Phi \rightarrow \Psi), \quad (\forall x)\Phi, \quad (\exists x)\Phi.$$

Так как

$$\bar{\Gamma} \models_{fin} (\neg\Phi) \iff \bar{\Gamma} \not\models_{fin} \Phi$$

и

$$I(\Phi) = \text{Л} \iff I(\neg\Phi) = \text{И},$$

то

$$\bar{\Gamma} \models_{fin} (\neg\Phi) \iff I((\neg\Phi)) = \text{И}.$$

Нетрудно показать, что

$$\bar{\Gamma} \models_{fin} (\Phi \& \Psi) \iff \bar{\Gamma} \models_{fin} \Phi \text{ и } \bar{\Gamma} \models_{fin} \Psi.$$

Кроме того, по определению интерпретации I

$$I(\Phi) = \text{И} \text{ и } I(\Psi) = \text{И} \iff I((\Phi \& \Psi)) = \text{И}.$$

Значит,

$$\bar{\Gamma} \models_{fin} (\Phi \& \Psi) \iff I((\Phi \& \Psi)) = \text{И}.$$

Покажем, что для **локально полного** множества формул $\bar{\Gamma}$ и произвольных формул Φ и Ψ имеет место эквивалентность

$$\bar{\Gamma} \models_{fin} (\Phi \vee \Psi) \iff \bar{\Gamma} \models_{fin} \Phi \text{ или } \bar{\Gamma} \models_{fin} \Psi$$

В самом деле, если

$$\bar{\Gamma} \models_{fin} \Phi \text{ или } \bar{\Gamma} \models_{fin} \Psi,$$

то, конечно,

$$\bar{\Gamma} \models_{fin} (\Phi \vee \Psi).$$

Обратно, предположим, что

$$\bar{\Gamma} \models_{fin} (\Phi \vee \Psi).$$

Покажем, что тогда

$$\bar{\Gamma} \models_{fin} \Phi \text{ или } \bar{\Gamma} \models_{fin} \Psi.$$

Предположим противное, т. е. что

$$\bar{\Gamma} \not\models_{fin} \Phi \text{ и } \bar{\Gamma} \not\models_{fin} \Psi.$$

Так как $\bar{\Gamma}$ – **локально полное** множество формул, то тогда

$$\bar{\Gamma} \models_{fin} (\neg\Phi) \text{ и } \bar{\Gamma} \models_{fin} (\neg\Psi),$$

а, значит,

$$\bar{\Gamma} \models_{fin} ((\neg\Phi) \& (\neg\Psi)),$$

поэтому

$$\bar{\Gamma} \models_{fin} \neg(\Phi \vee \Psi).$$

Так как выше мы предположили, что

$$\bar{\Gamma} \models_{fin} (\Phi \vee \Psi),$$

то получаем противоречие с предположением о **локальной совместности** множества формул $\bar{\Gamma}$.

В итоге получаем

$$\bar{\Gamma} \models_{fin} (\Phi \vee \Psi) \iff \bar{\Gamma} \models_{fin} \Phi \text{ или } \bar{\Gamma} \models_{fin} \Psi$$

и

$$I(\Phi) = \text{И} \text{ или } I(\Psi) = \text{И} \iff I((\Phi \vee \Psi)) = \text{И},$$

поэтому

$$\bar{\Gamma} \models_{fin} (\Phi \vee \Psi) \iff I((\Phi \vee \Psi)) = И.$$

Доказательство эквивалентности

$$\bar{\Gamma} \models_{fin} (\Phi \rightarrow \Psi) \iff I(\Phi \rightarrow \Psi) = И$$

проводится по той же схеме с использованием локальной полноты и локальной совместности множества формул $\bar{\Gamma}$.

Остается рассмотреть формулы вида $(\exists x)\Phi$ и $(\forall x)\Phi$. Именно при их рассмотрении нам понадобится свойство Генкина.

Если Φ – формула, не содержащая свободных переменных, отличных от x , то по определению

$$\begin{aligned} \mathcal{A}_{\tau^+} \models (\exists x)\Phi &\iff \\ \mathcal{A}_{\tau^+} \models \Phi_x[t] &\text{ для имени } t \text{ некоторого индивида } t \text{ из } A, \text{ т. е. терма } t. \end{aligned}$$

Покажем, что имеет место эквивалентность:

$$\bar{\Gamma} \models_{fin} (\exists x)\Phi \iff I((\exists x)\Phi) = И.$$

Если

$$\bar{\Gamma} \models_{fin} (\exists x)\Phi,$$

то в силу свойства Генкина найдется такой замкнутый терм t (даже константа c), что

$$((\exists x)\Phi \rightarrow \Phi_x[t]) \in \Gamma^+ \subseteq \bar{\Gamma},$$

значит,

$$\bar{\Gamma} \models_{fin} ((\exists x)\Phi \rightarrow \Phi_x[t]),$$

поэтому

$$\bar{\Gamma} \models_{fin} \Phi_x[t].$$

По индуктивному предположению тогда $I(\Phi_x[t]) = И$, поэтому и

$$I((\exists x)\Phi) = И.$$

Если же $I((\exists x)\Phi) = И$, то найдется такой замкнутый терм t , что $I(\Phi_x[t]) = И$. По индуктивному предположению тогда

$$\bar{\Gamma} \models_{fin} \Phi_x[t].$$

Так как

$$\bar{\Gamma} \models_{fin} (\Phi_x[t] \rightarrow (\exists x)\Phi),$$

то

$$\bar{\Gamma} \models_{fin} (\exists x)\Phi.$$

Тем самым доказано, что

$$\bar{\Gamma} \models_{fin} (\exists x)\Phi \iff I((\exists x)\Phi) = \text{И}.$$

По той же схеме доказывается, что

$$\bar{\Gamma} \models_{fin} (\forall x)\Phi \iff I((\forall x)\Phi) = \text{И}.$$

В итоге доказано, что для произвольной формулы Φ имеет место эквивалентность:

$$\bar{\Gamma} \models_{fin} \Phi \iff I(\Phi) = \text{И}.$$

Если Φ – произвольная формула из множества $\bar{\Gamma}$, то, очевидно, $\bar{\Gamma} \models_{fin} \Phi$, поэтому $I(\Phi) = \text{И}$.

Значит, $I(\bar{\Gamma}) = \text{И}$, поэтому множество формул $\bar{\Gamma}$ является **совместным**, а значит, **совместным** является и исходное множество формул Γ . \square

Второй вариант доказательства будет основан на понятии фильтрованного произведения.

Напомним основные определения, относящиеся к понятию **фильтрованного произведения алгебраических систем**.

Для произвольного множества I множество $P(I)$ всех его подмножеств является булевой алгеброй относительно операций \cup и \cap . Фильтры в булевой алгебре $P(I)$ называются фильтрами над множеством I .

Определение 3.6.9. *Фильтром над множеством I называется произвольная непустая система подмножеств D множества I , удовлетворяющая следующим условиям:*

- 1) если $X \in D$ и $Y \in D$, то $X \cap Y \in D$,
- 2) если $X \in D$ и $X \subseteq Y$, то $Y \in D$,
- 3) $\emptyset \notin D$.

Из пунктов 1) и 2) легко получить эквивалентность: для любых подмножеств X и Y множества I : $X \in D$ и $Y \in D$ тогда и только тогда, когда $X \cap Y \in D$.

Если $X \in D$ или $Y \in D$, то $X \cup Y \in D$. Фильтр, для которого верно обратное утверждение, называется **простым**.

Определение 3.6.10. *Фильтр над множеством I называется **простым**, если для любых подмножеств X и Y множества I из того, что $X \in D$ или $Y \in D$, следует, что $X \cup Y \in D$.*

Для простого фильтра D имеет место эквивалентность: для любых подмножеств X и Y множества I $X \in D$ или $Y \in D$ тогда и только тогда, когда $X \cup Y \in D$.

Определение 3.6.11. *Фильтр над множеством I называется **максимальным**, если он не содержится ни в каком отличном от него фильтре.*

Определение 3.6.12. *Фильтр над множеством I называется **ультрафильтром**, если для любого подмножества X множества I либо $X \in D$, либо $(I \setminus X) \in D$.*

Используя аксиому выбора, было доказано, что понятия простого, максимального и ультрафильтра эквивалентны между собой. Кроме того было доказано, что любой фильтр содержится в максимальном фильтре.

Рассмотрим семейство $(\mathcal{A}_i)_{i \in I}$ алгебраических систем сигнатуры τ с основными множествами A_i ($i \in I$). Чтобы несколько упростить обозначения, алгебраическую операцию $f^{\mathcal{A}_i}$, предикат $p^{\mathcal{A}_i}$ и элемент $c^{\mathcal{A}_i}$, соответствующие в алгебраической системе \mathcal{A}_i соответственно функциональному символу f , предикатному символу p и константе c сигнатуры τ , будем обозначать коротко через f , p и c соответственно. Это не приведет к недоразумениям.

Напомним понятие *прямого произведения* семейства алгебраических систем $(\mathcal{A}_i)_{i \in I}$, обобщающее хорошо известные из курса "Алгебра" понятия прямого произведения семейства групп или колец. Прямое произведение семейства алгебраических систем $(\mathcal{A}_i)_{i \in I}$ обозначается через $\prod_{i \in I} \mathcal{A}_i$. Основным множеством системы $\prod_{i \in I} \mathcal{A}_i$ служит прямое произведение $\prod_{i \in I} A_i$ основных множеств A_i систем \mathcal{A}_i . Напомним, что элементами множества $\prod_{i \in I} A_i$ являются всевозможные функции g из множества I во множество $\bigcup_{i \in I} A_i$ такие, что при любом i из I : $g(i) \in A_i$.

Каждому n -местному функциональному символу f сопоставляется n -местная алгебраическая операция, определенная на множестве $\prod_{i \in I} A_i$, которая будет обозначаться через f , что не приведет к недоразумению. Для произвольных элементов g_1, g_2, \dots, g_n и любого i из I полагаем

$$f(g_1, g_2, \dots, g_n)(i) = f(g_1(i), g_2(i), \dots, g_n(i)).$$

Каждому n -местному предикатному символу p сопоставляется n -местный предикат, определенный на множестве $\prod_{i \in I} A_i$, который будет обозначаться через p , что не приведет к недоразумению. Для произвольных элементов g_1, g_2, \dots, g_n полагаем

$$p(g_1, g_2, \dots, g_n) = \text{И} \iff \text{при любом } i : p(g_1(i), g_2(i), \dots, g_n(i)) = \text{И}.$$

Каждому константному символу c сопоставляется элемент из множества $\prod_{i \in I} A_i$, который обозначается через c , что не приведет к недоразумению. Для произвольного i из I полагаем

$$c(i) = c.$$

Прямое произведение $\prod_{i \in I} \mathcal{A}_i$ семейства алгебраических систем $(\mathcal{A}_i)_{i \in I}$ одной и той же сигнатуры τ с точки зрения математической логики особого интереса

не представляет. Большой интерес представляет *фильтрованное произведение* семейства алгебраических систем $(\mathcal{A}_i)_{i \in I}$ по произвольному фильтру D , которое будет обозначаться через $\prod_{i \in I} \mathcal{A}_i / D$

Напомним определение этого понятия.

Пусть $(\mathcal{A}_i)_{i \in I}$ – семейство алгебраических систем сигнатуры τ с основными множествами A_i ($i \in I$), а D – фильтр на множестве индексов I . На прямом произведении $\prod_{i \in I} A_i$ основных множеств A_i систем \mathcal{A}_i введем отношение эквивалентности \equiv_D . Пусть g и h – элементы из $\prod_{i \in I} A_i$. Полагаем

$$g \equiv_D h \iff \{i \mid g(i) = h(i)\} \in D.$$

Рефлексивность и симметричность отношения \equiv_D очевидны, а его транзитивность следует из включения

$$\{i \mid g(i) = h(i)\} \cap \{i \mid h(i) = t(i)\} \subseteq \{i \mid g(i) = t(i)\}.$$

Обозначим через $[g]$ класс эквивалентности с представителем g , т. е.

$$[g] = \{h \mid g \equiv_D h\}.$$

Множество классов эквивалентности, называемое фактормножеством множества $\prod_{i \in I} A_i$ по отношению эквивалентности \equiv_D , обозначается через $\prod_{i \in I} A_i / \equiv_D$. *Наделим множество $\prod_{i \in I} A_i / \equiv_D$ структурой алгебраической системы сигнатуры τ .*

Каждому n -местному функциональному символу f сигнатуры τ сопоставим n -местную алгебраическую операцию, определенную на множестве $\prod_{i \in I} A_i / \equiv_D$, которую будем обозначать через f , что не приведет к недоразумению. Для произвольных элементов $[g_1], [g_2], \dots, [g_n]$ из $\prod_{i \in I} A_i / \equiv_D$ полагаем

$$f([g_1], [g_2], \dots, [g_n]) = [f(g_1, g_2, \dots, g_n)].$$

Независимость определения от выбора представителей в классах эквивалентности $[g_1], [g_2], \dots, [g_n]$ следует из включения

$$\begin{aligned} \{i \mid g_1(i) = h_1(i)\} \cap \{i \mid g_2(i) = h_2(i)\} \cap \dots \cap \{i \mid g_n(i) = h_n(i)\} \subseteq \\ \subseteq \{i \mid f(g_1(i), g_2(i), \dots, g_n(i)) = f(h_1(i), h_2(i), \dots, h_n(i))\}. \end{aligned}$$

Каждому n -местному предикатному символу p сопоставим n -местный предикат, определенный на множестве $\prod_{i \in I} A_i / \equiv_D$, который будем обозначать через p , что не приведет к недоразумению. Для произвольных элементов $[g_1], [g_2], \dots, [g_n]$ из $\prod_{i \in I} A_i / \equiv_D$ полагаем

$$p([g_1], [g_2], \dots, [g_n]) = \text{И} \iff \{i \mid p(g_1(i), g_2(i), \dots, g_n(i)) = \text{И}\} \in D.$$

Независимость определения от выбора представителей в классах эквивалентности $[g_1], [g_2], \dots, [g_n]$ следует из включения

$$\{i | g_1(i) = h_1(i)\} \cap \{i | g_2(i) = h_2(i)\} \cap \dots \cap \{i | g_n(i) = h_n(i)\} \cap \\ \cap \{i | p(g_1(i), g_2(i), \dots, g_n(i)) = \text{И}\} \subseteq \{i | p(h_1(i), h_2(i), \dots, h_n(i)) = \text{И}\}.$$

Если $=$ – выделенный 2-местный предикатный символ, то для произвольных элементов $[g_1]$ и $[g_2]$ из $\prod_{i \in I} A_i / \equiv_D$ получаем

$$([g_1], [g_2]) = \text{И} \iff \{i | (g_1(i), g_2(i)) = \text{И}\} \in D.$$

Т.е. выделенный 2-местный предикатный символ $=$ интерпретируется как обычное равенство, поэтому мы получаем **нормальную интерпретацию**.

Каждому константному символу c сигнатуры τ сопоставим элемент $[c]$ из множества $\prod_{i \in I} A_i / \equiv_D$, который будем обозначать через c , что не приведет к недоразумению. Напомним, что в квадратных скобках стоит функция, определенная для произвольного i из I равенством

$$c(i) = c.$$

Построенная алгебраическая система сигнатуры τ обозначается через

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

и называется *фильтрованным произведением семейства алгебраических систем $(\mathcal{A}_i)_{i \in I}$ сигнатуры τ по фильтру D* .

Пусть все свободные переменные формулы Φ содержатся в списке x_1, x_2, \dots, x_n . Ранее была доказана следующая теорема Лося.

Теорема 3.6.3 (Лось). Пусть $(\mathcal{A}_i)_{i \in I}$ – семейство алгебраических систем сигнатуры τ , D – ультрафильтр на множестве индексов I , а $\prod_{i \in I} A_i / \equiv_D$ – соответствующее фильтрованное произведение. Тогда для любых элементов $[g_1], [g_2], \dots, [g_n]$ из основного множества $\prod_{i \in I} A_i / \equiv_D$ системы $\prod_{i \in I} \mathcal{A}_i / \equiv_D$ имеет место следующая эквивалентность

$$\prod_{i \in I} \mathcal{A}_i / \equiv_D \models \Phi_{x_1, x_2, \dots, x_n}[[g_1], [g_2], \dots, [g_n]] \iff \\ \iff \{i | \mathcal{A}_i \models \Phi_{x_1, x_2, \dots, x_n}[g_1(i), g_2(i), \dots, g_n(i)]\} \in D.$$

Рассмотрим второй вариант доказательства **локальной теоремы К. Геделя – А.И. Мальцева** для логики предикатов первого порядка с равенством.

Пусть множество замкнутых формул Γ языка L_τ является **локально совместным**, т. е. каждое его конечное совместно. Покажем, что **совместно** и все множество формул Γ .

Обозначим через I семейство всех конечных подмножеств множества формул Γ . Для каждого i из множества I пусть Φ_i – это конъюнкция всех формул из i , а \mathcal{A}_i – алгебраическая система, в которой истинны все формулы из i , а значит, и формула Φ_i .

Для произвольного t из I полагаем

$$I_t = \{i \mid i \in I \text{ \& } \mathcal{A}_i \models \Phi_t\}.$$

Докажем, что семейство $(I_t)_{t \in I}$ подмножеств множества I обладает следующим свойством:

]it пересечение любого конечного числа множеств этого семейства непусто.

В самом деле пусть $I_{t_1}, I_{t_2}, \dots, I_{t_n}$ – элементы семейства, а $\Phi_{t_1}, \Phi_{t_2}, \dots, \Phi_{t_n}$ – соответствующие формулы. Обозначим через Φ конъюнкцию формул $\Phi_{t_1}, \Phi_{t_2}, \dots, \Phi_{t_n}$. По условию формула Φ выполнима. Пусть \mathcal{A}_{i_0} – соответствующая алгебраическая система. Тогда $i_0 \in I_{t_1} \cap I_{t_2} \cap \dots \cap I_{t_n}$.

В таком случае, как доказано в **Дополнении**, существует ультрафильтр D , содержащий все множества семейства $(I_t)_{t \in I}$.

Рассмотрим ультрапроизведение

$$\prod_{i \in I} \mathcal{A}_i / \equiv_D.$$

Покажем, что все формулы из множества Γ истинны на этой системе.

В самом деле, если Φ_t – произвольная формула из множества Γ , то

$$\{i \mid i \in I \text{ \& } \mathcal{A}_i \models \Phi_t\} = I_t \in D.$$

Поэтому

$$\prod_{i \in I} \mathcal{A}_i / \equiv_D \models \Phi_t.$$

Из доказанной теоремы легко получается следующая, на первый взгляд, более общая теорема, которая на самом деле эквивалентна доказанной теореме.

Теорема 3.6.4. Для любого множества формул Γ языка L_τ первого порядка с равенством и любой замкнутой формулы этого языка Φ имеет место эквивалентность:

$$\Gamma \models_{fin} \Phi \iff \Gamma \models \Phi.$$

Д о к а з а т е л ь с т в о. Если $\Gamma \models_{fin} \Phi$, то, конечно, $\Gamma \models \Phi$. Пусть $\Gamma \models \Phi$. Покажем, что тогда $\Gamma \models_{fin} \Phi$. Допустим противное, тогда для любого конечного подмножества Γ_0 множества Γ совместно множество $\Gamma_0 \cup \{(\neg\Phi)\}$, поэтому множество $\Gamma \cup \{(\neg\Phi)\}$ **локально совместно**. В силу предыдущей теоремы множество $\Gamma \cup \{(\neg\Phi)\}$ **совместно**, но это противоречит предположению $\Gamma \models \Phi$. \square

3.7. Исчисление предикатов с равенством

В этом параграфе рассматриваются некоторые вопросы для **Исчисления предикатов с равенством** произвольной сигнатуры

$$\tau = \langle C, F, P, \theta, \varphi \rangle.$$

Напомним, что это означает, что во множестве P предикатных символов выделен 2-местный предикатный символ, обозначаемый через $=$.

Язык L_τ **Исчисления предикатов с равенством** произвольной сигнатуры τ совпадает с языком L_τ **Логике предикатов с равенством** этой сигнатуры τ . Это означает, что совпадают алфавиты этих языков, понятия **терма** и **формулы**.

Как и в случае **Логике предикатов с равенством** формулу $=(t_1, t_2)$ будем записывать в более привычном виде $t_1 = t_2$.

Для **Логике предикатов с равенством** основными понятиями были понятие **нормальной интерпретации** и понятие **истинностное значение** $I(\Phi)$ замкнутой формулы Φ в нормальной интерпретации I .

Основными понятиями **Исчисления предикатов с равенством**, как и в случае **Исчисления предикатов** произвольной сигнатуры, будут понятия **Вывод** и **Выводимая формула**. Эти понятия определяются для **Исчисления предикатов с равенством** по той же схеме, что и для **Исчисления предикатов** произвольной сигнатуры.

3.7.1. Логические аксиомы и правила вывода

Аксиомы Исчисления предикатов с равенством

Зафиксируем произвольную сигнатуру τ с равенством. Все последующие определения будут относиться к **Исчислению предикатов с равенством** **ИПР** $_\tau$ этой сигнатуры τ , которое ради некоторой краткости будем называть просто **Исчислением предикатов с равенством** и обозначать через **ИПР** (без упоминания сигнатуры τ).

Для произвольных формул A, B и C **Исчисления предикатов с равенством** формула любого указанного ниже вида является **Логической аксиомой Исчисления предикатов с равенством**.

I_\rightarrow .

I.1. $(A \rightarrow (B \rightarrow A))$.

I.2. $((A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C)))$.

$\Pi_\&$.

II.1. $((A \& B) \rightarrow A)$.

II.2. $((A \& B) \rightarrow B)$.

II.3. $((A \rightarrow B) \rightarrow ((A \rightarrow C) \rightarrow (A \rightarrow (B \& C))))$.

III_∨.

III.1. $(\mathcal{A} \rightarrow (\mathcal{A} \vee \mathcal{B}))$.

III.2. $(\mathcal{B} \rightarrow (\mathcal{A} \vee \mathcal{B}))$.

III.3. $((\mathcal{A} \rightarrow \mathcal{C}) \rightarrow ((\mathcal{B} \rightarrow \mathcal{C}) \rightarrow ((\mathcal{A} \vee \mathcal{B}) \rightarrow \mathcal{C})))$.

IV_¬.

IV.1. $((\mathcal{A} \rightarrow (\neg \mathcal{B})) \rightarrow (\mathcal{B} \rightarrow (\neg \mathcal{A})))$.

IV.2. $((\neg(\neg \mathcal{A})) \rightarrow \mathcal{A})$.

Для произвольной формулы \mathcal{A} **Исчисления предикатов с равенством** и любого терма t *допустимого для подстановки* в формулу \mathcal{A} вместо свободных вхождений переменной x формула любого указанного ниже вида является **Логической аксиомой Исчисления предикатов с равенством**

V_∀.

V.1. $((\forall x)\mathcal{A} \rightarrow \mathcal{A}_x[t])$.

VI_∃.

VI.1. $(\mathcal{A}_x[t] \rightarrow (\exists x)\mathcal{A})$.

Каждая из следующих трех формул **Исчисления предикатов с равенством** является **Логической аксиомой Исчисления предикатов с равенством**.

VII₌.

VII.1. $(\forall x_1)x_1 = x_1$.

VII.2. $(\forall x_1)(\forall x_2)(x_1 = x_2 \rightarrow x_2 = x_1)$.

VII.3. $(\forall x_1)(\forall x_2)(\forall x_3)((x_1 = x_2 \& x_2 = x_3) \rightarrow x_1 = x_3)$.

Для произвольного n -местного функционального символа f и произвольного n -местного предикатного символа p каждая из следующих двух формул **Исчисления предикатов с равенством** является **Логической аксиомой Исчисления предикатов с равенством**.

VIII₌.

VIII.1.

$$(\forall x_1)(\forall x_2) \dots (\forall x_n)(\forall y_1)(\forall y_2) \dots (\forall y_n)((\dots(x_1 = y_1 \& x_2 = y_2) \& \dots) \& x_n = y_n) \rightarrow f(x_1, x_2, \dots, x_n) = f(y_1, y_2, \dots, y_n).$$

VIII.2.

$$(\forall x_1)(\forall x_2) \dots (\forall x_n)(\forall y_1)(\forall y_2) \dots (\forall y_n)((\dots(x_1 = y_1 \& x_2 = y_2) \& \dots) \& x_n = y_n) \rightarrow p(x_1, x_2, \dots, x_n) \longleftrightarrow p(y_1, y_2, \dots, y_n).$$

Правила вывода Исчисления предикатов с равенством

В *Исчислении Предикатов с равенством*, как и в рассматривавшемся выше *Исчислении Предикатов*, используются три **Правила вывода** – **Правило отделения** (*Modus Ponens*), **Правило Введения** \forall и **Правило Введения** \exists .

Правило Отделения (кратко это правило будем обозначать через *MP*):

$$\frac{\mathcal{A}, (\mathcal{A} \rightarrow \mathcal{B})}{\mathcal{B}}.$$

Эта запись означает, что по правилу *MP* из формул \mathcal{A} и $(\mathcal{A} \rightarrow \mathcal{B})$ получается формула \mathcal{B} . При этом формулы \mathcal{A} и $(\mathcal{A} \rightarrow \mathcal{B})$ называются **посылками** правила *MP*, а формула \mathcal{B} – его **заключением** или **непосредственным следствием** формул \mathcal{A} и $(\mathcal{A} \rightarrow \mathcal{B})$ по правилу *MP*.

Правило Введения \forall :

$$\frac{(\mathcal{B} \rightarrow \mathcal{A})}{(\mathcal{B} \rightarrow (\forall x)\mathcal{A})}.$$

при условии, что переменная x не входит свободно в формулу \mathcal{B} .

Эта запись означает, что по **Правилу Введения** \forall из формулы $(\mathcal{B} \rightarrow \mathcal{A})$ получается формула $(\mathcal{B} \rightarrow (\forall x)\mathcal{A})$. При этом формула $(\mathcal{B} \rightarrow \mathcal{A})$ называется **посылкой** **Правила Введения** \forall , а формула $(\mathcal{B} \rightarrow (\forall x)\mathcal{A})$ – его **заключением** или **непосредственным следствием** формулы $(\mathcal{B} \rightarrow \mathcal{A})$ по этому правилу.

Правило Введения \exists :

$$\frac{(\mathcal{A} \rightarrow \mathcal{B})}{((\exists x)\mathcal{A} \rightarrow \mathcal{B})}.$$

при условии, что переменная x не входит свободно в формулу \mathcal{B} .

Эта запись означает, что по **Правилу Введения** \exists из формулы $(\mathcal{A} \rightarrow \mathcal{B})$ получается формула $((\exists x)\mathcal{A} \rightarrow \mathcal{B})$. При этом формула $(\mathcal{A} \rightarrow \mathcal{B})$ называется **посылкой** **Правила Введения** \exists , а формула $((\exists x)\mathcal{A} \rightarrow \mathcal{B})$ – его **заключением** или **непосредственным следствием** формулы $(\mathcal{A} \rightarrow \mathcal{B})$ по этому правилу.

Вывод и Вывод из множества формул в Исчислении Предикатов с равенством

Определение понятий **Вывод** и **Вывод из множества формул в Исчислении Предикатов с равенством** практически ничем не отличается от определения понятий **Вывод** и **вывод из множества формул в Исчислении Предикатов**.

Определение 3.7.1. *Выводом в Исчислении Предикатов с равенством называется любая конечная последовательность*

$$\mathcal{B}_1, \dots, \mathcal{B}_n$$

формул *Исчисления Предикатов с равенством*, удовлетворяющая следующему условию:

для любого i ($i = 1, \dots, n$)

либо

1) формула B_i является **Логической аксиомой Ичисления Предикатов с равенством**,

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**,

либо

3) найдется число j меньшее, чем i , такое, что формула B_i получается из формулы B_j по правилу **Введения \forall** ,

либо

4) найдется число j меньшее, чем i , такое, что формула B_i получается из формулы B_j по правилу **Введения \exists** .

Определение 3.7.2. Формула B называется **выводимой в Ичислении Предикатов с равенством**, если существует **Вывод в Ичислении Предикатов с равенством**

$$B_1, \dots, B_n,$$

оканчивающийся этой формулой B .

Выражение $\vdash_{ИПР} A$ служит сокращенной записью утверждения

”формула A выводима в Ичислении Предикатов с равенством”.

В дальнейшем для сокращения индекс **ИПР** будем опускать, т. е. вместо $\vdash_{ИПР} A$ будем писать просто $\vdash A$.

Заметим, что для формул языка L_τ сигнатуры τ определены два понятия

формула Φ выводима в Ичислении Предикатов с равенством (сокращенное обозначение $\vdash_{ИПР} A$) и **формула Φ выводима в Ичислении Предикатов** (сокращенное обозначение $\vdash_{ИП} A$).

Так как все формулы языка L_τ сигнатуры τ , являющиеся **логическими аксиомами Ичисления Предикатов** являются **логическими аксиомами Ичисления Предикатов с равенством**, то, если **формула Φ выводима в Ичислении предикатов**, то **формула Φ выводима в Ичислении предикатов с равенством**, т. е. из $\vdash_{ИП} A$ следует $\vdash_{ИПР} A$.

Как и в случае **Ичисления Предикатов**, введем более общее понятие, чем понятие **Вывод в Ичислении Предикатов с равенством**, – понятие **Вывод из множества гипотез в Ичислении Предикатов с равенством**.

Пусть Γ – произвольное множество формул. Формулы из множества Γ будем называть **гипотезами или нелогическими аксиомами**.

Определение 3.7.3. *Выводом из множества формул Γ в Исчислении Предикатов с равенством* называется любая конечная последовательность

$$B_1, \dots, B_n$$

формул **Исчисления Предикатов с равенством**, удовлетворяющая следующему условию:

для любого i ($i = 1, \dots, n$)

либо

0) $B_i \in \Gamma$ (формула B_i является гипотезой или нелогической аксиомой),

либо

1) формула B_i является **Логической аксиомой Исчисления Предикатов с равенством**,

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**,

либо

3) найдется число j меньшее, чем i , такое, что формула B_i получается из формулы B_j по правилу **Введения \forall** ,

либо

4) найдется число j меньшее, чем i , такое, что формула B_i получается из формулы B_j по правилу **Введения \exists** .

Определение 3.7.4. Формула B называется выводимой в Исчислении Предикатов с равенством из множества формул Γ , если существует вывод в Исчислении предикатов с равенством из множества формул Γ

$$B_1, \dots, B_n,$$

оканчивающийся формулой B .

Выражение $\Gamma \vdash_{ИПР} A$ служит сокращенной записью утверждения

"формула A выводима в Исчислении Предикатов с равенством из множества формул Γ ".

Ясно, что если "формула A выводима в Исчислении предикатов из множества формул Γ ", то эта "формула A выводима в Исчислении Предикатов с равенством из множества формул Γ ". Т. е. из $\Gamma \vdash_{ИП} A$ следует $\Gamma \vdash_{ИПР} A$.

Между понятиями **выводимость из множества гипотез в Исчислении Предикатов с равенством** и **выводимость из множества гипотез в Исчислении Предикатов** существует тесная связь.

Обозначим через $AxEq$ множество всех формул языка L_{τ} , являющихся **логическими аксиомами Исчисления Предикатов с равенством** из группы VIII₌.

Тогда для произвольного множества Γ формул языка L_τ и любой формулы A этого языка справедлива эквивалентность:

формула A выводима в Исчислении Предикатов с равенством из множества гипотез Γ тогда и только тогда, когда формула A выводима в Исчислении Предикатов из множества гипотез $\Gamma \cup AxEq$.

Т. е.

$$\Gamma \vdash_{ИПР} A \iff \Gamma \cup AxEq \vdash_{ИП} A.$$

Используя эту эквивалентность, из доказанной ранее **Теоремы дедукции для Исчисления Предикатов** легко получить доказательство **Теоремы дедукции для Исчисления Предикатов с равенством**.

Теорема Дедукции. *Если $\Gamma, A \vdash_{ИПР} B$ и существует вывод D формулы B из множества формул $\Gamma \cup \{A\}$, в котором **Правило введения \forall** и **Правило введения \exists** не применяются по переменным, входящим свободно в формулу A , то $\Gamma \vdash_{ИПР} (A \rightarrow B)$.*

Обратно, если $\Gamma \vdash_{ИПР} (A \rightarrow B)$, то $\Gamma, A \vdash_{ИПР} B$.

3.7.2. Теорема адекватности для исчисления предикатов с равенством

Напомним, что формула Φ языка L первого порядка с равенством называется **логическим следствием** множества формул Γ , если Φ истинна в каждой нормальной модели для Γ , т. е. для любой нормальной интерпретации I языка L из того, что все формулы множества Γ истинны в нормальной интерпретации I следует, что в I истинна и формула Φ .

Основная цель этого параграфа – доказать следующую **Теорему Адекватности для Исчисления Предикатов с равенством**.

Теорема 3.7.1. *Для любой формулы A языка $L_{ИПР}$ Исчисления Предикатов с равенством и для любого множества формул Γ этого языка имеет место следующая эквивалентность:*

формула A является логическим следствием множества формул Γ в Логике Предикатов с равенством тогда и только тогда, когда формула A выводима из этого множества формул Γ в Исчислении Предикатов с равенством.

Как следствие мы получим **Теорему К. Геделя о полноте** для **Исчисления Предикатов с равенством**.

Теорема 3.7.2. *Для любой формулы A языка $L_{ИПР}$ Исчисления Предикатов с равенством имеет место следующая эквивалентность:*

A является тождественно истинной формулой Логики Предикатов с равенством тогда и только тогда, когда она выводима в Исчислении Предикатов с равенством.

Доказательство *Теоремы адекватности для Исчисления Предикатов с равенством* мы получим как следствие доказанной выше *Теоремы адекватности для Исчисления Предикатов*, точнее, эквивалентной ей *Теоремы непротиворечивости для Исчисления Предикатов*.

Покажем, что, как и в рассмотренном выше случае *Исчисления Предикатов*, *Теорема адекватности для Исчисления Предикатов с равенством* эквивалентна следующей *Теореме непротиворечивости для Исчисления Предикатов с равенством*.

Теорема 3.7.3. *Множество формул Δ языка $L_{ИПР}$ Исчисления Предикатов с равенством непротиворечиво тогда и только тогда, когда оно совместно.*

Предварительно докажем две леммы.

Лемма. *Если формула A языка $L_{ИПР}$ Исчисления Предикатов с равенством выводима в Исчислении Предикатов с равенством из множества формул Γ этого языка, то формула A является логическим следствием множества формул Γ в Логике Предикатов с равенством.*

Доказательство. Доказательство этой леммы легко провести индукцией по длине вывода, проверив предварительно истинность в любой нормальной интерпретации всех аксиом *Исчисления Предикатов с равенством*. \square

Лемма. *Если Δ – совместное множество формул языка $L_{ИПР}$, то Δ – непротиворечивое множество формул языка $L_{ИПР}$ Исчисления Предикатов с равенством.*

Доказательство. Пусть Δ – совместное множество формул и φ – нормальная интерпретация, в которой истинны все формулы из Δ .

Если бы множество формул Δ было противоречивым, то для некоторой замкнутой формулы A из Δ была бы выводима в *Исчислении Предикатов с равенством* как сама формула A , так и ее отрицание $(\neg A)$.

Тогда по предыдущей лемме обе эти формулы были бы логическим следствием множества формул Δ , а, значит, формула A и ее отрицание $(\neg A)$ были бы истинны в нормальной интерпретации φ , что невозможно. Значит, множество формул Δ непротиворечиво. \square

Приступаем к доказательству эквивалентности *Теоремы адекватности для Исчисления Предикатов с равенством* и *Теореме непротиворечивости для Исчисления Предикатов*.

Покажем, что *Теорема адекватности для Исчисления Предикатов с равенством* влечет *Теорему непротиворечивости для Исчисления Предикатов*.

Предположим, что *Теорема адекватности для Исчисления Предикатов с равенством* справедлива.

Докажем при этом предположении **Теорему непротиворечивости для Исчисления Предикатов**.

Если Δ – совместное множество формул, то его непротиворечивость следует из предыдущей леммы.

Пусть множество формул Δ непротиворечиво. Покажем, что оно совместно.

Если бы множество формул Δ не было совместным, то любая формула B была бы логическим следствием множества формул Δ , а значит, по **Теореме адекватности для Исчисления Предикатов с равенством**

любая формула B была бы выводима в **Исчислении Предикатов с равенством** из множества формул Δ , что невозможно в силу непротиворечивости множества формул Δ .

Покажем, что **Теорема непротиворечивости для Исчисления Предикатов** влечет **Теорему адекватности для Исчисления Предикатов с равенством**.

Если формула A выводима **Исчислении Предикатов с равенством** из множества формул Γ , то по выше доказанной лемме формула A является логическим следствием множества формул Γ в **Логике Предикатов с равенством**.

Пусть формула A является логическим следствием множества формул Γ в **Логике Предикатов с равенством**.

Покажем, что формула A выводима из множества формул Γ в **Исчислении Предикатов с равенством**.

Предположим противное, т. е. что формула A невыводима из множества формул Γ в **Исчислении Предикатов с равенством**.

Тогда по сделанному выше замечанию A невыводима из множества формул $\Gamma \cup AxEq$ в **Исчислении Предикатов** того же языка L .

По теореме 3.5.26 $\Gamma \cup AxEq \cup \{(\neg A)\}$ – непротиворечивое множество формул **Исчисления Предикатов** того же языка L .

Значит, $\Gamma \cup \{(\neg A)\}$ – непротиворечивое множество формул **Исчисления Предикатов с равенством** того же языка L .

Значит, по **Теореме непротиворечивости для Исчисления Предикатов с равенством** оно совместно.

Пусть φ – нормальная интерпретация, в которой истинны все формулы из множества $\Gamma \cup \{(\neg A)\}$. Значит, формула A ложна в этой интерпретации.

Но по предположению формула A является логическим следствием множества формул Γ в **Логике Предикатов с равенством**.

А так как все формулы из множества Γ истинны в нормальной интерпретации φ , то и формула A истинна в этой интерпретации. Полученное противоречие завершает доказательство эквивалентности **Теоремы адекватности для Исчисления Предикатов с равенством** и **Теоремы непротиворечивости для Исчисления Предикатов**.

Приступаем к доказательству **Теоремы непротиворечивости для Исчисления Предикатов с равенством**. Напомним формулировку этой те-

оремы

множество формул Δ языка $L_{ИПР}$ **Исчисления Предикатов с равенством** непротиворечиво тогда и только тогда, когда оно совместно.

То, что каждое совместное множество формул Δ языка $L_{ИПР}$ **Исчисления Предикатов с равенством** непротиворечиво, установлено в предыдущей лемме.

Остается доказать, что каждое непротиворечивое множество формул Δ языка $L_{ИПР}$ **Исчисления Предикатов с равенством** совместно.

Пусть Δ – непротиворечивое множество формул **Исчисления Предикатов с равенством** языка $L_{ИПР}$.

Тогда $\Delta \cup AxEq$ – непротиворечивое множество формул **Исчисления Предикатов** того же языка $L_{ИПР}$.

По **Теореме непротиворечивости для Исчисления Предикатов** того же языка $L_{ИПР}$ $\Delta \cup AxEq$ – совместное множество формул языка $L_{ИПР}$. Значит, существует интерпретация φ с основным множеством A для языка $L_{ИПР}$, в которой истинны все формулы из множества $\Delta \cup AxEq$.

По интерпретации φ с основным множеством A для языка $L_{ИПР}$ построим нормальную интерпретацию $\hat{\varphi}$ для этого языка, в которой истинны все формулы из множества Δ .

Обозначим через E 2-местный предикат $I(=)$ на основном множестве A .

Так как каждая из следующих трех формул **Исчисления Предикатов с равенством** входит во множество $AxEq$, то все они истинны в интерпретации I

$$\text{VII.1. } (\forall x_1)x_1 = x_1,$$

$$\text{VII.2. } (\forall x_1)(\forall x_2)(x_1 = x_2 \rightarrow x_2 = x_1),$$

$$\text{VII.3. } (\forall x_1)(\forall x_2)(\forall x_3)((x_1 = x_2 \& x_2 = x_3) \rightarrow x_1 = x_3).$$

Поэтому для любых трех элементов a, b и c основного множества A

$$\text{VII.1. } E(a, a),$$

$$\text{VII.2. } E(a, b) \rightarrow E(b, a),$$

$$\text{VII.3. } (E(a, b) \& E(b, c)) \rightarrow E(a, c).$$

Поэтому E – отношение эквивалентности на основном множестве A .

Обозначим через \hat{A} фактормножество множества A по отношению эквивалентности E , т. е. элементами множества \hat{A} являются классы эквивалентности $[a]$.

Построим нормальную интерпретацию \hat{I} с основным множеством \hat{A} .

Для произвольного n -местного функционального символа f и произвольных элементов $[a_1], \dots, [a_n]$ основного множества \hat{A} полагаем

$$\hat{I}(f)([a_1], \dots, [a_n]) = [I(f)(a_1, \dots, a_n)]. \quad (f)$$

Так как для произвольного n -местного функционального символа f во множество $AxEq$ входит формула **Исчисления Предикатов с равенством**

VIII.1.

$$\begin{aligned}
& (\forall x_1)(\forall x_2) \dots (\forall x_n)(\forall y_1)(\forall y_2) \dots (\forall y_n)((\dots (x_1 = y_1 \& x_2 = y_2) \& \dots) \& \\
& \quad x_n = y_n) \rightarrow \\
& \quad f(x_1, x_2, \dots, x_n) = f(y_1, y_2, \dots, y_n)),
\end{aligned}$$

то она истинна в интерпретации I .

Значит, для любых элементов a_1, b_1, \dots, a_n и b_n

$$\begin{aligned}
& (E(a_1, b_1) \& E(a_2, b_2) \& \dots \& \\
& \quad E(a_n, b_n) \rightarrow \\
& \quad E(f(a_1, a_2, \dots, a_n), f(b_1, b_2, \dots, b_n))),
\end{aligned}$$

поэтому определение (f) корректно.

Для произвольного n -местного предикатного символа p , отличного от $=$ и произвольных элементов $[a_1], \dots, [a_n]$ основного множества \hat{A} полагаем

$$\hat{I}(p)([a_1], \dots, [a_n]) = I(p)(a_1, \dots, a_n). \quad (p)$$

Так как для произвольного n -местного предикатного символа p во множество $AxEq$ входит формула **Исчисления Предикатов с равенством** VIII.2.

$$\begin{aligned}
& (\forall x_1)(\forall x_2) \dots (\forall x_n)(\forall y_1)(\forall y_2) \dots (\forall y_n)((\dots (x_1 = y_1 \& x_2 = y_2) \& \dots) \& \\
& \quad x_n = y_n) \rightarrow \\
& \quad p(x_1, x_2, \dots, x_n) \longleftrightarrow p(y_1, y_2, \dots, y_n)).
\end{aligned}$$

то она истинна в интерпретации I .

Значит, для любых элементов a_1, b_1, \dots, a_n и b_n

$$\begin{aligned}
& (E(a_1, b_1) \& E(a_2, b_2) \& \dots \& \\
& \quad E(a_n, b_n) \rightarrow \\
& \quad p(a_1, a_2, \dots, a_n) \longleftrightarrow p(b_1, b_2, \dots, b_n)).
\end{aligned}$$

поэтому определение (p) корректно.

Кроме того, полагаем, что $\hat{I}(=)$ – это обычное равенство на основном множестве \hat{A} .

Индукцией по построению формул нетрудно доказать, что

для произвольной формулы Φ , все свободные переменные которой содержатся в списке x_1, \dots, x_m , и произвольных элементов $[a_1], \dots, [a_m]$ основного множества \hat{A} выполняется равенство

$$\hat{I}(\Phi_{x_1, \dots, x_m}[[a_1], \dots, [a_m]]) = I(\Phi_{x_1, \dots, x_m}[a_1, \dots, a_m]).$$

Так как все формулы из множества Γ истинны в интерпретации I , то все они истинны в нормальной интерпретации \hat{I} .

3.8. Аксиоматическая теория множеств и формальная арифметика

В этом параграфе приводятся некоторые начальные сведения по аксиоматической теории множеств и формальной или аксиоматической арифметике.

Необходимость подведения под канторовскую "наивную" теорию множеств достаточно прочного математического фундамента была осознана уже в конце XIX - начале XX в. после обнаружения противоречий (парадоксов) в канторовской теории множеств.

Аксиоматическая теория множеств направлена на описание методами математической логики достаточно содержательных фрагментов "наивной" теории множеств. В качестве такой системы мы рассмотрим систему ZFC , введенную Е. Цермело (E. Zermelo) в 1908 году и расширенную А. Френкелем (A. Fraenkel) в 1922 году. Эта система теперь называется системой Цермело – Френкеля.

Сигнатура системы ZFC не содержит символов индивидуальных констант и функциональных символов, а содержит лишь два 2-местных предикатных символа \in и $=$.

Термами теории ZFC являются лишь индивидуальные переменные, поэтому элементарные формулы имеют вид $\in (x, y)$ и $= (x, y)$, где x и y – индивидуальные переменные. Мы их будем записывать в более привычном виде $x \in y$ и $x = y$.

Следующие **аксиомы равенства** относятся к логическим аксиомам **аксиома рефлексивности**:

$$(\forall x)(x = x),$$

аксиома симметричности:

$$(\forall x)(\forall y)(x = y \rightarrow y = x),$$

аксиома транзитивности:

$$(\forall x)(\forall y)(\forall z)((x = y \ \& \ y = z) \rightarrow x = z),$$

аксиомы замены:

$$(\forall x)(\forall y)(x = y \rightarrow (\forall z)(x \in z \leftrightarrow y \in z)),$$

$$(\forall x)(\forall y)(x = y \rightarrow (\forall z)(z \in x \leftrightarrow z \in y)).$$

Нелогические аксиомы системы ZFC – это следующие десять аксиом.

Z1. Аксиома объемности (экстенциональности):

$$(\forall x)(\forall y)((\forall z)(z \in x \leftrightarrow z \in y) \rightarrow x = y).$$

Z2. Аксиома существования пустого множества:

$$(\exists u)(\forall x)\neg(x \in u).$$

Множество u , существование которого гарантирует аксиома Z2, в силу аксиомы Z1 определено однозначно. Оно называется **пустым** множеством и обозначается через \emptyset .

Z3. Аксиома пары:

$$(\forall x)(\forall y)(\exists u)(\forall z)(z \in u \leftrightarrow (z = x \vee z = y)).$$

Множество u , существование которого гарантирует аксиома Z3, по элементам (множествам) x и y в силу аксиомы Z1 определено однозначно. Оно обозначается через $\{x, y\}$ и называется неупорядоченной парой элементов x и y .

Одноэлементное множество $\{x\}$, состоящее из x , – это $\{x, x\}$.

Z4. Аксиома суммы (объединения):

$$(\forall x)(\exists u)(\forall z)(z \in u \leftrightarrow (\exists t)(z \in t \& t \in x)).$$

Множество u , существование которого гарантирует аксиома Z4, по элементу (множеству) x в силу аксиомы Z1 определено однозначно. Оно обозначается через $\cup x$ и называется объединением всех элементов (множеств) x .

Из сформулированных аксиом следует, что для любых множеств x и y однозначно определено объединение $\cup \{x, y\}$, которое обозначается через $x \cup y$ и называется объединением множеств x и y . При этом

$$(\forall z)(z \in x \cup y \leftrightarrow (z \in x \vee z \in y)).$$

Введем обозначение: формула $x \subseteq y$ будет служить сокращением (обозначением) для формулы

$$(\forall z)(z \in x \rightarrow z \in y).$$

Z5. Аксиома степени:

$$(\forall x)(\exists u)(\forall z)(z \in u \leftrightarrow z \subseteq x).$$

Множество u , существование которого гарантирует аксиома Z5, по элементу (множеству) x в силу аксиомы Z1 определено однозначно. Оно обозначается через $P(x)$ и называется множеством всех подмножеств множества x или множеством-степенью множества x .

Z6. Аксиома бесконечности:

$$(\exists u)(\emptyset \in u \& (\forall x)(x \in u \rightarrow x \cup \{x\} \in u)).$$

Множество u , существование которого гарантирует аксиома Z6, называется **бесконечным** множеством. Оно, конечно, может быть неединственным.

Через $Inf(u)$ будем обозначать формулу

$$(\emptyset \in u \& (\forall x)(x \in u \rightarrow x \cup \{x\} \in u)).$$

Тогда **Аксиома бесконечности** запишется в виде $(\exists u)Inf(u)$.

Z7. Аксиома выделения в отличие от рассмотренных выше аксиом включает бесконечное множество аксиом вида

$$(\forall z_1) \dots (\forall z_n)(\forall x)(\exists u)(\forall z)(z \in u \leftrightarrow (z \in x \& A(z, z_1, \dots, z_n))),$$

где $A(z, z_1, \dots, z_n)$ – произвольная формула, все свободные переменные которой содержатся среди z, z_1, \dots, z_n . Переменные z_1, \dots, z_n называются параметрами и могут, конечно, отсутствовать. В этом случае **Аксиома выделения** принимает наиболее простой вид

$$(\forall x)(\exists u)(\forall z)(z \in u \leftrightarrow (z \in x \& A(z))),$$

При фиксированных x и $A(z)$ множество u , существование которого гарантирует аксиома Z7, в силу аксиомы Z1 определено однозначно. Оно обозначается через $\{z | z \in x \& A(z)\}$ и называется подмножеством множества x , состоящим из всех его элементов z , обладающих свойством $A(z)$.

Если в этой аксиоме убрать условие (подформулу) $z \in x$, т. е. заменить на формулу вида

$$(\exists u)(\forall z)(z \in u \leftrightarrow \& A(z)),$$

то получим **Аксиому свертывания** "наивной" теории множеств, которая, однако, ведет к противоречию, если, например, в качестве $A(z)$ взять "безобидную" на первый взгляд формулу $\neg(z \in z)$.

Для формулирования восьмой аксиомы, в качестве которой берется **Аксиома выбора**, нам потребуется определить в терминах множеств понятие функции. Это уже было сделано в первой главе. Напомним основные определения.

Упорядоченной парой $\langle x, y \rangle$ элементов (множеств) x и y назовем множество

$$\{\{x\}, \{x, y\}\}.$$

Заметим, что $\langle x, y \rangle \in P(P(x \cup y))$. Тогда декартово произведение $x \times y$ множеств x и y – это множество

$$\{z | z \in P(P(x \cup y)) \& (\exists u)(\exists v)(u \in x \& v \in y \& z = \langle u, v \rangle)\}.$$

Функцией назовем любое множество f такое, что

$$(\exists u)(f \subseteq u \times u) \& (\forall t)(\forall s_1)(\forall s_2)((\langle t, s_1 \rangle \in f \& \langle t, s_2 \rangle \in f) \rightarrow s_1 = s_2).$$

Последнюю формулу будем обозначать через $Fnc(f)$.

Z8. Аксиома выбора:

$$(\forall u)(\exists f)(Fnc(f) \& (\forall x)(x \in u \& \neg(x = \emptyset) \rightarrow f(x) \in x)).$$

Аксиома выбора "утверждает, что для любого множества u существует функция f , которая в каждом непустом элементе (множестве) x из u выбирает элемент $f(x)$ ". Заметим, что ни о какой единственности и "какой-либо определенности" функции f в этой аксиоме речь не идет.

Последние две аксиомы выглядят ”менее естественно”.

Следующая аксиома служит для определенного упрощения некоторых построений. Она ”утверждает, что не существует бесконечных убывающих цепей вида”

$$x_2 \in x_1, x_3 \in x_2, \dots x_{n+1} \in x_n, \dots$$

Z9. Аксиома фундирования:

$$(\forall x)(\neg(x = \emptyset) \rightarrow (\exists y)(y \in x \& (y \cap x = \emptyset))).$$

Здесь через $y \cap x$ обозначено множество

$$\{z \mid z \in y \& z \in x\}.$$

Заключительная аксиома ”содержательно утверждает, что при отображениях, задаваемых формулами рассматриваемого языка, полный образ множества является множеством”.

ZF10. Аксиома замены: пусть $\Phi(x, y)$ – формула с двумя свободными переменными x и y

$$(((\forall x)(\exists y)(\Phi(x, y) \& (\forall z)(\Phi(x, z) \rightarrow z = y))) \rightarrow (\forall u)(\exists v)(\forall t)(t \in v \longleftrightarrow (\exists s)(s \in u \& \Phi(t, s)))).$$

Формальная (аксиоматическая) система ZFC – это весьма сильная теория, практически любая математическая теорема может быть переведена на язык этой системы и выведена из сформулированных выше аксиом Z1 – Z10. В частности, в рамках аксиоматической системы ZFC могут быть сформулированы и доказаны рассмотренные варианты теоремы Рамсея – бесконечная, конечная и обобщенная конечная.

Существует еще несколько вариантов построения аксиоматической теории множеств.

Замена ”наивной” теории множеств той или иной аксиоматической системой позволяет придать точный математический смысл утверждениям о неразрешимости некоторых математических проблем и дать соответствующее математическое доказательство.

Обозначим через ZF аксиоматическую систему, полученную из системы ZFC удалением **Аксиомы выбора** Z8. В 1939 году К. Гедель доказал, что если аксиоматическая система ZF непротиворечива, то непротиворечива и аксиоматическая система $ZFC + CH$, полученная из системы ZFC добавлением **Континуум-гипотезы** (continuum hypothesis). Доказательство основано на построении средствами аксиоматической системы ZF модели для системы ZFC . Поэтому в рамках аксиоматической системы ZFC **Континуум-гипотезу** нельзя опровергнуть (как и **Аксиому выбора**).

В 1963 году П. Коэн доказал, что если аксиоматическая система ZF непротиворечива, то непротиворечива и каждая из следующих четырех аксиоматических систем: $ZF + C + CH$, $ZF + C + \neg CH$, $ZF + \neg C + CH$, $ZF + \neg C + \neg CH$,

полученных из системы ZF добавлением любой комбинации из **Аксиомы выбора**, **Континуум-гипотезы** или их отрицаний.

Результаты К. Геделя и П. Коэна показывают, что если аксиоматическая система ZF непротиворечива, то в рамках аксиоматической системы ZFC невозможно доказать ни **Континуум-гипотезу**, ни ее отрицание. Т. е. **Континуум-гипотеза** в рамках аксиоматической системы ZFC принципиально неразрешима. Аналогичным образом в рамках аксиоматической системы ZF принципиально неразрешима **Аксиома выбора**, т. е. ее нельзя ни доказать, ни опровергнуть.

Из других многочисленных интересных примеров математических утверждений, принципиально неразрешимых в рамках аксиоматической системы ZF , т. е. без использования **Аксиомы выбора**, отметим следующее: если аксиоматическая система ZF непротиворечива, то в ее рамках невозможно ни доказать, ни опровергнуть утверждение о существовании неизмеримого по Лебегу подмножества множества действительных чисел, утверждение о счетности объединения счетного семейства счетных множеств, утверждение об эквивалентности определения предела функции в точке по Гейне и по Коши.

Обозначим через ZFC_{fin} аксиоматическую систему, полученную из системы ZFC удалением **Аксиомы бесконечности** Z6.

В рамках аксиоматической системы ZFC_{fin} может быть проведено доказательство конечной теоремы Рамсея, однако, как было установлено в конце XX века,

обобщенную (усиленную) конечную теорему Рамсея в рамках аксиоматической системы ZFC_{fin} доказать невозможно.

Обсуждение вопроса о том, как можно доказать последнее утверждение, далеко выходит за рамки настоящего пособия. На этом мы завершим наше весьма поверхностное знакомство с аксиоматической теорией множеств.

В заключение рассмотрим один из широко распространенных вариантов формализации (аксиоматизации) теории натуральных чисел или арифметики в широком смысле слова.

Рассмотрим теорию ArP первого порядка с равенством, называемую *формальной или аксиоматической арифметикой* или *арифметикой Пеано*.

Сигнатура системы ArP содержит единственный символ индивидуальной константы 1, два 2-двуместных функциональных символа, обозначаемых традиционно через $+$ и \cdot и называемых соответственно "сложение" и "умножение", один 1-местный функциональный символ s и один 2-местный предикатный символ $=$.

Понятия терма и формулы теории ArP определяются обычным образом. При этом по сложившейся традиции для произвольных термов t_1 и t_2 термы $+(t_1, t_2)$ и $\cdot(t_1, t_2)$ обозначаются через $t_1 + t_2$ и $t_1 \cdot t_2$, а элементарная формула $=(t_1, t_2)$ — через $t_1 = t_2$.

Следующие **аксиомы равенства** относятся к логическим аксиомам

аксиома рефлексивности:

$$(\forall x)(x = x),$$

аксиома симметричности:

$$(\forall x)(\forall y)(x = y \rightarrow y = x),$$

аксиома транзитивности:

$$(\forall x)(\forall y)(\forall z)((x = y \& y = z) \rightarrow x = z),$$

аксиомы замены:

$$(\forall x)(\forall y)(x = y \rightarrow s(x) = s(y)),$$

$$(\forall x_1)(\forall y_1)(\forall x_2)(\forall y_2)(x_1 = y_1 \& x_2 = y_2 \rightarrow x_1 + x_2 = y_1 + y_2),$$

$$(\forall x_1)(\forall y_1)(\forall x_2)(\forall y_2)(x_1 = y_1 \& x_2 = y_2 \rightarrow x_1 \cdot x_2 = y_1 \cdot y_2).$$

Нелогические аксиомы системы ArP – это следующие аксиомы.

$$ArP1. (\forall x)\neg(1 = s(x)).$$

$$ArP2. (\forall x)(\forall y)(s(x) = s(y) \rightarrow x = y).$$

$$ArP3. (\forall x)(x + 1 = s(x)).$$

$$ArP4. (\forall x)(\forall y)(x + s(y) = s(x + y)).$$

$$ArP5. (\forall x)(x \cdot 1 = x).$$

$$ArP6. (\forall x)(\forall y)(x \cdot s(y) = (x \cdot y) + x).$$

ArP7. $((\mathcal{A}_x[1] \& (\forall x)(\mathcal{A} \rightarrow \mathcal{A}_x[s(x)])) \rightarrow (\forall x)\mathcal{A})$, \mathcal{A} – произвольная формула теории ArP .

Последняя аксиома носит название *принцип математической индукции* и представляет собой схему, задающую счетное множество аксиом – для каждой формулы \mathcal{A} своя аксиома. Таким образом, теория ArP задается счетным множеством нелогических аксиом.

Можно показать, что многие теоремы элементарной теории чисел, могут быть выражены формулами теории ArP , которые могут быть выведены из ее аксиом (логических и нелогических) в рамках **Исчисления Предикатов с равенством**. Рассмотрение этого вопроса мы перенесем в продолжение пособия, в котором будет рассмотрено доказательство знаменитой теоремы К. Геделя о неполноте любой ”достаточно” богатой ”эффективно” аксиоматизированной (формальной) теории (при условии ее непротиворечивости).

3.9. Теоремы Д. Кенига и Ф. Рамсея

Рассмотрим две классические теоремы из теории бесконечных графов, доказательства которых основаны на **Аксиоме выбора** – теоремы Д. Кенига и Ф. Рамсея.

При изложении доказательства этих теорем мы будем придерживаться в основном подхода из монографии К. Куратовского и А. Мостовского [23].

В конце параграфа содержится небольшой по объему материал, несколько выходящий за рамки канторовской "наивной" теории множеств. Для его понимания необходимо знание некоторых, впрочем, достаточно простых фактов из математической логики. Читатель может при первом чтении ознакомиться с этим материалом и вернуться к нему вновь после изучения соответствующих разделов математической логики. Конечно, этот материал можно было и бы и не включать в пособие. Однако, по нашему мнению, его включение позволяет без использования сложных математических понятий показать читателю, как изучение достаточно естественных теоретико-множественных понятий приводит к вопросам, получение ответов на которые оказывается невозможным без средств математической логики. Кроме того, этот материал может служить наглядной демонстрацией "силы и мощи теоретико-множественных методов", позволяющих решать сложные проблемы "конечной математики" путем "выхода в бесконечную область", т. е. привлекая к доказательству теорем, относящихся к достаточно естественным и простым комбинаторным вопросам о конечных множествах, технику работы с бесконечными множествами. А математическая логика дает возможность доказать, что этот "выход в бесконечную область" вызван не нашей недостаточной изобретательностью "в конечной области", а необходим по существу – без такого выхода соответствующие теоремы невозможно доказать.

Пусть $f : A \rightarrow A$ – отображение множества A в себя.

Конечная последовательность c_1, c_2, \dots, c_n элементов множества A называется *ветвью длины n* , если выполняются равенства

$$c_1 = f(c_2), c_2 = f(c_3), \dots, c_{n-1} = f(c_n).$$

Бесконечная последовательность $c_1, c_2, \dots, c_n, \dots$ элементов множества A называется *бесконечной ветвью*, если выполняются равенства

$$c_1 = f(c_2), c_2 = f(c_3), \dots, c_{n-1} = f(c_n), \dots$$

Элемент c_1 называется *начальной вершиной* ветви.

Теорема 3.9.1 (Д. Кёниг). Пусть $f : A \rightarrow A$ – такое отображение множества A в себя, что для любого элемента u из A множество уровня

$$f^{-1}(\{u\}) = \{x \mid u = f(x)\}$$

конечно. Если для элемента w множества A и любого натурального числа n существует ветвь длины n , начинающаяся в w , то существует и бесконечная ветвь с началом в w .

Д о к а з а т е л ь с т в о. Обозначим через B множество всех элементов u множества A таких, что для любого натурального числа n существует ветвь длины n , начинающаяся в u . По условию теоремы элемент w принадлежит B .

Докажем, что для любого элемента u из множества B в этом множестве найдется такой элемент v , что $u = f(v)$, т. е. $f^{-1}(\{u\}) \cap B \neq \emptyset$.

Предположим противное. Пусть u – такой элемент из множества B , что в этом множестве нет элемента v такого, что $u = f(v)$. Это означает, что для любого элемента v_i из конечного множества

$$f^{-1}(\{u\}) = \{v_1, v_2, \dots, v_m\}$$

найдется такое число n_i , что не существует ветви длины n_i , начинающейся в v_i .

Обозначим через n наибольшее из чисел n_1, \dots, n_m .

Значит, для любого элемента v такого, что $u = f(v)$, не существует ветви длины n , начинающейся в v .

Поэтому не существует ветви длины $n + 1$, начинающейся в u . Что противоречит выбору элемента u .

Рассмотрим **функцию выбора** φ , которая для каждого непустого множества вида $f^{-1}(\{u\}) \cap B$ дает элемент из этого множества

$$\varphi(f^{-1}(\{u\}) \cap B) \in f^{-1}(\{u\}) \cap B.$$

Кроме того, полагаем $\varphi(\emptyset) = w$.

Зададим бесконечную последовательность $c_1, c_2, \dots, c_n, \dots$ элементов множества A равенствами

$$c_1 = w, \quad c_{n+1} = \varphi(f^{-1}(\{c_n\}) \cap B)$$

Покажем, что при любом m $c_{m+1} \in f^{-1}(\{c_m\}) \cap B$.

При $m = 0$ получаем $c_0 = w \in B$, $f^{-1}(\{c_0\}) \cap B \neq \emptyset$, поэтому

$$c_1 = \varphi(f^{-1}(\{c_0\}) \cap B) \in f^{-1}(\{c_0\}) \cap B.$$

Предположим, что $c_{n+1} \in f^{-1}(\{c_n\}) \cap B$.

Тогда $f^{-1}(\{c_{n+1}\}) \cap B \neq \emptyset$, поэтому

$$c_{n+2} = \varphi(f^{-1}(\{c_{n+1}\}) \cap B) \in f^{-1}(\{c_{n+1}\}) \cap B.$$

Таким образом, при любом n выполняется равенство $c_n = f(c_{n+1})$, т. е. $c_1, c_2, \dots, c_n, \dots$ – бесконечная ветвь с началом в w . \square

Теорема Ф. Рамсея может быть сформулирована либо в терминах неориентированных графов без петель, либо в терминах симметричных антирефлексивных отношений, либо в терминах разбиений множества всех 2-элементных подмножеств произвольного множества на конечное число непересекающихся подмножеств (классов). Первый вариант формулировки в определенной степени "более нагляден". Его мы и рассмотрим, а затем обсудим третий вариант и от него перейдем к разбиениям множества всех 2-элементных подмножеств

произвольного множества на конечное число классов и к аналогичным разбиениям t -элементных подмножеств. Начнем мы с наиболее простого варианта теоремы Ф. Рамсея.

Для неориентированного графа без петель $G = \langle V, E \rangle$ с множеством вершин V и множеством ребер E через \overline{G} будем обозначать дополнительный граф $\overline{G} = \langle V, \overline{E} \rangle$, где для любых двух различных вершин u и v выполнена эквивалентность

в \overline{E} есть ребро, соединяющее вершины u и v тогда и только тогда, когда в E отсутствует ребро, соединяющее вершины u и v .

Теорема 3.9.2 (Ф. Рамсей). *Если $G = \langle V, E \rangle$ – неориентированный граф без петель с бесконечным множеством вершин V , то либо G , либо \overline{G} содержит полный подграф с бесконечным множеством вершин.*

Сформулированный вариант теоремы Ф. Рамсея допускает следующую, возможно, более наглядную, формулировку.

Для произвольного множества (вершин) V обозначим через $[V]_2$ полный неориентированный граф без петель с этим множеством вершин, т. е. в этом графе любые две различные вершины соединены ребром. Неориентированному графу без петель $G = \langle V, E \rangle$ можно поставить в соответствие раскраску ребер полного графа $[V]_2$ двумя цветами – одним цветом раскрашиваются ребра, включаемые в множество ребер E графа G , а другим – невключаемые. Приходим к следующей формулировке.

Произвольным образом раскрасим ребра полного графа $[V]_2$ двумя цветами. Тогда теорема Ф. Рамсея утверждает, что найдется такое бесконечное подмножество $U \subseteq V$, что все ребра полного подграфа $[U]_2$ оказались выкрашенными в один цвет.

Д о к а з а т е л ь с т в о. Идея доказательства достаточно проста – строятся три бесконечные последовательности вершин графа $[V]_2$, цветов и подграфов, которые и позволят доказать существование бесконечного подмножества $U \subseteq V$ с требуемым свойством.

Полагаем $V_0 = V$.

Выбираем вершину $v_0 \in V_0$. Эта вершина соединена бесконечным числом ребер с вершинами из $V_0 \setminus \{v_0\}$. Среди этих ребер бесконечное число ребер одного цвета, который обозначим через c_0 , а бесконечное множество соответствующих этим ребрам вершин из $V \setminus \{v_0\}$ – через V_1 . Тогда

$$v_0 \in V_0, \quad V_0 \supseteq V_1,$$

все ребра, соединяющие вершину v_0 с вершинами из множества V_1 ,

выкрашены в один цвет c_0 .

Выбираем вершину $v_1 \in V_1$. Эта вершина соединена бесконечным числом ребер с вершинами из $V_1 \setminus \{v_1\}$. Среди этих ребер бесконечное число ребер одного

цвета, который обозначим через c_1 , а бесконечное множество соответствующих этим ребрам вершин из $V_1 \setminus \{v_1\}$ – через V_2 . Тогда

$v_1 \in V_1$, $V_1 \supseteq V_2$,
все ребра, соединяющие вершину v_1 с вершинами из множества V_2 ,
выкрашены в один цвет c_1 .

Предположим, что уже выбраны вершина v_{n-1} , цвет c_{n-1} и бесконечные множества вершин $V_{n-1} \supseteq V_n$ так, что

$v_{n-1} \in V_{n-1}$, $V_{n-1} \supseteq V_n$,
все ребра, соединяющие вершину v_{n-1} с вершинами из множества V_n ,
выкрашены в один цвет c_{n-1} .

Выбираем вершину $v_n \in V_n$. Эта вершина соединена бесконечным числом ребер с вершинами из $V_n \setminus \{v_n\}$. Среди этих ребер бесконечное число ребер одного цвета, который обозначим через c_n , а бесконечное множество соответствующих этим ребрам вершин из $V_n \setminus \{v_n\}$ – через V_{n+1} . Тогда

$v_n \in V_n$, $V_n \supseteq V_{n+1}$,
все ребра, соединяющие вершину v_n с вершинами из множества V_{n+1} ,
выкрашены в один цвет c_n .

Получаем три бесконечные последовательности

последовательность вершин:

$v_0, v_1, \dots, v_n, \dots$;

последовательность цветов:

$c_0, c_1, \dots, c_n, \dots$;

последовательность бесконечных подграфов:

$[V_0]_2 \supseteq [V_1]_2 \supseteq \dots \supseteq [V_n]_2 \supseteq \dots$,

такие, что

$v_n \in V_n \setminus V_{n+1}$,
все ребра, соединяющие вершину v_n с вершинами из множества V_{n+1} ,
выкрашены в один цвет c_n .

Обозначим через \mathbf{c} тот цвет, который встречается бесконечное число раз в последовательность цветов:

$c_0, c_1, \dots, c_n, \dots$

Пусть

$$\mathbf{c} = c_{i_0} = c_{i_1} = \dots = c_{i_n} = \dots$$

Обозначим через U бесконечное множество вершин

$$v_{i_0}, v_{i_1}, \dots, v_{i_n}, \dots$$

Тогда все ребра бесконечного полного подграфа $[U]_2$ выкрашены в один цвет \mathbf{c} .

В предложенном доказательстве есть "слабое место" – мы не доказали, что соответствующие три бесконечные последовательности вершин графа $[V]_2$, цветов и подграфов *существуют*. В частности, *нуждается в доказательстве существования бесконечного множества вершин*

$$\{v_0, v_1, \dots, v_n, \dots\}.$$

Такое доказательство должно опираться на некоторые явно сформулированные аксиомы теории множеств. В нашем случае это будет **Аксиома выбора**.

Обозначим через φ функцию выбора для семейства всех непустых подмножеств множества вершин V , т. е. функция φ в каждом непустом подмножестве U множества V выделяет элемент $\varphi(U) \in U$. Для произвольной вершины v обозначим через $V_G(v)$ ($\bar{V}_G(v)$) множество вершин смежных с вершиной v в графе $V_G(v)$ ($\bar{V}_G(v)$).

Ребро, соединяющее вершины v и u , мы рассматриваем как множество $\{v, u\}$ из двух элементов v и u (неупорядоченная пара этих элементов).

По индукции определим четыре последовательности, из которых две состоят из подмножеств множества V вершин графа G , третья – из вершин этого графа, а четвертая – из натуральных чисел.

$$\begin{aligned} T_0 &= V, \quad A_0 = V, \quad v_0 = \varphi(V), \quad f_0 = 0; \\ T_{n+1} &= \{x \mid x \in A_n \text{ \& множество } V_G(x) \cap A_n \text{ бесконечно} \} \end{aligned}$$

$$\begin{aligned} v_{n+1} &= \begin{cases} \varphi(T_{n+1}), & T_{n+1} \neq \emptyset; \\ v_0, & T_{n+1} = \emptyset; \end{cases} \\ A_{n+1} &= \begin{cases} V_G(v_{n+1}) \cap A_n, & T_{n+1} \neq \emptyset; \\ \emptyset, & T_{n+1} = \emptyset; \end{cases} \\ f_{n+1} &= \begin{cases} 0, & T_{n+1} \neq \emptyset; \\ 1, & T_{n+1} = \emptyset. \end{cases} \end{aligned}$$

Возможны два случая.

Случай 1. При любом n $f_{n+1} = 0$. В этом случае индукцией по n доказывается, что при любом n

$$\begin{aligned} v_{n+1} &\in T_{n+1}, \\ \text{множество } V_G(x) \cap A_n &\text{ бесконечно,} \\ A_{n+1} &\subseteq V_G(v_{n+1}) \cap A_n, \\ T_{n+1} &\subseteq A_n. \end{aligned}$$

Отсюда следует, что при $k > j \geq 0$ $A_k \subseteq A_{k-1} \subseteq A_j$. Так как $v_k \in T_k \subseteq A_{k-1}$ и $v_k \notin V_G(v_k)$, то $v_k \in A_{k-1} \setminus A_k$, поэтому $v_k \in A_j \setminus A_k$. Значит, множество вершин

$$\{v_k \mid k = 0, 1, \dots\}$$

бесконечно и любые две из этих вершин соединены ребром в графе G , т. е. в G имеется бесконечный полный подграф.

Случай 2. Найдется такое i , что $f_{i+1} = 1$, значит, $T_{i+1} = \emptyset$. Через i_0 обозначим наименьшее из таких i . Значит, при любом $i \leq i_0$: $f_i = 0$ и $f_{i_0+1} = 1$. Поэтому $T_i \neq \emptyset$, значит, $a_i = \varphi(T_i) \in T_i$. Но $T_{i_0+1} = \emptyset$.

Рассмотрим множество A_{i_0} . При $i_0 = 0$ это множество совпадает с множеством V всех вершин графа G , а при $i_0 > 0$ — с множеством $V_G(a_{i_0}) \cap A_{i_0-1}$. Это множество бесконечно, так как $a_{i_0} \in T_{i_0}$. В любом случае множество A_{i_0} бесконечно.

По индукции определим последовательность подмножеств этого множества и последовательность его элементов.

$$\begin{aligned} B_0 &= A_{i_0}, \quad b_0 = \varphi(B_0), \\ B_{n+1} &= \begin{cases} V_{\overline{G}}(b_n) \cap B_n, & B_n \neq \emptyset; \\ \emptyset, & B_n = \emptyset; \end{cases} \\ b_{n+1} &= \begin{cases} \varphi(B_{n+1}), & B_{n+1} \neq \emptyset; \\ b_0, & B_{n+1} = \emptyset. \end{cases} \end{aligned}$$

Построенные множества образуют убывающую последовательность. По индукции докажем, что каждое из этих множеств бесконечно.

$B_0 = A_{i_0}$ — бесконечное множество.

Предположим, что B_n — бесконечное множество.

Докажем бесконечность множества $B_{n+1} = V_{\overline{G}}(b_n) \cap B_n$.

Если бы это множество было конечным, то в силу бесконечности множества B_n бесконечным было бы множество $B_n \setminus (V_{\overline{G}}(b_n) \cap \{b_n\})$. Но

$$B_n \setminus (V_{\overline{G}}(b_n) \cap \{b_n\}) \subseteq (V_G(b_n) \cap \{B_n\}) \subseteq (V_G(b_n) \cap \{A_{i_0}\}),$$

значит, $b_n \in T_{i_0+1}$, что противоречит пустоте последнего множества.

Полученное противоречие показывает, что каждое из множеств B_n бесконечно. Значит, в частности, каждое из них непусто, поэтому при любом n : $b_n \in B_n$. При $n > t$ получаем

$$b_n \in B_n \subseteq B_{m+1} \subseteq V_{\overline{G}}(b_m),$$

значит, вершины b_n и b_m соединены ребром в графе \overline{G} . Поэтому граф \overline{G} содержит бесконечный полный подграф с множеством вершин

$$\{b_0, b_1, \dots, b_n, \dots\}.$$

□

В качестве следствия теоремы Ф. Рамсея рассмотрим следующий интересный пример из указанной выше монографии К. Куратовского и А. Мостовского [23].

По произвольному множеству V натуральных чисел построим граф с множеством вершин V . Вершины, соответствующие натуральным числам u и v , соединяем ребром тогда и только тогда, когда числа u и v взаимно просты. Из теоремы Ф. Рамсея следует, что

если V – произвольное бесконечное множество натуральных чисел, то оно содержит такое бесконечное подмножество U , что либо любые два содержащихся в нем числа взаимно просты, либо любые два содержащихся в нем числа не взаимно просты, т. е. имеют неединичный общий делитель.

Нетрудно понять, что на самом деле фактически доказан более общий, чем сформулированный в теореме, вариант теоремы Ф. Рамсея –

если ребра полного графа $[V]_2$ произвольным образом раскрасить k цветами, то найдется такое бесконечное подмножество $U \subseteq V$, что все ребра полного подграфа $[U]_2$ выкрашены в один цвет.

Впрочем, общий случай легко получается из случая $k = 2$ по индукции – переход от k к $k + 1$ проводится по следующей схеме. Предположим, что все ребра полного графа $[V]_2$ произвольным образом раскрашены в $k + 1$ цвет. Обозначим эти цвета через c_1, \dots, c_{k+1} .

Возьмем два новых цвета c'_1 и c'_2 , которыми следующим образом раскрасим ребра полного графа $[V]_2$: если ребро e полного графа $[V]_2$ было раскрашено цветом c_1 , то раскрасим его цветом c'_1 , в противном случае, т. е. если ребро e полного графа $[V]_2$ было раскрашено одним из цветов c_2, \dots, c_{k+1} , то раскрасим его цветом c'_2 .

Тогда найдется такое бесконечное подмножество $U \subseteq V$, что все ребра полного подграфа $[U]_2$ выкрашены в один цвет, т. е. либо в цвет c'_1 , либо в цвет c'_2 .

В первом случае теорема доказана, а во втором случае для завершения доказательства достаточно применить индуктивное предположение.

Перейдем к другой формулировке. Ребро e произвольного неориентированного графа G без петель с концевыми вершинами u и v можно отождествить с 2-элементным подмножеством $\{u, v\}$ множества V , т. е. считать, что

$$E \subseteq [V]^2 = \{\{u, v\} \mid u, v \in V \text{ и } u \neq v\}.$$

Тогда множество ребер полного графа $[V]_2$ – это просто множество $[V]^2$ всех 2-элементных подмножеств множества V . Раскраске ребер полного графа $[V]_2$

в k цветов соответствует разбиение множества $[V]^2$ всех 2-элементных подмножеств множества V в объединение k непустых попарно непересекающихся подмножеств U_1, \dots, U_k .

Поэтому из вышесказанного следует справедливость следующей теоремы.

Теорема 3.9.3. Пусть V – произвольное бесконечное множество, $[V]^2$ – множество всех его 2-элементных подмножеств, k – натуральное число, W_1, \dots, W_k – такие подмножества множества V_2 , что

$$[V]^2 = W_1 \cup \dots \cup W_k,$$

$$\text{при } 1 \leq i < j \leq k : \quad W_i \cap W_j = \emptyset.$$

Тогда найдется такое бесконечное подмножество U множества V и такое число i_0 ($1 \leq i_0 \leq k$), что $[U]^2 \subseteq W_{i_0}$, т. е. все 2-элементные подмножества бесконечного множества U содержатся в одном подмножестве W_{i_0} .

Последняя теорема допускает естественное обобщение.

Теорема 3.9.4. Пусть V – произвольное бесконечное множество, $[V]^t$ – множество всех его t -элементных подмножеств, k – натуральное число, W_1, \dots, W_k – такие подмножества множества $[V]^t$, что

$$V_t = W_1 \cup \dots \cup W_k,$$

$$\text{при } 1 \leq i < j \leq k : \quad W_i \cap W_j = \emptyset.$$

Тогда найдется такое бесконечное подмножество U множества V и такое число i_0 ($1 \leq i_0 \leq k$), что $[U]^t \subseteq W_{i_0}$, т. е. все t -элементные подмножества бесконечного множества U содержатся в одном подмножестве W_{i_0} .

Последняя теорема может быть переформулирована на языке отображений.

Теорема 3.9.5. Пусть V – произвольное бесконечное множество, $[V]^t$ – множество всех его t -элементных подмножеств, k – натуральное число и f – отображение множества $[V]^t$ во множество $\{1, 2, \dots, k\}$, т. е.

$$f : [V]^t \rightarrow \{1, 2, \dots, k\}.$$

Тогда найдется такое бесконечное подмножество U множества V и такое число i_0 ($1 \leq i_0 \leq k$), что для любого u из $[U]^t$ $f(u) = i_0$, т. е. все t -элементные подмножества бесконечного множества U отображение f переводит в одно и то же число i_0 .

Сформулированный вариант теоремы Ф. Рамсея допускает следующую, достаточно наглядную, формулировку на языке гиперграфов.

Для произвольного множества (вершин) V и фиксированного натурального числа t обозначим через V_t множество всех его t -элементных подмножеств.

Каждый элемент e из V_t , т. е. t -элементное подмножество множества V , будем называть *гиперребром* размерности t .

Через $[V]_t$ обозначим *полный неориентированный t -гиперграф* с этим множеством вершин, т. е. в этом гиперграфе любые t различных вершин соединены ребром размерности t .

Гиперграф размерности t – это $G = \langle V, E \rangle$, где E – подмножество множества V_t всех t -элементных подмножеств множества V , т. е. элементами E являются некоторые *гиперребра* размерности t .

Предыдущая теорема может быть переформулирована следующим образом на языке гиперграфов.

Теорема 3.9.6 (Ф. Рамсей). *Если гиперребра полного неориентированного гиперграфа $[V]_t$ с бесконечным множеством вершин V произвольным образом раскрасить k цветами, то найдется такое бесконечное подмножество $U \subseteq V$, что все ребра полного гиперграфа $[U]_t$ будут выкрашены в один цвет.*

Доказательство. Доказательство проведем по ранее уже использованной схеме – построим три бесконечные последовательности вершин гиперграфа $[V]_t$, цветов и подгиперграфов, которые и позволят доказать существование бесконечного подмножества $U \subseteq V$ с требуемым свойством.

Полагаем $V_0 = V$.

Выбираем вершину $v_0 \in V_0$. Эта вершина соединена бесконечным числом гиперребер с вершинами из $V_0 \setminus \{v_0\}$. Среди этих гиперребер бесконечное число гиперребер одного цвета, который обозначим через c_0 , а бесконечное множество соответствующих этим гиперребрам вершин из $V \setminus \{v_0\}$ – через V_1 . Тогда

$$v_0 \in V_0, \quad V_0 \supseteq V_1,$$

все гиперребра, соединяющие вершину v_0 с вершинами из множества V_1 ,
выкрашены в один цвет c_0 .

Выбираем вершину $v_1 \in V_1$. Эта вершина соединена бесконечным числом гиперребер с вершинами из $V_1 \setminus \{v_1\}$. Среди этих гиперребер бесконечное число гиперребер одного цвета, который обозначим через c_1 , а бесконечное множество соответствующих этим гиперребрам вершин из $V_1 \setminus \{v_1\}$ – через V_2 . Тогда

$$v_1 \in V_1, \quad V_1 \supseteq V_2,$$

все гиперребра, соединяющие вершину v_1 с вершинами из множества V_2 ,
выкрашены в один цвет c_1 .

Предположим, что уже выбраны вершина v_{n-1} , цвет c_{n-1} и бесконечные множества вершин $V_{n-1} \supseteq V_n$ так, что

$$v_{n-1} \in V_{n-1}, \quad V_{n-1} \supseteq V_n,$$

все гиперребра, соединяющие вершину v_{n-1} с вершинами из множества V_n ,
выкрашены в один цвет c_{n-1} .

Выбираем вершину $v_n \in V_n$. Эта вершина соединена бесконечным числом гиперребер с вершинами из $V_n \setminus \{v_n\}$. Среди этих гиперребер бесконечное число гиперребер одного цвета, который обозначим через c_n , а бесконечное множество соответствующих этим гиперребрам вершин из $V_n \setminus \{v_n\}$ – через V_{n+1} . Тогда

$$v_n \in V_n, V_n \supseteq V_{n+1},$$

все гиперребра, соединяющие вершину v_n с вершинами из множества V_{n+1} ,
выкрашены в один цвет c_n .

Получаем три бесконечные последовательности

последовательность вершин:

$$v_0, v_1, \dots, v_n, \dots;$$

последовательность цветов:

$$c_0, c_1, \dots, c_n, \dots;$$

последовательность бесконечных подгиперграфов:

$$[V_0]_t \supseteq [V_1]_t \supseteq \dots \supseteq [V_n]_t \supseteq \dots,$$

такие, что

$$v_n \in V_n \setminus V_{n+1},$$

все гиперребра, соединяющие вершину v_n с вершинами из множества V_{n+1} ,
выкрашены в один цвет c_n .

Обозначим через \mathbf{c} тот цвет, который встречается бесконечное число раз в последовательность цветов:

$$c_0, c_1, \dots, c_n, \dots$$

Пусть

$$\mathbf{c} = c_{i_0} = c_{i_1} = \dots = c_{i_n} = \dots$$

Через U обозначим бесконечное множество вершин

$$v_{i_0}, v_{i_1}, \dots, v_{i_n}, \dots$$

Тогда все гиперребра бесконечного полного подгиперграфа $[U]_t$ выкрашены в один цвет \mathbf{c} .

В предложенном доказательстве, как и выше, есть "слабое место" – мы не доказали, что соответствующие три бесконечные последовательности вершин графа $[V]_t$, цветов и подгиперграфов *существуют*. В частности, нуждается в доказательстве существование бесконечного множества вершин

$$\{v_0, v_1, \dots, v_n, \dots\}.$$

Такое доказательство должно опираться на некоторые явно сформулированные аксиомы теории множеств. Это можно сделать, как было сделано выше, на основе **Аксиомы выбора**.

Возможно и доказательство индукцией по t на основе уже доказаного выше утверждения для $t = 2$. При этом, конечно, была использована **Аксиомы выбора**. \square

Индукцией по p доказывается следующее обобщение рассмотренных выше теорем.

Теорема 3.9.7. Пусть p – произвольное фиксированное число, V – произвольное бесконечное множество, V_{fin} – множество всех его конечных подмножеств, k – натуральное число, W_1, \dots, W_k – такие подмножества множества V_{fin} , что

$$V_{fin} = W_1 \cup \dots \cup W_k,$$

$$\text{при } 1 \leq i < j \leq k : \quad W_i \cap W_j = \emptyset.$$

Тогда найдется такое бесконечное подмножество U множества V , что для любого $t \leq p$ найдется такое число $i(t)$ ($1 \leq i(t) \leq k$), что $[U]^t \subseteq W_{i(t)}$, т. е. все t -элементные подмножества бесконечного множества U содержатся в одном подмножестве $W_{i(t)}$.

Мы не утверждаем, что все t -элементные подмножества множества U при любом $t \leq p$ содержатся в одном и том же подмножестве W_{i_0} . Например, это не так в случае

$$W_1 = [V]^1, \quad W_2 = \bigcup_{t=2}^{\infty} [V]^t.$$

Мы лишь утверждаем, что для любого $t \leq p$ найдется подходящее число $i(t)$ ($1 \leq i(t) \leq k$) такое, что $[U]^t \subseteq W_{i(t)}$, т. е. все t -элементные подмножества бесконечного множества U содержатся в одном подмножестве $W_{i(t)}$ (но для каждого t такое подмножество может быть свое).

Следующий пример, заимствованный из [3], показывает, что дальнейшее обобщение рассмотренных теорем путем отказа от ограничения $t \leq p$ невозможно. Т. е. следующее утверждение не может быть доказано.

Пусть V – произвольное бесконечное множество, V_{fin} – множество всех его конечных подмножеств, k – натуральное число, W_1, \dots, W_k – такие подмножества множества V_{fin} , что

$$V_{fin} = W_1 \cup \dots \cup W_k,$$

$$\text{при } 1 \leq i < j \leq k : \quad W_i \cap W_j = \emptyset.$$

Тогда найдется такое бесконечное подмножество U множества V , что для любого t найдется такое число $i(t)$ ($1 \leq i(t) \leq k$), что

$$[U]^t \subseteq W_{i(t)},$$

т. е. все t -элементные подмножества бесконечного множества U содержатся в одном подмножестве $W_{i(t)}$.

Следующий пример показывает, что последнее утверждение неверно.

Для конечного множества A натуральных чисел обозначим через $|A|$ число элементов во множестве A .

Пусть W_1 состоит из всех таких конечных подмножеств A множества натуральных чисел N , для которых $|A| \in A$, а $W_2 = N_{fin} \setminus W_1$. Тогда $N_{fin} = W_1 \cup W_2$ и $W_1 \cap W_2 = \emptyset$.

Пусть U – произвольное бесконечное множество натуральных чисел.

Выбираем в U число $t \geq 2$ и t попарно различных и отличных от t чисел a_1, \dots, a_t .

Тогда

$$\begin{aligned} \{t, a_2, \dots, a_t\} \in [U]^t, \quad \{a_1, a_2, \dots, a_t\} \in [U]^t, \\ \{t, a_2, \dots, a_t\} \in W_1, \quad \{a_1, a_2, \dots, a_t\} \in W_2. \end{aligned}$$

Рассмотренные теоремы Ф. Рамсея относятся к разбиениям бесконечных множеств и к бесконечным графам и гиперграфам. Поэтому их можно условно назвать "бесконечными" теоремами Ф. Рамсея. Эти теоремы не представляется возможным даже сформулировать на языке формальной арифметики Пеано, т. е. без использования теоретико-множественного языка.

Ф. Рамсеем доказаны аналоги рассмотренных теорем для конечных графов и разбиений конечных множеств. По ряду причин, о которых будет сказано позже, эти аналоги представляют особый интерес для математической логики.

Начнем с самого простого варианта "конечных" теорем Ф. Рамсея.

Теорема 3.9.8 (Ф. Рамсей). *Для любого натурального числа n существует такое натуральное число q , что для любого неориентированного графа без петель G с q вершинами либо он сам, либо его дополнение \overline{G} содержит полный подграф (клику) на n вершинах.*

Эта теорема может быть доказана чисто комбинаторными методами без использования бесконечных множеств. Такое доказательство может быть даже переведено на язык элементарной арифметики, т. е. в нем речь будет идти о натуральных числах, а не о их множествах и об операциях сложения и умножения натуральных чисел. Доказательство может быть проведено в формальной арифметике Пеано ArP , если вместо конечных множеств натуральных чисел говорить о их *номерах*, используя для этого, например, функцию К. Геделя

$$\Gamma(a, b, i) = \text{rest}(a, 1 + (i + 1)b),$$

обладающую следующим фундаментальным свойством:

для любой конечной последовательности натуральных чисел a_0, a_1, \dots, a_n найдутся такие натуральные числа a и b , что выполняются равенства

$$\Gamma(a, b, 0) = a_0, \Gamma(a, b, 1) = a_1, \dots, \Gamma(a, b, n) = a_n.$$

Указанные натуральные числа a и b можно считать *номером* множества натуральных чисел

$$\{a_0, a_1, \dots, a_n\}.$$

Однако такое доказательство будет достаточно громоздким.

Покажем, что этот вариант "конечных" теорем Ф. Рамсея можно легко получить как *следствие "бесконечных" теорем Ф. Рамсея и теоремы компактности или теоремы о локальном логическом следствии из математической логики*.

Рассмотрим **Логику предикатов с равенством** в сигнатуре, содержащей лишь два 2-местных предикатных символа $=$ и R , причем предикатный символ $=$ будет интерпретироваться как обычное равенство, т. е. мы будем рассматривать лишь *нормальные модели*.

Обозначим через $G(R)$ следующую формулу

$$(\forall x)(\forall y)(\neg R(x, x) \& (R(x, y) \longrightarrow R(y, x))),$$

через Φ_n – формулу

$$(\exists x_1) \dots (\exists x_n) (\bigwedge_{1 \leq i < j \leq n} \neg x_i = x_j \& (\bigwedge_{1 \leq i < j \leq n} R(x_i, x_j) \vee \bigwedge_{1 \leq i < j \leq n} \neg R(x_i, x_j))),$$

а через R_n – формулу $(G(R) \longrightarrow \Phi_n)$.

По "бесконечной" теореме Ф. Рамсея формула R_n истинна на любой бесконечной системе $\langle M; R \rangle$, поэтому *формула R_n является логическим следствием следующего бесконечного множества формул*

$$\{\mathcal{E}_1, \mathcal{E}_2, \dots, \mathcal{E}_m, \dots\},$$

где через \mathcal{E}_m обозначена формула $(\exists y_1) \dots (\exists y_m) (\bigwedge_{1 \leq i < j \leq m} \neg y_i = y_j)$, "содержательно утверждающая, что система содержит не менее чем m элементов". По теореме о локальном следствии существует такое число $q(n)$, что *формула R_n логически следует из конечного множества формул*

$$\{\mathcal{E}_1, \mathcal{E}_2, \dots, \mathcal{E}_{q(n)}\}.$$

Последнее и означает, что *для любого графа G с $q(n)$ и более вершинами либо он сам, либо его дополнение \overline{G} содержит полный подграф (клику) на n вершинах*.

Задача нахождения по произвольному числу n наименьшего числа $q(n)$ с указанным свойством представляет собой весьма непростую комбинаторную проблему.

Приведем теперь наиболее общий вариант "конечной" теоремы Ф. Рамсея.

Теорема 3.9.9 (Ф. Рамсей). *Для произвольных натуральных чисел k, m_1, \dots, m_k и t существует такое число $N(k, m_1, \dots, m_k, t)$, что для произвольного множества V , содержащего не менее, чем $N(k, m_1, \dots, m_k, t)$ элементов, и*

любых подмножеств W_1, \dots, W_k множества $[V]^t$ всех t -элементных подмножеств множества V таких, что

$$[V]^t = W_1 \cup \dots \cup W_k,$$

$$\text{при } 1 \leq i < j \leq k: \quad W_i \cap W_j = \emptyset,$$

найдется такое число i_0 ($1 \leq i_0 \leq k$) и такое подмножество U множества V , содержащее не менее, чем m_{i_0} элементов, что $[U]^t \subseteq W_{i_0}$, т. е. все t -элементные подмножества множества U содержатся в одном и том же подмножестве W_{i_0} .

И эта теорема может быть доказана чисто комбинаторными методами без использования бесконечных множеств. Однако такое доказательство будет достаточно громоздким.

Комбинаторное доказательство может быть даже переведено на язык элементарной арифметики, т. е. в нем речь будет идти о натуральных числах, а не об их множествах и об операциях сложения и умножения натуральных чисел. Доказательство может быть проведено в формальной арифметике Пеано ArP , если вместо конечных множеств натуральных чисел говорить об их *номерах*, используя для этого, например, функцию К. Геделя

$$\Gamma(a, b, i) = \text{rest}(a, 1 + (i + 1)b).$$

И этот достаточно общий вариант "конечных" теорем Ф. Рамсея нетрудно получить как *следствие "бесконечных" теорем Ф. Рамсея и теоремы компактности или теоремы о локальном логическом следствии из математической логики*.

Последнее утверждение для нас интересно тем, что некоторое его обобщение, которое допускает формулировку на языке элементарной арифметики, можно доказать в теории множеств с использованием бесконечных множеств и **Аксиомы выбора**, однако нельзя доказать в формальной арифметике Пеано ArP , т. е. элементарными методами, конечно, при условии, что арифметика Пеано ArP непротиворечива. Это одно из первых математически содержательных утверждений, доказуемых в "обычной" математике, но недоказуемых в формальной арифметике Пеано ArP .

Для произвольных натуральных чисел k, m_1, \dots, m_k и t обозначим через $R(k, m_1, \dots, m_k, t)$ наименьшее из чисел $N(k, m_1, \dots, m_k, t)$, о которых идет речь в предыдущей теореме. Числа $R(k, m_1, \dots, m_k, t)$ носят название чисел Рамсея. С ними связан ряд нерешенных на сегодняшний день проблем. Но эта тема уже далеко выходит за рамки пособия.

Д о к а з а т е л ь с т в о. теоремы 3.9.9. Для произвольного натурального числа t через $S(t)$ обозначим множество всех подстановок чисел $\{1, 2, \dots, t\}$, т. е. множество всех биективных отображений этого множества чисел на себя.

Для произвольных фиксированных натуральных чисел k, m_1, \dots, m_k и t рассмотрим следующие формулы, в которых R, R_1, \dots, R_k — t -местные предикаты.

$$HE_t \Rightarrow (\forall x_1) \dots (\forall x_t) (R(x_1, \dots, x_t) \longrightarrow (\bigwedge_{\pi \in S(t)} R(x_{\pi(1)}, \dots, x_{\pi(t)}) \& \bigwedge_{1 \leq i < j \leq t} \neg x_i = x_j)).$$

$$P \Rightarrow (\forall x_1) \dots (\forall x_t) ((\bigvee_{i=1}^k P_i(x_1, \dots, x_t) \iff \bigwedge_{1 \leq i < j \leq t} \neg x_i = x_j) \& \neg((\exists x_1) \dots (\exists x_t) (\bigvee_{1 \leq i < j \leq t} (P_i(x_1, \dots, x_t) \& P_j(x_1, \dots, x_t)))))).$$

Заметим, что формула P задает на области интерпретации разбиение ее t -элементных подмножеств на k попарно непересекающихся классов, а формула HE_t гарантирует, что предикат $R(x_1, \dots, x_t)$ выделяет некоторые t -элементные подмножества (гиперребра размерности t).

Для произвольных натуральных чисел m и t обозначим через $PS(m, t)$ множество всех t -элементных подмножеств множества $\{1, 2, \dots, m\}$. Пусть G — это следующая формула

$$\bigvee_{i=1}^k (\exists x_1) \dots (\exists x_{m_i}) (\bigwedge_{1 \leq l < s \leq m_i} \neg x_l = x_s \& \bigwedge_{\{j_1, j_2, \dots, j_t\} \in PS(m_i, t)} P_i(x_{j_1}, x_{j_2}, \dots, x_{j_t})).$$

Обозначим через $\Phi(m_1, \dots, m_k, t)$ формулу $HE_t \& P \& G$.

В силу "бесконечной" теоремы Ф. Рамсея формула $\Phi(m_1, \dots, m_k, t)$ истинна на любой бесконечной системе $\langle M; R, P_1, \dots, P_k \rangle$, поэтому *эта формула логически следует из следующего бесконечного множества формул*

$$\{\mathcal{E}_1, \mathcal{E}_2, \dots, \mathcal{E}_m, \dots\},$$

где через \mathcal{E}_m обозначена формула $(\exists y_1) \dots (\exists y_m) (\bigwedge_{1 \leq i < j \leq m} \neg y_i = y_j)$, "содержательно утверждающая, что система содержит не менее чем m элементов". По теореме о локальном следствии существует такое число $N = N(k, m_1, \dots, m_k, t)$, что *формула $\Phi(m_1, \dots, m_k, t)$ логически следует из конечного множества формул*

$$\{\mathcal{E}_1, \mathcal{E}_2, \dots, \mathcal{E}_N\}.$$

Заметим, что тогда

$$\mathcal{E}_{N(k, m_1, \dots, m_k, t)} \models \Phi(m_1, \dots, m_k, t).$$

Значит, для произвольных натуральных чисел k, m_1, \dots, m_k и t существует такое число $N(k, m_1, \dots, m_k, t)$, что для произвольного множества V , содержащего

не менее, чем $N(k, m_1, \dots, m_k, t)$ элементов, и любых подмножеств W_1, \dots, W_k множества $[V]^t$ всех t -элементных подмножеств множества V таких, что

$$[V]^t = W_1 \cup \dots \cup W_k,$$

$$\text{при } 1 \leq i < j \leq k : \quad W_i \cap W_j = \emptyset,$$

найдется такое число i_0 ($1 \leq i_0 \leq k$) и такое подмножество U множества V , содержащее не менее, чем m_{i_0} элементов, что $[U]^t \subseteq W_{i_0}$, т. е. все t -элементные подмножества множества U содержатся в одном подмножестве W_{i_0} . \square

В заключение рассмотрим так называемую "обобщенную конечную" теорему Ф. Рамсея, которая занимает "промежуточное место" между следующими двумя вариантами "бесконечной" и "конечной" теорем Ф. Рамсея.

Теорема 3.9.10. *Для произвольных натуральных чисел k, m и t , произвольного бесконечного множества V натуральных чисел и любых непустых подмножеств W_1, \dots, W_k множества $[V]^t$ всех t -элементных подмножеств множества V таких, что*

$$V_t = W_1 \cup \dots \cup W_k,$$

$$\text{при } 1 \leq i < j \leq k : \quad W_i \cap W_j = \emptyset,$$

найдется такое бесконечное подмножество U множества V и такое число i_0 ($1 \leq i_0 \leq k$), что $[U]^t \subseteq W_{i_0}$, т. е. все t -элементные подмножества бесконечного множества U содержатся в одном и том же подмножестве W_{i_0} .

Теорема 3.9.11. *Для произвольных натуральных чисел k, m и t существует такое число $N(k, m, t)$, что для произвольного множества V натуральных чисел, содержащего не менее, чем $N(k, m, t)$ элементов, и любых непустых подмножеств W_1, \dots, W_k множества $[V]^t$ всех t -элементных подмножеств множества V таких, что*

$$[V]^t = W_1 \cup \dots \cup W_k,$$

$$\text{при } 1 \leq i < j \leq k : \quad W_i \cap W_j = \emptyset,$$

найдется такое число i_0 ($1 \leq i_0 \leq k$) и такое подмножество U множества V , содержащее не менее, чем m элементов, что $[U]^t \subseteq W_{i_0}$, т. е. все t -элементные подмножества множества U содержатся в одном и том же подмножестве W_{i_0} .

Для произвольного непустого множества V натуральных чисел через $\min(V)$ будем обозначать *наименьший элемент* множества V , а для произвольного конечного множества V натуральных чисел через $|V|$, как и выше, будем обозначать *число элементов* множества V .

Теорема 3.9.12 (Обобщенная конечная теорема Ф. Рамсея). *Для произвольных натуральных чисел k , m и t существует такое число $N(k, m, t)$, что для произвольного множества V натуральных чисел, содержащего не менее, чем $N(k, m, t)$ элементов, и любых непустых подмножеств W_1, \dots, W_k множества $[V]^t$ всех t -элементных подмножеств множества V таких, что*

$$[V]^t = W_1 \cup \dots \cup W_k,$$

$$\text{при } 1 \leq i < j \leq k: \quad W_i \cap W_j = \emptyset,$$

найдется такое число i_0 ($1 \leq i_0 \leq k$) и такое подмножество U множества V , содержащее не менее, чем m элементов, что $[U]^t \subseteq W_{i_0}$, т. е. все t -элементные подмножества множества U содержатся в одном и том же подмножестве W_{i_0} , и $\min(U) \leq |U|$.

Обобщенная конечная теорема Ф. Рамсея так же, как и "бесконечная" теорема Ф. Рамсея, может быть доказана с использованием теоретико-множественных методов. Это доказательство может быть проведено в рамках аксиоматической теории множеств, например, в системе ZFC . Однако такое доказательство невозможно в рамках системы ZFC_{fin} , полученной из системы ZFC удалением аксиомы бесконечности (конечно, при условии непротиворечивости последней системы).

Обобщенная конечная теорема Ф. Рамсея, может быть сформулирована на языке элементарной арифметики – в этой формулировке речь будет идти о натуральных числах, а не о их множествах и об операциях сложения и умножения натуральных чисел, а вместо конечных множеств натуральных чисел можно говорить об их *номерах*, используя для этого, например, функцию К. Геделя

$$\Gamma(a, b, i) = \text{rest}(a, 1 + (i + 1)b).$$

Однако доказательство такого варианта обобщенной конечной теоремы Ф. Рамсея не может быть проведено в формальной арифметике Пеано ArP , конечно, при условии (предположении) ее непротиворечивости.

Д о к а з а т е л ь с т в о. По чисто техническим причинам, в частности, чтобы продемонстрировать возможность проведения доказательства в рамках системы ZFC , удобно считать, что множество натуральных чисел включает число нуль 0, и рассматривать натуральные числа как множества, например, полагая

$$0 \hat{=} \emptyset, \quad n + 1 \hat{=} n \cup \{n\},$$

таким образом, $N + 1$ – это множество, состоящее из натуральных чисел 0, 1, ..., n .

Для фиксированных t и k рассмотрим все $N \geq t$.

При $N = t$ в N найдется лишь одно подмножество из t элементов и возможно k его распределений по k классам разбиения

$$[N]^t = W_1 \cup \dots \cup W_k.$$

Семейство множеств $(W_i)_{1 \leq i \leq k}$ будем называть разбиением множества $[N]^t$ или разбиением t -подмножеств множества N и обозначать одной буквой, например, P .

Построим бесконечное дерево с конечными ветвлениями, вершины которого будут помечены парами (N, P) , где P – разбиение t -подмножеств множества N на k классов.

В начальную вершину дерева помещаем t . Эту вершину соединяем с k вершинами, помеченными парами $(t, P_0^{(s)})$, где $s = 1, 2, \dots, k$.

Индуктивный переход от $N = \{0, 1, \dots, N-1\}$ к

$$N+1 = N \cup \{N\} = \{0, 1, \dots, N-1, N\}.$$

По каждой вершине (N, P) , где $P = (W_i)_{1 \leq i \leq k}$ – разбиение множества $[N]^t$, т. е. разбиение t -подмножеств множества N на k попарно непересекающихся классов

$$[N]^t = W_1 \cup \dots \cup W_k,$$

построим конечное множество новых вершин вида $(N+1, P')$, где

$$P' = (W'_i)_{1 \leq i \leq k} -$$

согласованное с разбиением P множества N разбиение множества

$$(N+1)_t,$$

т. е. такое разбиение t -подмножеств множества $N+1$ на k попарно непересекающихся классов

$$(N+1)_t = W'_1 \cup \dots \cup W'_k,$$

что при любом $1 \leq i \leq k$: $W_i \subseteq W'_i$. Разбиение P' получается из разбиения P размещением по классам t подмножеств множества $N+1$, имеющих вид $\{a_1, \dots, a_{t-1}, N\}$, где $\{a_1, \dots, a_{t-1}\} \subseteq N$. Число таких t -подмножеств равно $\binom{N}{t-1}$, а, значит, каждая вершина (N, P) порождает $k \binom{N}{t-1}$ новых вершин.

При фиксированных t и k каждая пара вида (N, P) , где $P = (W_i)_{1 \leq i \leq k}$ – разбиение множества $[N]^t$, встретится в качестве метки некоторой вершины построенного дерева.

Вершину (N, P) назовем "хорошей", если существует такое конечное подмножество $V \subseteq N$, содержащее не менее чем t элементов, что $\min(V) \leq |V|$ и все t -подмножества множества V содержатся в одном классе разбиения P . Если (N, P) – "хорошая" вершина, P' – согласованное с P разбиение множества $[(N+1)]^t$, то $(N+1, P')$ – "хорошая" вершина. Вершину, не являющуюся "хорошей", будем называть "плохой".

Покажем, что в построенном дереве лишь конечное число "плохих" вершин.

Предположим противное, т. е. что в этом дереве существует бесконечно много "плохих" вершин.

Если $(N + 1, P')$ – ”плохая” вершина, то и (N, P) – ”плохая” вершина, а так как построенное дерево имеет конечное ветвление, то каждый его уровень содержит конечное множество вершин, значит, существуют сколь угодно длинные конечные ветви, все вершины которых ”плохие”, поэтому по теореме Кёнига в этом дереве есть и бесконечная ветвь, все вершины которой ”плохие”.

Вершины этой бесконечной ветви помечены согласованными разбиениями (N, P_N) , которые задают некоторое разбиение $P^* = (W_i^*)_{1 \leq i \leq k}$ множества всех t -элементных подмножеств множества \mathcal{N} всех натуральных чисел:

если $\{a_1, a_2, \dots, a_t\}$ – t -элементное подмножество множества \mathcal{N} всех натуральных чисел, $N = \max(a_1, a_2, \dots, a_t)$, то $\{a_1, a_2, \dots, a_t\} \subseteq N + 1$ и разбиение P_{N+1} t -элементных подмножеств множества $N + 1$ определяет, какому из классов разбиения $P^ = (W_i^*)_{1 \leq i \leq k}$ множества всех t -элементных подмножеств множества \mathcal{N} всех натуральных чисел принадлежит подмножество $\{a_1, a_2, \dots, a_t\}$. Корректность этого определения следует из согласованности разбиений $P_{N+2}, P_{N+3}, P_{N+4}, \dots$.*

Применим к разбиению $P^* = (W_i^*)_{1 \leq i \leq k}$ множества всех t -элементных подмножеств множества \mathcal{N} всех натуральных чисел ”бесконечную” теорему Ф. Рамсея, получим бесконечное множество U натуральных чисел, все t -элементные подмножества которого содержатся в одном классе разбиения P^* . Выбираем в U конечное подмножество V такое, что

$$\min(V) \leq |V|, \quad m \leq |V|.$$

Полагаем $N = \max(V)$. Тогда $V \subseteq N + 1$ и все t -элементные подмножества множества V содержатся в одном классе разбиения P_{N+1} . Что противоречит условию $(N + 1, P_{N+1})$ – ”плохая” вершина.

Значит, в построенном дереве лишь конечное число ”плохих” вершин. Поэтому начиная с некоторого уровня все вершины ”хорошие”. Номер любого такого уровня можно взять в качестве числа $N(k, m, t)$.

Это завершает доказательство обобщенной конечной теоремы Ф. Рамсея. \square

В качестве применения конечной теоремы Рамсея, рассмотрим следующее утверждение, носящее название ”Теорема Шура” [3].

Если каждое натуральное число ”окрашено” в один из k ”цветов”, то найдутся три такие натуральных числа a, b и c , что они ”окрашены” в один ”цвет” и $a + b = c$.

”Окрасим” каждое 2-элементное множество $\{u, v\}$ ($u < v$) тем же ”цветом”, которым ”окрашено” натуральное число $v - u$.

Применим теорему Рамсея к рассматриваемой ситуации, т. е. при $m = 3$ и $t = 2$. Существует такое число $n = N(k, 3, 2) \geq 3$, что во множестве

$$N_n = \{0, 1, \dots, n - 1\}$$

натуральных чисел найдется такое подмножество U , содержащее 3 элемента, что все элементы из U_2 одного ”цвета”.

Возьмем в U три элемента i, j и l . Пусть $i < j < l$.

Тогда 2-элементные множества $\{i, j\}$, $\{i, l\}$ и $\{j, l\}$ одного "цвета". Значит, числа $a = j - i$, $b = l - j$ и $c = l - i$ одного "цвета" и $a + b = c$.

3.10. Разрешимость логики одноместных предикатов

В этом параграфе мы рассмотрим один из простейших вариантов *Логике предикатов* – *Логике одноместных предикатов*, которая также называется *Монадической логикой предикатов* или просто *Монадической логикой*.

Сигнатура Монадической логики предикатов, которую мы будем обозначать через $\tau_{м.л.}$, содержит лишь одноместные предикатные символы. Она имеет вид

$$\tau_{м.л.} = \langle \emptyset, \emptyset, P, \theta, \varphi \rangle,$$

т. е. множество C *символов индивидуальных констант* и множество F *функциональных символов* пусты, а множество P *предикатных символов* состоит лишь из одноместных предикатных символов: если $p \in P$, то $\varphi(p) = 1$.

Проблема тождественной истинности для Логике Предикатов сигнатуры τ . Для произвольной замкнутой формулы *Логике Предикатов сигнатуры τ* определить, является ли она тождественно истинной.

Проблема выполнимости для Логике предикатов сигнатуры τ . Для произвольной замкнутой формулы *Логике Предикатов сигнатуры τ* определить, является ли она выполнимой.

Так как для произвольной замкнутой формулы Φ любой сигнатуры имеют место эквивалентности

формула Φ является тождественно истинной тогда и только тогда, когда формула $(\neg\Phi)$ не является выполнимой,

формула Φ является выполнимой тогда и только тогда, когда формула $(\neg\Phi)$ не является тождественно истинной,

то **Проблема тождественной истинности для Логике Предикатов сигнатуры τ** алгоритмически разрешима тогда и только тогда, когда алгоритмически разрешима **Проблема выполнимости для Логике Предикатов сигнатуры τ** .

Теорема 3.10.1. *Проблема тождественной истинности и Проблема выполнимости для замкнутых формул Монадической Логике Предикатов алгоритмически разрешимы.*

Так как **Проблема тождественной истинности для монадической логики предикатов** алгоритмически разрешима тогда и только тогда,

когда алгоритмически разрешима **Проблема выполнимости для монадической логики предикатов**, то достаточно доказать алгоритмическую разрешимость **Проблемы выполнимости для монадической логики предикатов**.

Доказательство разобьем на несколько лемм.

Лемма. Если все входящие в замкнутую формулу Φ Монадической Логике Предикатов предикатные символы содержатся в списке p_1, \dots, p_n , то

формула Φ истинна в некоторой интерпретации тогда и только тогда, когда она истинна в некоторой интерпретации, основное множество которой содержит не более, чем 2^n элементов.

Д о к а з а т е л ь с т в о. Очевидно достаточно доказать, что если формула Φ истинна в некоторой интерпретации, то она истинна в некоторой интерпретации, основное множество которой содержит не более, чем 2^n элементов.

Пусть формула Φ истинна в интерпретации I с основным множеством A . Чтобы несколько упростить обозначения, будем имя \bar{a} элемента a основного множества A обозначать просто через a .

На множестве A введем отношение эквивалентности \equiv , полагая для произвольных его элементов a и b :

$$a \equiv b \iff$$

$$I(p_1)(a) = I(p_1)(b) \& \dots \& I(p_n)(a) = I(p_n)(b).$$

Легко понять, что отношение \equiv действительно является отношением эквивалентности, т. е. оно рефлексивно, симметрично и транзитивно.

Обозначим через A_1 фактормножество A/\equiv множества A по отношению эквивалентности \equiv .

Через τ_1 обозначим сигнатуру монадической логики предикатов с пустыми множествами индивидных констант и функциональных символов и множеством предикатных символов $P_1 = \{p_1, \dots, p_n\}$, т. е. в P_1 входят лишь те предикатные символы из P , которые входят в формулу Φ .

Построим интерпретацию I_1 с основным множеством A_1 языка L_{τ_1} . Для этого достаточно задать предикаты $I_1(p_1), \dots, I_1(p_n)$.

Для любого i ($1 \leq i \leq n$) и произвольного $[a] \in A_1$ полагаем

$$I_1(p_i)([a]) = I(p_i)(a).$$

Легко понять, что определение корректно, т. е. не зависит от выбора представителя в классе эквивалентности.

Индукцией по построению формул докажем, что для любой формулы Ψ языка L_{τ_1} , все свободные переменные которой содержатся в списке x_1, \dots, x_k , и для произвольных элементов a_1, \dots, a_k множества A выполняется равенство

$$I_1(\Psi_{x_1, \dots, x_k} [[a_1], \dots, [a_k]]) = I(\Psi_{x_1, \dots, x_k} [a_1, \dots, a_k]).$$

База индукции.

Пусть Ψ – элементарная формула языка L_{τ_1} . Тогда она имеет вид $p_i(x_j)$ для некоторых i ($1 \leq i \leq n$) и j ($1 \leq j \leq k$). Доказываемое равенство в этом случае следует из равенств

$$\begin{aligned} I_1(\Psi_{x_1, \dots, x_k} [[a_1], \dots, [a_k]]) &= I_1(p_i(x_j)_{x_1, \dots, x_k} [[a_1], \dots, [a_k]]) = \\ &= I_1(p_i([a_j])) = I_1(p_i)([a_j]) = \\ &= I(p_i)(a_j) = I(p_i(a_j)) = \\ &= I(p_i(x_j)_{x_1, \dots, x_k} [a_1, \dots, a_k]) = I(\Psi_{x_1, \dots, x_k} [a_1, \dots, a_k]). \end{aligned}$$

Индуктивный переход.

Пусть формула Ψ имеет один из следующих видов

$$(\neg \mathcal{A}), (\mathcal{A} \& \mathcal{B}), (\mathcal{A} \vee \mathcal{B}), (\mathcal{A} \rightarrow \mathcal{B}), (\forall x_t) \mathcal{A}, (\exists x_t) \mathcal{A}.$$

Для первых трех случаев доказательства следуют из индуктивного предположения и следующих равенств, в которых через \circ обозначена любая из трех пропозициональных связок $\&$, \vee , \rightarrow ,

$$\begin{aligned} I_1((\neg \mathcal{A})_{x_1, \dots, x_k} [[a_1], \dots, [a_k]]) &= I_1((\neg \mathcal{A}_{x_1, \dots, x_k} [[a_1], \dots, [a_k]])) = \\ &= H_{\neg}(I_1(\mathcal{A}_{x_1, \dots, x_k} [[a_1], \dots, [a_k]])) = H_{\neg}(I(\mathcal{A}_{x_1, \dots, x_k} [a_1, \dots, a_k])) = \\ &= I((\neg \mathcal{A}_{x_1, \dots, x_k} [a_1, \dots, a_k])) = I((\neg \mathcal{A})_{x_1, \dots, x_k} [a_1, \dots, a_k]); \\ I_1((\mathcal{A} \circ \mathcal{B})_{x_1, \dots, x_k} [[a_1], \dots, [a_k]]) &= \\ &= I_1((\mathcal{A}_{x_1, \dots, x_k} [[a_1], \dots, [a_k]] \circ \mathcal{B}_{x_1, \dots, x_k} [[a_1], \dots, [a_k]])) = \\ &= H_{\circ}(I_1(\mathcal{A}_{x_1, \dots, x_k} [[a_1], \dots, [a_k]]), I_1(\mathcal{B}_{x_1, \dots, x_k} [[a_1], \dots, [a_k]])) = \\ &= H_{\circ}(I(\mathcal{A}_{x_1, \dots, x_k} [a_1, \dots, a_k]), I(\mathcal{B}_{x_1, \dots, x_k} [a_1, \dots, a_k])) = \\ &= I((\mathcal{A}_{x_1, \dots, x_k} [a_1, \dots, a_k] \circ \mathcal{B}_{x_1, \dots, x_k} [a_1, \dots, a_k])) = \\ &= I((\mathcal{A} \circ \mathcal{B})_{x_1, \dots, x_k} [a_1, \dots, a_k]). \end{aligned}$$

Остается рассмотреть случаи, когда формула Ψ имеет один из следующих двух видов

$$(\forall x_t) \mathcal{A}, (\exists x_t) \mathcal{A}.$$

Чтобы не усложнять обозначения, без ограничения общности можно считать, что $k < t$.

Тогда

$$\begin{aligned} I_1((\forall x_t) \mathcal{A}_{x_1, \dots, x_k} [[a_1], \dots, [a_k]]) &= \text{И} \iff \\ &\text{для любого } [a] \text{ из } A_1 : I_1((\mathcal{A}_{x_1, \dots, x_k} [[a_1], \dots, [a_k]])_{x_t} [[a]]) = \text{И}, \end{aligned}$$

$$\begin{aligned} I((\forall x_t) \mathcal{A}_{x_1, \dots, x_k} [a_1, \dots, a_k]) &= \text{И} \iff \\ &\text{для любого } a \text{ из } A : I((\mathcal{A}_{x_1, \dots, x_k} [a_1, \dots, a_k])_{x_t} [a]) = \text{И}. \end{aligned}$$

Остается заметить, что при сделанных предположениях

$$(\mathcal{A}_{x_1, \dots, x_k} [[a_1], \dots, [a_k]])_{x_t} [[a]] = (\mathcal{A}_{x_1, \dots, x_k, x_t} [[a_1], \dots, [a_k], [a]]),$$

$$(\mathcal{A}_{x_1, \dots, x_k} [a_1, \dots, a_k])_{x_t} [a] = (\mathcal{A}_{x_1, \dots, x_k, x_t} [a_1, \dots, a_k, a])$$

и по индуктивному предположению

$$I_1((\mathcal{A}_{x_1, \dots, x_k, x_t} [[a_1], \dots, [a_k], [a]])) = I((\mathcal{A}_{x_1, \dots, x_k, x_t} [a_1, \dots, a_k, a])).$$

Кроме того, следует учесть, что когда класс $[a]$ ”пробегают” все множество A_1 , его представители a ”пробегают” все множество A .

Случай, когда формула Ψ имеет вид $(\exists x_t)\mathcal{A}$, рассматривается совершенно аналогично.

В частности, для рассматриваемой формулы Φ получаем равенства

$$I_1(\Phi) = I(\Phi) = \text{И}.$$

Значит, формула Φ истинна в интерпретации I_1 , основное множество A_1 которой содержит не более, чем 2^n элементов. \square

Лемма. Если замкнутая формула Φ **логики предикатов** произвольной сигнатуры τ истинна в некоторой интерпретации I с основным множеством A и $A \subseteq B$, то Φ истинна в некоторой интерпретации \hat{I} с основным множеством B .

Доказательство. Зафиксируем во множестве A некоторый элемент a . Для каждого элемента b из множества B определим элемент \hat{b} из множества A следующими равенствами

$$\hat{b} = \begin{cases} b, & \text{если } b \in A; \\ a, & \text{если } b \in (B \setminus A). \end{cases}$$

По интерпретации I с основным множеством A языка $L_\tau(A)$ произвольной сигнатуры τ построим интерпретацию \hat{I} с основным множеством B языка $L_\tau(B)$, полагая:

если c - символ индивидуальной константы сигнатуры τ , то полагаем $\hat{I}(c) = I(c)$,

если \bar{b} - имя элемента из множества B , то полагаем $\hat{I}(\bar{b}) = I(\hat{b})$,

если f - n -местный функциональный символ сигнатуры τ , а b_1, \dots, b_n - произвольные элементы множества B , то полагаем

$$\hat{I}(f)(b_1, \dots, b_n) = I(f)(\hat{b}_1, \dots, \hat{b}_n),$$

если p - n -местный предикатный символ сигнатуры τ , а b_1, \dots, b_n - произвольные элементы множества B , то полагаем

$$\hat{I}(p)(b_1, \dots, b_n) = I(p)(\hat{b}_1, \dots, \hat{b}_n).$$

Заметим, что

$$\widehat{I(f)(b_1, \dots, b_n)} = I(f)(\hat{b}_1, \dots, \hat{b}_n).$$

Индукцией по построению термов докажем, что для любого терма t языка L_τ сигнатуры τ , все свободные переменные которого содержатся в списке x_1, \dots, x_k , и любых элементов b_1, \dots, b_k множества B выполняется равенство

$$\hat{I}(t_{x_1, \dots, x_k} [b_1, \dots, b_k]) = I(t_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k]).$$

База индукции.

Если t - это символ c индивидуальной константы сигнатуры τ , то

$$\hat{I}(t_{x_1, \dots, x_k} [b_1, \dots, b_k]) = \hat{I}(c) = I(c) = I(t_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k]).$$

Если t - это имя \bar{b} элемента b множества B , то

$$\hat{I}(t_{x_1, \dots, x_k} [b_1, \dots, b_k]) = \hat{I}(\bar{b}) = I(\hat{b}) = I(t_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k]).$$

Если t - это индивидуальная переменная x_i , то

$$\hat{I}(t_{x_1, \dots, x_k} [b_1, \dots, b_k]) = \hat{I}(x_i) = I(\hat{x}_i) = I(t_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k]).$$

Индуктивный переход.

Пусть терм t имеет вид $f(t_1, \dots, t_n)$, где f - n -местный функциональный символ сигнатуры τ , а t_1, \dots, t_n - термы. Воспользовавшись индуктивным предположением, получим равенства

$$\begin{aligned} \hat{I}(t_{x_1, \dots, x_k} [b_1, \dots, b_k]) &= \hat{I}(f(t_1, \dots, t_n)_{x_1, \dots, x_k} [b_1, \dots, b_k]) = \\ &= \hat{I}(f((t_1)_{x_1, \dots, x_k} [b_1, \dots, b_k], \dots, (t_n)_{x_1, \dots, x_k} [b_1, \dots, b_k])) = \\ &= \hat{I}(f)(\hat{I}((t_1)_{x_1, \dots, x_k} [b_1, \dots, b_k]), \dots, \hat{I}((t_n)_{x_1, \dots, x_k} [b_1, \dots, b_k])) = \\ &= \hat{I}(f)(I((t_1)_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k]), \dots, I((t_n)_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k])) = \\ &= I(f)(I((t_1)_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k]), \dots, I((t_n)_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k])) = \\ &= I(f((t_1)_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k], \dots, (t_n)_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k])) = \\ &= I(f(t_1, \dots, t_n)_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k])) = \\ &= I(t_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k]). \end{aligned}$$

Индукцией по построению формул докажем, что для любой формулы Ψ языка L_τ , все свободные переменные которой содержатся в списке x_1, \dots, x_k , и для произвольных элементов b_1, \dots, b_k множества B выполняется равенство

$$\hat{I}(\Psi_{x_1, \dots, x_k} [b_1, \dots, b_k]) = I(\Psi_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k]).$$

База индукции.

Пусть Ψ - элементарная формула языка L_τ . Тогда она имеет вид $p(t_1, \dots, t_m)$, где p - n -местный предикатный символ, а t_1, \dots, t_m - термы.

Система равенств

$$\begin{aligned} p(t_1, \dots, t_m)_{x_1, \dots, x_k} [b_1, \dots, b_k] &= \\ p((t_1)_{x_1, \dots, x_k} [b_1, \dots, b_k], \dots, (t_m)_{x_1, \dots, x_k} [b_1, \dots, b_k]); \\ p(t_1, \dots, t_m)_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k] &= \\ p((t_1)_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k], \dots, (t_m)_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k]) \end{aligned}$$

дает систему равенств

$$\begin{aligned} \hat{I}(p(t_1, \dots, t_m)_{x_1, \dots, x_k} [b_1, \dots, b_k]) &= \\ \hat{I}(p((t_1)_{x_1, \dots, x_k} [b_1, \dots, b_k], \dots, (t_m)_{x_1, \dots, x_k} [b_1, \dots, b_k])) &= \\ \hat{I}(p)(\hat{I}((t_1)_{x_1, \dots, x_k} [b_1, \dots, b_k]), \dots, \hat{I}((t_m)_{x_1, \dots, x_k} [b_1, \dots, b_k])) &= \\ \hat{I}(p)(I((t_1)_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k]), \dots, I((t_m)_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k])) &= \\ I(p)(I((t_1)_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k]), \dots, I((t_m)_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k])) &= \\ I(p((t_1)_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k], \dots, (t_m)_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k])) &= \\ I(p(t_1, \dots, t_m)_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k]). \end{aligned}$$

Индуктивный переход.

Пусть формула Ψ имеет один из следующих видов

$$(\neg \mathcal{A}), (\mathcal{A} \& \mathcal{B}), (\mathcal{A} \vee \mathcal{B}), (\mathcal{A} \rightarrow \mathcal{B}), (\forall x_t) \mathcal{A}), (\exists x_t) \mathcal{A}).$$

Для первых трех случаев доказательства следуют из индуктивного предположения и следующих равенств, в которых через \circ обозначена любая из трех пропозициональных связок $\&$, \vee , \rightarrow ,

$$\begin{aligned} \hat{I}((\neg \mathcal{A})_{x_1, \dots, x_k} [b_1, \dots, b_k]) &= \hat{I}((\neg \mathcal{A})_{x_1, \dots, x_k} [b_1, \dots, b_k]) = \\ H_{\neg}(\hat{I}(\mathcal{A}_{x_1, \dots, x_k} [b_1, \dots, b_k])) &= H_{\neg}(I(\mathcal{A}_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k])) = \\ I((\neg \mathcal{A})_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k])) &= I((\neg \mathcal{A})_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k])); \\ \hat{I}((\mathcal{A} \circ \mathcal{B})_{x_1, \dots, x_k} [b_1, \dots, b_k]) &= \\ \hat{I}((\mathcal{A}_{x_1, \dots, x_k} [b_1, \dots, b_k] \circ \mathcal{B}_{x_1, \dots, x_k} [b_1, \dots, b_k])) &= \\ H_{\circ}(\hat{I}(\mathcal{A}_{x_1, \dots, x_k} [b_1, \dots, b_k]), \hat{I}(\mathcal{B}_{x_1, \dots, x_k} [b_1, \dots, b_k])) &= \\ H_{\circ}(I(\mathcal{A}_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k]), I(\mathcal{B}_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k])) &= \\ I((\mathcal{A}_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k] \circ \mathcal{B}_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k])) &= \\ I((\mathcal{A} \circ \mathcal{B})_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k]). \end{aligned}$$

Остается рассмотреть случаи, когда формула Ψ имеет один из следующих двух видов

$$(\forall x_t) \mathcal{A}), (\exists x_t) \mathcal{A}).$$

Чтобы не усложнять обозначения, без ограничения общности можно считать, что $k < t$.

Допустим, что

$$\hat{I}((\forall x_t)\mathcal{A}_{x_1, \dots, x_k} [b_1, \dots, b_k]) = \text{И}.$$

Тогда для любого элемента b из множества B выполняется равенство:

$$\hat{I}((\mathcal{A}_{x_1, \dots, x_k} [b_1, \dots, b_k])_{x_t} [b]) = \text{И},$$

Так как

$$(\mathcal{A}_{x_1, \dots, x_k} [b_1, \dots, b_k])_{x_t} [b] = \mathcal{A}_{x_1, \dots, x_k, x_t} [b_1, \dots, b_k, b],$$

то, используя индуктивное предположение, получаем

$$\begin{aligned} \text{И} &= \hat{I}((\mathcal{A}_{x_1, \dots, x_k} [b_1, \dots, b_k])_{x_t} [b]) = \\ &= \hat{I}(\mathcal{A}_{x_1, \dots, x_k, x_t} [b_1, \dots, b_k, b]) = \\ &= I(\mathcal{A}_{x_1, \dots, x_k, x_t} [\hat{b}_1, \dots, \hat{b}_k, \hat{b}]) = \\ &= I((\mathcal{A}_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k])_{x_t} [\hat{b}]). \end{aligned}$$

В частности, для любого элемента c множества A получаем

$$\text{И} = I((\mathcal{A}_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k])_{x_t} [\hat{c}]) = I((\mathcal{A}_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k])_{x_t} [c]),$$

так как в этом случае $\hat{c} = c$.

Допустим, что

$$I((\forall x_t)\mathcal{A}_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k]) = \text{И}.$$

Пусть b - произвольный элемент множества B . Так как $\hat{b} \in A$, то выполняются равенства

$$\begin{aligned} \text{И} &= I((\mathcal{A}_{x_1, \dots, x_k} [\hat{b}_1, \dots, \hat{b}_k])_{x_t} [\hat{b}]) = \\ &= I(\mathcal{A}_{x_1, \dots, x_k, x_t} [\hat{b}_1, \dots, \hat{b}_k, \hat{b}]) = \\ &= \hat{I}(\mathcal{A}_{x_1, \dots, x_k, x_t} [b_1, \dots, b_k, b]) = \\ &= \hat{I}((\mathcal{A}_{x_1, \dots, x_k} [b_1, \dots, b_k])_{x_t} [b]), \end{aligned}$$

значит,

$$\hat{I}((\forall x_t)\mathcal{A}_{x_1, \dots, x_k} [b_1, \dots, b_k]) = \text{И}.$$

Случай, когда формула Ψ имеет вид $(\exists x_t)\mathcal{A}$, рассматривается совершенно аналогично.

В частности, для произвольной замкнутой формулы Φ **логики предикатов** произвольной сигнатуры τ получаем равенство

$$I(\Phi) = \hat{I}(\Phi),$$

а значит, если $I(\Phi) = \text{И}$, то $\hat{I}(\Phi) = \text{И}$. □

В качестве следствия двух предыдущих лемм получаем

Лемма. Если все входящие в замкнутую формулу Φ **Монадической Логике Предикатов** предикатные символы содержатся в списке p_1, \dots, p_n , то

формула Φ истинна в некоторой интерпретации тогда и только тогда, когда она истинна в некоторой интерпретации, основное множество которой содержит 2^n элементов.

Так как при построении интерпретаций природа элементов основного множества не играет роли, то можно считать, что если I – интерпретация с конечным основным множеством A , состоящим из m элементов, то $A = \{1, 2, \dots, m\}$.

Лемма. Если все входящие в замкнутую формулу Φ **Монадической Логике Предикатов** предикатные символы содержатся в списке p_1, \dots, p_n , то можно построить такую формулу $\hat{\Phi}$ **Логике Высказываний**, что

формула Φ выполнима тогда и только тогда, когда выполнима формула $\hat{\Phi}$.

Д о к а з а т е л ь с т в о. Пусть $m = 2^n$ и $A_m = \{1, 2, \dots, m\}$. По произвольной формуле Φ сигнатуры $\tau(A_m)$ построим бескванторную формулу Φ^* той же сигнатуры по следующим правилам

- 1) если Φ – элементарная формула, то Φ^* – это Φ ,
- 2) $(\neg\Phi)^* = (\neg\Phi^*)$,
- 3) $(\Phi \vee \Psi)^* = (\Phi^* \vee \Psi^*)$,
- 4) $(\Phi \& \Psi)^* = (\Phi^* \& \Psi^*)$,
- 5) $(\Phi \rightarrow \Psi)^* = (\Phi^* \rightarrow \Psi^*)$,
- 6) $((\exists x)\Phi)^* = \bigvee_{j=1}^m \Phi_x[j]$,
- 7) $((\forall x)\Phi)^* = \big\&_{j=1}^m \Phi_x[j]$.

Из замкнутой формулы Φ^* формула $\hat{\Phi}$ получается заменой каждой элементарной подформулы вида $p_i(j)$ на пропозициональную переменную $A_{i,j}$.

Используя доказанные выше леммы, нетрудно показать, что замкнутая формула Φ **Монадической Логике Предикатов** выполнима тогда и только тогда, когда выполнима формула **Логике Высказываний** $\hat{\Phi}$. \square

Доказательство теоремы 3.10.1 получается как непосредственное следствие доказанных лемм.

3.11. Неразрешимость логики двуместных предикатов

Этот параграф посвящен доказательству фундаментальной теоремы А. Черча о неразрешимости **Проблемы тождественной истинности для Логике Предикатов**, сигнатура которой содержит хотя бы один двуместный предикатный символ. Как уже отмечалось выше, разрешимость **Проблемы**

тождественной истинности для Логике Предикатов сигнатуры τ равносильна разрешимости **Проблемы выполнимости для Логике Предикатов сигнатуры τ** .

Это был исторически первый пример алгоритмически неразрешимой проблемы, возникшей в математике вне теории алгоритмов и даже до ее создания. **Проблема выполнимости для Логике Предикатов** была сформулирована в начале XX века Д. Гильбертом после создания логики предикатов первого порядка и оставалась нерешенной в течение нескольких лет. Она получила название *проблемы разрешимости* (Entscheidungsproblem) логики (исчисления) предикатов. Невозможность построения алгоритма, решающего **Проблему выполнимости для Логике Предикатов** была доказана А. Черчем в 1936 году.

Теорема 3.11.1. *Невозможен алгоритм, позволяющий по произвольной замкнутой формуле логики предикатов первого порядка с равенством, алфавит которой содержит 2-местный функциональный символ, определить, является ли эта формула тождественно истинной.*

Доказательство. Обозначим через \cdot двуместный функциональный символ, входящий по предположению в алфавит рассматриваемого исчисления предикатов первого порядка с равенством.

Пусть Π - конечно определенная полугруппа с двумя образующими элементами, имеющая алгоритмически неразрешимую проблему равенства слов [12]:

$$\Pi = \langle a_1, a_2 \mid A_1(a_1, a_2) = B_1(a_1, a_2), \dots, A_m(a_1, a_2) = B_m(a_1, a_2) \rangle.$$

Каждое слово $W = w_1 w_2 w_3 \dots w_n$ мы рассматриваем как терм

$$(\dots((w_1 \cdot w_2) \cdot w_3) \cdot \dots) \cdot w_n,$$

который, чтобы не усложнять обозначений, будем по-прежнему обозначать через W .

Для произвольных двух слов $U(a_1, a_2)$ и $V(a_1, a_2)$ в алфавите $\{a_1, a_2\}$ обозначим через $\Phi_{U,V}$ следующую формулу

$$(\forall x_1)(\forall x_2)((\forall x)(\forall y)(\forall z)x \cdot (y \cdot z) = (x \cdot y) \cdot z \rightarrow (\bigwedge_{i=1}^m A_i(x_1, x_2) = B_i(x_1, x_2) \rightarrow U(x_1, x_2) = V(x_1, x_2))).$$

Нетрудно понять, что имеет место следующая эквивалентность

$$U(a_1, a_2) = V(a_1, a_2) \text{ в полугруппе } \Pi \iff \text{формула } \Phi_{U,V} \text{ тождественно истинна.}$$

Напомним, что тождественная истинность формулы $\Phi_{U,V}$ означает, что она истинна в любой **нормальной интерпретации**. Это завершает доказательство теоремы 3.11.1. \square

Покажем, что аналогичная теорема справедлива и для *чистого* исчисления предикатов первого порядка с равенством, т. е. исчисления, алфавит которого не содержит функциональных символов.

Предположим, что алфавит чистого исчисления предикатов первого порядка содержит 3-местный предикатный символ p .

Обозначим через $F_{U,V}$ следующую формулу

$$(\forall x_1)(\forall x_2)(\exists y)(\forall y_1)(p(x_1, x_2, y) \& (p(x_1, x_2, y_1) \rightarrow y_1 = y)) \rightarrow (\Phi_{U,V})^*,$$

где для произвольной формулы Φ через Φ^* обозначена формула, полученная заменой функционального символа \cdot на предикатный символ p по следующему правилу:

1. по формуле Φ строим равносильную ей формулу Φ_1 заменой в формуле Φ каждой подформулы вида $t_1 = t_2$, где t_1, t_2 - термы, на равносильную ей формулу вида

$$(\exists v_1)(\exists v_2) \dots (\exists v_q) \Psi, \text{ где } \Psi = \big\&_{i=1}^k \varphi_i$$

и каждая из формул φ_i имеет вид $x \cdot y = z$;

2. по формуле Φ_1 строим формулу Φ^* заменой в формуле Φ_1 каждой подформулы вида $x \cdot y = z$ на формулу $p(x, y, z)$.

Нетрудно понять, что имеет место следующая эквивалентность

$$U(a_1, a_2) = V(a_1, a_2) \text{ в полугруппе } \Pi \iff \text{формула } F_{U,V} \text{ тождественно истинна.}$$

И здесь тождественная истинность формулы $F_{U,V}$ означает, что она истинна в любой **нормальной интерпретации**.

Покажем, как можно от нормальных интерпретаций перейти к произвольным интерпретациям.

Заметим, что формула $F_{U,V}$ содержит 3-местный предикатный символ p и предикат равенства $=$, при этом для любой нормальной интерпретации I с основным множеством A : $I(=)$ - это обычное равенство на A .

Пусть E - новый 2-местный предикатный символ.

Обозначим через $AxEq$ конъюнкцию следующих замкнутых формул

$$\begin{aligned} &(\forall x)E(x, x); \quad (\forall x)(\forall y)(E(x, y) \rightarrow E(y, x)); \\ &(\forall x)(\forall y)(\forall z)((E(x, y) \& E(y, z)) \rightarrow E(x, z)); \\ &(\forall x_1)(\forall y_1)(\forall x_2)(\forall y_2)(\forall x_3)(\forall y_3)((E(x_1, y_1) \& E(x_2, y_2) \& E(x_3, y_3)) \rightarrow \\ &\quad (p(x_1, x_2, x_3) \longleftrightarrow p(y_1, y_2, y_3))). \end{aligned}$$

Для произвольной формулы F , содержащей из нелогических связок лишь 3-местный предикатный символ p и предикат равенства $=$, обозначим через F^+

формулу, полученную из формулы F заменой каждой элементарной подформулы вида $x = y$ на $E(x, y)$.

Введем временные обозначения:

через τ_{\equiv} обозначим сигнатуру с пустым множеством индивидных символов, пустым множеством функциональных символов, множество предикатных символов которой содержит лишь 3-местный предикатный символ p и предикат равенства $=$, а через τ_E – сигнатуру, полученную из сигнатуры τ_{\equiv} заменой 2-местного предикатного символа $=$ на 2-местный предикатный E .

Лемма. *Замкнутая формула F сигнатуры τ_{\equiv} истинна в любой нормальной интерпретации тогда и только тогда, когда замкнутая формула сигнатуры τ_E $(AxEq \rightarrow F^+)$ истинна в любой интерпретации.*

Д о к а з а т е л ь с т в о. Предположим, что замкнутая формула

$$(AxEq \rightarrow F^+)$$

истинна в любой интерпретации языка L_{τ_E} .

Покажем, что замкнутая формула F истинна в любой нормальной интерпретации языка $L_{\tau_{\equiv}}$.

Пусть I_{\equiv} – произвольная нормальная интерпретация с основным множеством A языка $L_{\tau_{\equiv}}$ сигнатуры τ_{\equiv} .

Построим интерпретацию I_E с тем же основным множеством A языка L_{τ_E} сигнатуры τ_E . Полагаем

$$I_E(p) = I_{\equiv}(p), \quad I_E(E) = I_{\equiv}(=A),$$

где через $=_A$ обозначено обычное равенство на множестве A .

Индукцией по построению формул нетрудно доказать, что для произвольной замкнутой формулы Φ сигнатуры τ_{\equiv} выполняется равенство

$$I_E(\Phi^+) = I_{\equiv}(\Phi).$$

Так как по предположению замкнутая формула $(AxEq \rightarrow F^+)$ истинна в любой интерпретации языка L_{τ_E} , то

$$I_E((AxEq \rightarrow F^+)) = \text{И.}$$

Из построения интерпретации I_E следует, что

$$I_E(AxEq) = \text{И.}$$

Поэтому

$$I_E(F^+) = \text{И.}$$

Значит,

$$I_{\equiv}(F) = \text{И.}$$

Предположим, что замкнутая формула F истинна в любой нормальной интерпретации языка $L_{\tau=}$.

Покажем, что замкнутая формула $(AxEq \rightarrow F^+)$ истинна в любой интерпретации языка L_{τ_E} .

Пусть I – произвольная интерпретация языка L_{τ_E} с основным множеством A .

Если $I(AxEq) = \mathbb{I}$, то, конечно,

$$I((AxEq \rightarrow F^+)) = \mathbb{I}$$

Предположим, что $I(AxEq) = \mathbb{I}$. Тогда

$$I((\forall x)E(x, x) \& (\forall x)(\forall y)(E(x, y) \rightarrow E(y, x)) \& (\forall x)(\forall y)(\forall z)((E(x, y) \& E(y, z)) \rightarrow E(x, z))) = \mathbb{I},$$

значит, $I(E)$ – отношение эквивалентности на множестве A . Обозначим $I(E)$ через \equiv , а через A_1 фактормножество A/\equiv множества A по отношению эквивалентности \equiv .

Построим интерпретацию I_1 языка L_{τ_E} с основным множеством A_1 .

Полагаем, что $I_1(E)$ – это обычное равенство на основном множестве A_1 . Остается лишь задать интерпретацию $I_1(p)$ 3-местного предикатного символа p .

Полагаем для произвольных элементов $[a_1]$, $[a_2]$ и $[a_3]$ основного множества A_1

$$I_1(p)([a_1], [a_2], [a_3]) = I(p)(a_1, a_2, a_3).$$

Корректность определения следует из следующего замечания.

Так как

$$I((\forall x_1)(\forall y_1)(\forall x_2)(\forall y_2)(\forall x_3)(\forall y_3)((E(x_1, y_1) \& E(x_2, y_2) \& E(x_3, y_3)) \rightarrow (p(x_1, x_2, x_3) \longleftrightarrow p(y_1, y_2, y_3)))) = \mathbb{I},$$

то из $a_1 \equiv b_1$, $a_2 \equiv b_2$ и $a_3 \equiv b_3$ следует, что

$$I(p)(a_1, a_2, a_3) = I(p)(b_1, b_2, b_3).$$

Индукцией по построению формул нетрудно показать, что для произвольной замкнутой формулы Φ языка L_{τ_E} выполняется равенство

$$I_1(\Phi) = I(\Phi).$$

Интерпретацию I_1 можно рассматривать как нормальную интерпретацию I'_1 языка $L_{\tau=}$.

Индукцией по построению формул нетрудно показать, что для произвольной замкнутой формулы F языка $L_{\tau=}$ выполняются равенства

$$I_1(F^+) = I'_1(F).$$

Окончательно получаем

$$I(F^+) = I_1(F^+) = I'_1(F) = \text{И},$$

так как по предположению замкнутая формула F истинна в любой нормальной интерпретации языка $L_{\tau=}$.

Значит,

$$I((AxEq \rightarrow F^+)) = \text{И},$$

что завершает доказательство леммы. \square

Теорема 3.11.2. *Невозможен алгоритм, позволяющий по произвольной замкнутой формуле чистой логики предикатов первого порядка, алфавит которой содержит лишь 2-местный и 3-местный предикатные символы, определить, является ли эта формула тождественно истинной.*

Д о к а з а т е л ь с т в о. Из доказанных лемм следует эквивалентность

$$U(a_1, a_2) = V(a_1, a_2) \text{ в полугруппе } \Pi \iff \text{формула } (AxEq \rightarrow F_{U,V}^+) \text{ тождественно истинна.}$$

Поэтому утверждение теоремы следует из неразрешимости проблемы равенства слов для полгруппы Π . \square

Оставшаяся часть параграфа посвящена доказательству аналогичного утверждения для чистого исчисления предикатов первого порядка, алфавит которого содержит по крайней мере один 2-местный предикатный символ. В изложении этого материала мы придерживаемся книги Дж. Булоса и Р. Джеффри [3].

Лемма. *Для любого 3-местного предиката P на множестве натуральных чисел существует такой 2-местный предикат $q(u, v)$, что для произвольных натуральных чисел a, b и c справедлива эквивалентность*

$$\begin{aligned} P(a, b, c) = \text{И} \iff & (\exists w)(\exists x)(\exists y)(\exists z)(\neg q(w, w) \& \\ & q(w, x) \& q(x, y) \& q(y, z) \& q(z, w) \& q(w, a) \& q(x, b) \& q(y, c) \& q(z, a) \& \\ & \neg q(a, x) \& \neg q(b, y) \& \neg q(c, z)) = \text{И}. \end{aligned}$$

Д о к а з а т е л ь с т в о. Упорядочим отношением \preccurlyeq множество троек $\langle a, b, c \rangle$ натуральных чисел (целых неотрицательных чисел), полагая для произвольных натуральных чисел $\alpha, \beta, \gamma, a, b$ и c

$$\begin{aligned} \langle \alpha, \beta, \gamma \rangle \preccurlyeq \langle a, b, c \rangle \iff & \text{либо } \alpha + \beta + \gamma < a + b + c, \\ & \text{либо } \alpha + \beta + \gamma = a + b + c \text{ и } \alpha < a, \\ & \text{либо } \alpha + \beta + \gamma = a + b + c, \alpha = a \text{ и } \beta < b. \end{aligned}$$

Нетрудно проверить, что отношение \preccurlyeq является отношением линейного порядка на множестве троек натуральных чисел и при этом тройка $\langle 0, 0, 0 \rangle$ — наименьший элемент.

Занумеруем тройки натуральных чисел, расположенные в соответствии с порядком \preccurlyeq , натуральными числами, начиная с 1, т. е. номером наименьшей тройки $\langle 0, 0, 0 \rangle$ является число 1. Номер тройки $\langle a, b, c \rangle$ будем обозначать через $g(\langle a, b, c \rangle)$ или просто через $g(a, b, c)$.

Заметим, что указанная нумерация троек натуральных чисел строится следующим образом:

все тройки $\langle a, b, c \rangle$ натуральных чисел распадаются на группы: две тройки $\langle \alpha, \beta, \gamma \rangle$ и $\langle a, b, c \rangle$ попадают в одну группу тогда и только тогда, когда

$$\alpha + \beta + \gamma = a + b + c.$$

Эти группы троек натуральных чисел располагаются в порядке возрастания указанной суммы, а внутри групп тройки упорядочены указанным выше способом, т. е. лексикографически.

Отметим ряд достаточно технических фактов, связанных с выбранной нумерацией троек натуральных чисел.

Ноль 0 не является номером никакой тройки натуральных чисел.

Если $n = g(a, b, c)$, то

$a, b, c < n$.

Если $a < n$ и $w = 4n + 1$, то $a < w - 4$.

В самом деле, если $a < n$, то $a + 1 \leq n$, поэтому

$$4a + 4 \leq 4n < 4n + 1 = w.$$

Значит, $a \leq 4a < w - 4$.

Отсюда легко получаем, что

если $a, b, c < n$ и $w = 4n + 1$, $x = 4n + 2$, $y = 4n + 3$ и $z = 4n + 4$, то каждое из чисел a , b и c меньше каждого из чисел $w - 4$, $x - 4$, $y - 4$ и $z - 4$.

Определим предикат $q(x, y)$:

пусть $n = g(a, b, c)$, полагаем

$$\begin{aligned} q(4n + 1, d) &= \text{И} \iff d = 4n + 2 \text{ или } d = a; \\ q(4n + 2, d) &= \text{И} \iff d = 4n + 2, \text{ или } d = 4n + 3, \text{ или } d = b; \\ q(4n + 3, d) &= \text{И} \iff d = 4n + 3, \text{ или } d = 4n + 4, \text{ или } d = c; \\ q(4n + 4, d) &= \text{И} \iff d = 4n + 4, \text{ или } d = 4n + 1, \text{ или} \\ &\quad (d = a \text{ и } P(a, b, c) = \text{И}), \end{aligned}$$

во всех остальных случаях предикат $q(m, d)$ ложен.

Заметим, что если $q(m, d) = \text{И}$, то $d \leq m + 1$.

Нетрудно проверить, что для любого m существует не более одного d такого, что $d < m - 4$ и $q(m, d) = \text{И}$.

Покажем, что справедлива эквивалентность

$$P(a, b, c) = \text{И} \iff (\exists w)(\exists x)(\exists y)(\exists z)(\neg q(w, w) \& q(w, x) \& q(x, y) \& q(y, z) \& q(z, w) \& q(w, a) \& q(x, b) \& q(y, c) \& q(z, a) \& \neg q(a, x) \& \neg q(b, y) \& \neg q(c, z)) = \text{И}.$$

Для некоторого сокращения обозначим через $Q(w, x, y, z, a, b, c)$ формулу

$$(\neg q(w, w) \& q(w, x) \& q(x, y) \& q(y, z) \& q(z, w) \& q(w, a) \& q(x, b) \& q(y, c) \& q(z, a) \& \neg q(a, x) \& \neg q(b, y) \& \neg q(c, z)).$$

Покажем, что

$$P(a, b, c) = \text{И} \iff (\exists w)(\exists x)(\exists y)(\exists z)Q(w, x, y, z, a, b, c) = \text{И}.$$

Предположим, что $P(a, b, c) = \text{И}$.

Укажем такие w, x, y и z , что

$$Q(w, x, y, z, a, b, c) = \text{И}.$$

Пусть $n = g(a, b, c)$, полагаем

$$w = 4n + 1, x = 4n + 2, y = 4n + 3, z = 4n + 4.$$

Легко проверяется выполнение условий $\neg q(w, w), q(w, x), q(x, y), q(y, z), q(z, w), q(w, a), q(x, b), q(y, c)$ и $q(z, a)$.

Остается проверить выполнение условий $\neg q(a, x), \neg q(b, y)$ и $\neg q(c, z)$.

Для этого воспользуемся сделанным выше замечанием:

если $q(m, d) = \text{И}$, то $d \leq m + 1$

и покажем, что $a + 1 < x, b + 1 < y, c + 1 < z$.

Но это следует из отмеченного выше факта

если $a, b, c < n$ и $w = 4n + 1, x = 4n + 2, y = 4n + 3$ и $z = 4n + 4$, то каждое из чисел a, b и c меньше каждого из чисел $w - 4, x - 4, y - 4$ и $z - 4$,

достаточно только напомнить, что $a, b, c < g(a, b, c) = n$.

Итак, мы показали, что

$$P(a, b, c) = \text{И} \implies (\exists w)(\exists x)(\exists y)(\exists z)Q(w, x, y, z, a, b, c) = \text{И}.$$

Докажем обратную импликацию

$$(\exists w)(\exists x)(\exists y)(\exists z)Q(w, x, y, z, a, b, c) = \text{И} \implies P(a, b, c) = \text{И}.$$

Сделать это будет несколько сложнее.

Предположим, что $(\exists w)(\exists x)(\exists y)(\exists z)Q(w, x, y, z, a, b, c) = \text{И}$, и покажем, что тогда $P(a, b, c) = \text{И}$.

Пусть W, X, Y и Z такие, что $Q(W, X, Y, Z, a, b, c) = \text{И}$, т. е.

$$\begin{aligned} &(\neg q(W, W) \& \\ & q(W, X) \& q(X, Y) \& q(Y, Z) \& q(Z, W) \& q(W, a) \& q(X, b) \& q(Y, c) \& \\ & q(Z, a) \& \neg q(a, X) \& \neg q(b, Y) \& \neg q(c, Z)) = \text{И}. \end{aligned}$$

Так как

$$(\neg q(W, W) \& q(W, X)) = \text{И},$$

то найдется такое $n \geq 1$, что $W = 4n + 1$.

Так как $n \geq 1$, то найдутся такие α, β и γ , что $n = g(\langle \alpha, \beta, \gamma \rangle)$.

Прежде всего покажем, что

$$X = 4n + 2, Y = 4n + 3, Z = 4n + 4.$$

Для этого используем условие

$$\begin{aligned} &(q(W, X) \& q(X, Y) \& q(Y, Z) \& q(Z, W) \& q(W, a) \& q(X, b) \& q(Y, c) \& \\ & q(Z, a) \& \neg q(a, X) \& \neg q(b, Y) \& \neg q(c, Z)) = \text{И}. \end{aligned}$$

Напомним, что если $q(m, d) = \text{И}$, то $d \leq m + 1$, поэтому из условия

$$(q(W, X) \& q(X, Y) \& q(Y, Z) \& q(Z, W)) = \text{И}$$

следуют неравенства

$$X + 3 \geq Y + 2 \geq Z + 1 \geq W.$$

Поэтому $X \geq W - 3$.

Аналогично доказываются неравенства $Y \geq X - 3$ и $Z \geq Y - 3$.

Значит, $X \not\leq W - 4$, $Y \not\leq X - 4$ и $Z \not\leq Y - 4$.

Напомним, что для *любого* m существует не более одного d такого, что $d < m - 4$ и $q(m, d) = \text{И}$.

Так как $q(4n + 1, X) = \text{И}$ и $n = g(\langle \alpha, \beta, \gamma \rangle)$, то либо $X = 4n + 2 = W + 1$, либо $X = \alpha$. Но в последнем случае $X < W - 4$, что неверно, поэтому $X = 4n + 2 = W + 1$.

Так как $q(Z, 4n + 1) = \text{И}$, то $Z \neq 4n + 2 = W + 1$, $Z \neq 4n + 3 = W + 2$.

Так как $q(X, Y) = \text{И}$, $X = 4n + 2$ и $Y \not\leq X - 4$, то остаются две возможности: либо $Y = X$, либо $Y = X + 1$.

Если $Y = X = W + 1 = 4n + 2$, то из условий $q(Y, Z) = \text{И}$ и $Z \not\leq Y - 4$ получаем $q(4n + 2, Z) = \text{И}$ две возможности:

либо $Z = 4n + 2 = W + 1$, либо $Z = 4n + 3 = W + 2$.

Тогда условие $q(Z, W) = \text{И}$ дает две возможности:

$$\text{либо } q(4n + 2, 4n + 1) = \text{И} \text{ либо } q(4n + 3, 4n + 1) = \text{И}.$$

Однако ни одна из них не выполняется, значит, $Y = X + 1 = 4n + 3$.

Покажем, что $Z = 4n + 4$.

Так как $q(Y, Z) = \text{И}$, $Y = 4n + 3$ и $Z \not\leq Y - 4$, то остаются две возможности: либо $Z = Y = 4n + 3$, либо $Z = Y + 1 = 4n + 4$.

Если $Z = Y = 4n + 3$, то условие $q(Z, W) = \text{И}$ принимает вид

$$q(4n + 3, 4n + 1) = \text{И},$$

что неверно. Поэтому $Z = Y + 1 = 4n + 4$.

Остается показать, что

$$\langle \alpha, \beta, \gamma \rangle = \langle \alpha, \beta, \gamma \rangle.$$

Тогда из условий

$$q(Z, a) = q(4n + 4, a) = \text{И и}$$

$$g(\langle \alpha, \beta, \gamma \rangle) = g(\langle \alpha, \beta, \gamma \rangle)$$

и неравенства $a < n$ следует, что

$$P(a, b, c) = \text{И}.$$

Для доказательства равенства

$$\langle \alpha, \beta, \gamma \rangle = \langle \alpha, \beta, \gamma \rangle$$

используем условия

$$(q(W, a) \& q(X, b) \& q(Y, c) \&$$

$$\neg q(a, X) \& \neg q(b, Y) \& \neg q(c, Z)) = \text{И}.$$

Так как

$$W = 4n + 1, X = 4n + 2, Y = 4n + 3, Z = 4n + 4,$$

то непосредственная проверка показывает, что

$$(q(X, X) \& q(X, Y) \& q(Y, Y) \&$$

$$q(Y, Z) \& q(Z, Z)) = \text{И},$$

поэтому

$$a \neq X, b \neq X, b \neq Y, c \neq Y, c \neq Z.$$

Из условий $q(W, a) = \text{И}$, $W = 4n + 1$ и $n = g(\langle \alpha, \beta, \gamma \rangle)$ следует, что либо $a = 4n + 2 = X$, либо $a = \alpha$. Что вместе с условием $a \neq X$ дает равенство $a = \alpha$.

Из условий $q(X, b) = \text{И}$, $X = 4n + 2$ и $n = g(\langle \alpha, \beta, \gamma \rangle)$ следует, что либо $b = 4n + 2 = X$, либо $b = 4n + 3 = Y$, либо $b = \beta$. Что вместе с условиями $b \neq X$ и $b \neq Y$ дает равенство $b = \beta$.

Из условий $q(Y, c) = \text{И}$, $Y = 4n + 3$ и $n = g(\langle \alpha, \beta, \gamma \rangle)$ следует, что либо $c = 4n + 3 = Y$, либо $c = 4n + 4 = Z$, либо $c = \gamma$. Что вместе с условиями $c \neq Y$ и $c \neq Z$ дает равенство $c = \gamma$.

Значит,

$$\langle \alpha, \beta, \gamma \rangle = \langle \alpha, \beta, \gamma \rangle,$$

поэтому

$$n = g(\langle \alpha, \beta, \gamma \rangle) = g(\langle \alpha, \beta, \gamma \rangle)$$

Тогда из условий

$$q(Z, a) = q(4n + 4, a) = \text{И и}$$

$$g(\langle \alpha, \beta, \gamma \rangle) = g(\langle \alpha, \beta, \gamma \rangle)$$

и неравенства $a < n$ следует, что

$$P(a, b, c) = \text{И}.$$

Это завершает доказательство леммы. \square

Лемма. По произвольной замкнутой формуле Φ чистой логики предикатов первого порядка, алфавит которой содержит лишь 2-местный и 3-местный предикатные символы, можно построить формулу $\hat{\Phi}$ чистой логики предикатов первого порядка, алфавит которой содержит лишь два 2-местных предикатных символа, такую, что формула Φ выполнима тогда и только тогда, когда выполнима формула $\hat{\Phi}$.

Доказательство. Пусть Φ – замкнутая формула чистой логики предикатов первого порядка, алфавит которой содержит лишь 2-местный предикатный символ p и 3-местный предикатный символ P .

Построим формулу $\hat{\Phi}$ чистой логики предикатов первого порядка, алфавит которой содержит лишь два 2-местных предикатных символа p и q , заменив в формуле Φ каждую элементарную подформулу вида $P(s, u, v)$ на формулу

$$\begin{aligned} (\exists w)(\exists x)(\exists y)(\exists z)(\neg q(w, w) \& \\ q(w, x) \& q(x, y) \& q(y, z) \& q(z, w) \& q(w, s) \& q(x, u) \& q(y, v) \& q(z, s) \& \\ \neg q(s, x) \& \neg q(u, y) \& \neg q(v, z)) = \text{И}. \end{aligned}$$

Для завершения доказательства достаточно воспользоваться предыдущей леммой. \square

Лемма. По произвольной замкнутой формуле Φ чистой логики предикатов первого порядка, алфавит которой содержит лишь два 2-местных предикатных символа, можно построить формулу $\tilde{\Phi}$ чистой логики предикатов первого порядка, алфавит которой содержит лишь один 3-местный предикатный символ, такую, что формула Φ выполнима тогда и только тогда, когда выполнима формула $\tilde{\Phi}$.

Д о к а з а т е л ь с т в о. Пусть алфавит чистой логики предикатов содержит лишь 2-местные предикатные символы p_1 и p_2 , а Q – новый 3-местный предикатный символ.

По произвольной замкнутой формуле Φ чистой логики предикатов первого порядка, алфавит которой содержит лишь два 2-местных предикатных символа p_1 и p_2 , следующим образом построим замкнутую формулу $\tilde{\Phi}$ чистой логики предикатов первого порядка, алфавит которой содержит лишь один 3-местных предикатный символ Q :

- 1) пусть x_1 и x_2 – две различные переменные, не входящие в формулу Φ ,
- 2) в формуле Φ каждую элементарную подформулу вида $p_i(u, v)$ заменим на $Q(x_i, u, v)$, полученную формулу обозначим через Φ_1 ,
- 3) обозначим через $\tilde{\Phi}$ формулу $(\forall x_1)(\forall x_2)\Phi_1$.

Нетрудно проверить, что формула Φ выполнима тогда и только тогда, когда выполнима формула $\tilde{\Phi}$. \square

Лемма. По произвольной замкнутой формуле Φ чистой логики предикатов первого порядка, алфавит которой содержит лишь 2-местный и 3-местный предикатные символы, можно построить формулу Φ^* чистой логики предикатов первого порядка, алфавит которой содержит лишь один 2-местный предикатный символ, такую, что формула Φ выполнима тогда и только тогда, когда выполнима формула $\tilde{\Phi}$.

Д о к а з а т е л ь с т в о. В силу доказанных лемм в качестве формулы Φ^* можно взять формулу $\tilde{\tilde{\Phi}}$. \square

Из теоремы 3.11.1 и доказанных лемм следует следующая теорема А. Черча

Теорема 3.11.3. (А. Черч) Невозможен алгоритм, позволяющий по произвольной замкнутой формуле логики предикатов первого порядка, алфавит которой содержит лишь один 2-местный предикатный символ, определить, является ли эта формула тождественно истинной.

Другая равносильная формулировка теоремы А. Черча.

Теорема 3.11.4. (А. Черч) Невозможен алгоритм, позволяющий по произвольной замкнутой формуле логики предикатов первого порядка, алфавит которой содержит лишь один 2-местный предикатный символ, определить, является ли эта формула выполнимой.

ГЛАВА 4.

ДОПОЛНЕНИЕ

4.1. Булевы алгебры

В этом разделе приведены основные сведения о **булевой алгебре** – одной из наиболее важных с точки зрения математической логики алгебраических структур.

Определение 4.1.1. *Булевой алгеброй* называется непустое множество \mathcal{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 \mathcal{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 \mathcal{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 \mathcal{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 \mathcal{B} выполняются равенства

$$a \cap 1 = a, \quad a \cup 0 = a.$$

5. Аксиомы дополнения:

для любого элемента a из множества \mathcal{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

$$\langle \langle \mathcal{B} \mid \{0, 1\}, \{\bar{}\}, \{\cap, \cup\} \rangle \rangle.$$

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

$$\langle \langle \mathcal{B} \mid \{0, 1\}, \{\bar{}\}, \{\cap, \cup\} \rangle \rangle$$

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 $\bar{}$, \cap и \cup определим естественным образом, полагая для произвольных подмножеств A и B множества $\mathcal{P}(U)$

$$\bar{A} \equiv U \setminus A,$$

$$A \cap B \text{ — пересечение множеств } A \text{ и } B,$$

$$A \cup B \text{ — объединение множеств } A \text{ и } B.$$

Легко проверяется выполнимость аксиом булевой алгебры.

Построенная булева алгебра называется **алгеброй подмножеств** множества U . В случае пустого множества U получается нулевая булева алгебра.

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. если $A, B \in \mathcal{B}$, то $\bar{A} \in \mathcal{B}, A \cap B \in \mathcal{B}$ и $A \cup B \in \mathcal{B}$.

Например, в качестве \mathcal{B} можно взять систему, состоящую лишь из двух подмножеств \emptyset и U непустого 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 \mathfrak{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 \mathcal{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 \mathcal{B} выполняются равенства

$$a \cap e = a,$$

то $e = 1$.

Симметричным образом, если элемент e обладает свойством:

для любого элемента a из множества \mathcal{B} выполняются равенства

$$a \cup e = a,$$

то $e = 0$.

Кроме того, для любого элемента a из множества \mathcal{B} выполняются равенства

$$a \cup 1 = 1, \quad a \cap 0 = 0.$$

Покажем, что если для элементов a и b из множества \mathcal{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

$$a \cap \bar{b} = 0 \iff b \cup \bar{a} = 1.$$

Отсюда легко получить эквивалентность

$$a \leq b \iff \bar{b} \leq \bar{a}.$$

Нетрудно показать, что относительно введенного отношения частичного порядка \leq выполняются равенства

$$a \cap b = \inf\{a, b\}, \quad a \cup b = \sup\{a, b\}.$$

Подмножество $\mathcal{C} \subseteq \mathcal{B}$ основного множества \mathcal{B} булевой алгебры

$$\mathfrak{B} = \langle \langle \mathcal{B} \mid \{0, 1\}, \{-\}, \{\cap, \cup\} \rangle \rangle$$

называется **подалгеброй** булевой алгебры \mathfrak{B} , если оно замкнуто относительно операций булевой алгебры \mathfrak{B} , т. е. $0, 1 \in \mathcal{C}$ и если $a, b \in \mathcal{C}$, то $a \cap b \in \mathcal{C}$, $a \cup b \in \mathcal{C}$ и $\bar{a} \in \mathcal{C}$. Подалгебра \mathcal{C} булевой алгебры \mathfrak{B} сама является булевой алгеброй относительно ограничений на ней операций булевой алгебры \mathfrak{B} .

Так как пересечение произвольного семейства подалгебр булевой алгебры само является подалгеброй, то для произвольного подмножества $\mathcal{X} \subseteq \mathcal{B}$ существует единственная минимальная относительно включения \subseteq подалгебра булевой алгебры \mathfrak{B} , содержащая это подмножество \mathcal{X} . Эта подалгебра обозначается через $\mathfrak{B}(\mathcal{X})$ и называется подалгеброй булевой алгебры \mathfrak{B} , порожденной подмножеством \mathcal{X} .

Введем полезное обозначение a^ε , где a — произвольный элемент булевой алгебры \mathfrak{B} , а $\varepsilon \in \{-1, 1\}$: $a^{-1} = \bar{a}$, $a^1 = a$.

Полагаем $\bigcup_{i=1}^0 b_i = 0$ и $\bigcap_{i=1}^0 b_i = 1$.

Теорема 4.1.1. Если $\mathcal{X} \subseteq \mathcal{B}$ — подмножество основного множества \mathcal{B} булевой алгебры \mathfrak{B} , то порожденная им подалгебра $\mathfrak{B}(\mathcal{X})$ состоит из всевозможных элементов вида

$$\bigcup_{i=1}^m \bigcap_{j=1}^{n_i} a_{ij}^{\varepsilon_{ij}},$$

где $m \geq 0$, при любом i : $n_i \geq 0$ при любых i и j : $a_{ij} \in \mathcal{X}$.

Д о к а з а т е л ь с т в о. Обозначим через \mathcal{C} множество элементов вида

$$\bigcup_{i=1}^m \bigcap_{j=1}^{n_i} a_{ij}^{\varepsilon_{ij}}.$$

Так как \mathcal{C} содержит множество \mathcal{X} и содержится в любой подалгебре булевой алгебры \mathfrak{B} , содержащей множество \mathcal{X} , то $\mathcal{C} \subseteq \mathfrak{B}(\mathcal{X})$.

Используя основные свойства булевой алгебры, нетрудно показать, что \mathcal{C} – подалгебра булевой алгебры \mathfrak{B} , а так как \mathcal{C} содержит множество \mathcal{X} , то $\mathfrak{B}(\mathcal{X}) \subseteq \mathcal{C}$. Из этих двух включений получаем необходимое равенство $\mathfrak{B}(\mathcal{X}) = \mathcal{C}$. \square

Аналогично доказывается следующая теорема.

Теорема 4.1.2. *Если $\mathcal{X} \subseteq \mathcal{B}$ – подмножество основного множества \mathcal{B} булевой алгебры \mathfrak{B} , то порожденная им подалгебра $\mathfrak{B}(\mathcal{X})$ состоит из всевозможных элементов вида*

$$\bigcap_{i=1}^m \bigcup_{j=1}^{n_i} a_{ij}^{\varepsilon_{ij}},$$

где $m \geq 0$, при любом i : $n_i \geq 0$ при любых i и j : $a_{ij} \in \mathcal{X}$.

Теорема 4.1.3. *Если $\mathcal{X} \subseteq \mathcal{B}$ – конечное подмножество основного множества \mathcal{B} булевой алгебры \mathfrak{B} , состоящее из n элементов, то порожденная им подалгебра $\mathfrak{B}(\mathcal{X})$ содержит не более чем 2^{2^n} элементов.*

Д о к а з а т е л ь с т в о. Пусть $\mathcal{X} = \{a_1, \dots, a_n\}$. Из теоремы 4.1.1 и равенств

$$\begin{aligned} A \cap B \cap C \cap B \cap D &= A \cap B \cap C \cap D, \quad A \cap B \cap C \cap \bar{B} \cap D = A \cap \bar{B} \cap C \cap B \cap D = 0, \\ A \cup 0 &= A, \quad B = (B \cap A) \cup (B \cap \bar{A}) \end{aligned}$$

и других равенств, выполняющихся в любой булевой алгебре, следует, что каждый элемент подалгебры $\mathfrak{B}(\mathcal{X})$ представим в виде

$$\bigcup_{i=1}^m \bigcap_{j=1}^n a_j^{\varepsilon_{ij}}.$$

где $m \geq 0$. Так как элементов вида $\bigcap_{j=1}^n a_j^{\varepsilon_j}$ не более чем 2^n , то в подалгебре $\mathfrak{B}(\mathcal{X})$ не более чем 2^{2^n} элементов. \square

Булева алгебра \mathfrak{B} называется σ -алгеброй, если для любого счетного семейства $(a_i)_{i \in \mathbb{N}}$ ее элементов относительно введенного отношения частичного порядка \leq существует **точная верхняя грань** \sup для счетного множества элементов

$$\{a_1, a_2, \dots, a_n, \dots\},$$

которая обозначается через $\bigcup_{i \in N} a_i$. Т. е. это такой элемент a булевой алгебры \mathfrak{B} , что при любом i : $a_i \leq a$ и для любого элемента b булевой алгебры \mathfrak{B} , если при любом i : $a_i \leq b$, то $a \leq b$.

В σ -алгебре \mathfrak{B} для любого счетного семейства $(a_i)_{i \in N}$ ее элементов относительно введенного отношения частичного порядка \leq существует **точная нижняя грань** \inf для счетного множества элементов

$$\{a_1, a_2, \dots, a_n, \dots\},$$

которая равна $\overline{\bigcup_{i \in N} \bar{a}_i}$ и обозначается через $\bigcap_{i \in N} a_i$.

Для произвольного множества U множество всех его подмножеств $\mathcal{P}(U)$ является σ -алгеброй. В этом случае для любого счетного семейства $(A_i)_{i \in N}$ ее элементов, т. е. подмножеств множества U ,

$$\begin{aligned} \bigcup_{i \in N} A_i & \text{ — объединение множеств } A_i \ (i \in N), \\ \bigcap_{i \in N} A_i & \text{ — пересечение множеств } A_i \ (i \in N). \end{aligned}$$

Эта булева σ -алгебра называется σ -алгеброй подмножеств множества U .

Подмножество $\mathcal{C} \subseteq \mathcal{B}$ основного множества \mathcal{B} булевой σ -алгебры

$$\mathfrak{B} = \langle \langle \mathcal{B} \mid \{0, 1\}, \{\bar{\cdot}\}, \{\cap, \cup\} \rangle \rangle$$

называется σ -**подалгеброй** булевой σ -алгебры \mathfrak{B} , если оно является **подалгеброй** булевой алгебры \mathfrak{B} , т. е. замкнуто относительно операций булевой алгебры \mathfrak{B} , т. е. $0, 1 \in \mathcal{C}$ и если $a, b \in \mathcal{C}$, то $a \cap b \in \mathcal{C}$, $a \cup b \in \mathcal{C}$ и $\bar{a} \in \mathcal{C}$ и для любого счетного семейства $(a_i)_{i \in N}$ элементов из \mathcal{C} $\bigcup_{i \in N} a_i \in \mathcal{C}$.

σ -подалгебра \mathcal{C} булевой σ -алгебры \mathfrak{B} сама является булевой σ -алгеброй относительно ограничений на ней операций булевой алгебры \mathfrak{B} .

Так как пересечение произвольного семейства σ -подалгебр булевой σ -алгебры само является σ -подалгеброй, то для произвольного подмножества $\mathcal{X} \subseteq \mathcal{B}$ существует единственная минимальная относительно включения \subseteq σ -подалгебра булевой алгебры \mathfrak{B} , содержащая это подмножество \mathcal{X} . Эта подалгебра обозначается через $\mathfrak{B}_\sigma(\mathcal{X})$ и называется σ -подалгеброй булевой σ -алгебры \mathfrak{B} , порожденной подмножеством \mathcal{X} .

Если в качестве множества U взять множество R^n , а в качестве подмножества $\mathcal{X} \subseteq \mathcal{P}(R^n)$ — множество всех *открытых подмножеств* множества R^n , то порожденная подмножеством \mathcal{X} σ -подалгебра $\mathfrak{B}_\sigma(\mathcal{X})$ булевой σ -алгебры $\mathcal{P}(R^n)$ называется σ -**алгеброй борелевских подмножеств** пространства R^n и обозначается через $\mathcal{B}(R^n)$.

По той же схеме, которая была использована при доказательстве теоремы 4.1.1, можно доказать, что

σ -подалгебра $\mathcal{B}(R^n)$ борелевских подмножеств состоит из всевозможных элементов вида

$$\bigcup_{i=1}^{\infty} \bigcap_{j=1}^{\infty} A_{ij}^{\varepsilon_{ij}},$$

где при любых i и j : A_{ij} – открытое подмножество, $\varepsilon_{ij} \in \{-1, +1\}$ и A_{ij}^{+1} – это A_{ij} , A_{ij}^{-1} – это дополнение A_{ij} , а значит, замкнутое подмножество.

Аналогично, σ -подалгебра $\mathcal{B}(R^n)$ борелевских подмножеств состоит из всевозможных элементов вида

$$\bigcap_{i=1}^{\infty} \bigcup_{j=1}^{\infty} A_{ij}^{\varepsilon_{ij}},$$

где при любых i и j : A_{ij} – открытое подмножество, $\varepsilon_{ij} \in \{-1, +1\}$ и A_{ij}^{+1} – это A_{ij} , A_{ij}^{-1} – это дополнение A_{ij} .

Так как множество в R^n является открытым тогда и только тогда, когда его дополнение замкнуто, то, очевидно, справедливы и следующие два утверждения

σ -подалгебра $\mathcal{B}(R^n)$ борелевских подмножеств состоит из всевозможных элементов вида

$$\bigcup_{i=1}^{\infty} \bigcap_{j=1}^{\infty} F_{ij}^{\varepsilon_{ij}},$$

где при любых i и j : F_{ij} – замкнутое подмножество, $\varepsilon_{ij} \in \{-1, +1\}$ и F_{ij}^{+1} – это F_{ij} , F_{ij}^{-1} – это дополнение F_{ij} , а значит, открытое подмножество;

σ -подалгебра $\mathcal{B}(R^n)$ борелевских подмножеств состоит из всевозможных элементов вида

$$\bigcap_{i=1}^{\infty} \bigcup_{j=1}^{\infty} F_{ij}^{\varepsilon_{ij}},$$

где при любых i и j : F_{ij} – замкнутое подмножество, $\varepsilon_{ij} \in \{-1, +1\}$ и F_{ij}^{+1} – это F_{ij} , F_{ij}^{-1} – это дополнение F_{ij} .

σ -подалгебра $\mathcal{B}(R^n)$ борелевских подмножеств играет важную роль в математическом анализе, теории меры и теории вероятностей.

4.2. Фильтры на булевых алгебрах

Определение 4.2.1. *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 4.2.2. Фильтр, не содержащийся ни в каком отличном от него фильтре, называется **максимальным**.

Теорема 4.2.1. Любой фильтр содержится в некотором максимальном фильтре.

Доказательство. 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

$$F = \cup_{U \in K} U.$$

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 4.2.3. 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 4.2.4. 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 4.2.2. 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**.

Д о к а з а т е л ь с т в о. 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

Понятия **фильтра** и **ультрафильтра** широко используются не только в математической логике, но и в других разделах математики, в частности, в математическом анализе обобщением различных понятий предела функции выступает понятие **предела функции по фильтру**. Понятие **ультрафильтра** играет важную роль в доказательстве следующей теоремы Стоуна о булевых алгебрах.

Теорема 4.2.3. *Любая булева алгебра изоморфна алгебре подмножеств некоторого множества.*

Любая конечная булева алгебра изоморфна алгебре всех подмножеств некоторого множества.

Д о к а з а т е л ь с т в о. Пусть \mathfrak{B} – произвольная булева алгебра. Обозначим через U множество всех **ультрафильтров** на \mathfrak{B} . Для произвольного элемента a булевой алгебры \mathfrak{B} обозначим через $h(a)$ подмножество множества U : $h(a) = \{F \mid a \in F \in U\}$. Так как для любого фильтра F выполняется эквивалентность

$$a \cap b \in F \iff a \in F \text{ \& } b \in F,$$

а для любого ультрафильтра F выполняются эквивалентности

$$a \cup b \in F \iff a \in F \vee b \in F$$

и

$$\bar{a} \in F \iff a \notin F,$$

то $h(a \cap b) = h(a) \cap h(b)$, $h(a \cup b) = h(a) \cup h(b)$ и $h(\bar{a}) = U \setminus h(a)$.

Кроме того, если a и b – элементы булевой алгебры и неверно, что $a \leq b$, то ультрафильтр F , состоящий из всех элементов c таких, что $a \leq c$, содержит a , но не содержит b .

Значит, h – **изоморфизм булевой алгебры \mathfrak{B} на алгебру подмножеств множества U** .

Если булева алгебра \mathfrak{B} конечная, то любой фильтр F на ней имеет наименьший и наибольший элементы: если F состоит из элементов a_1, \dots, a_m , то $a_1 \cap \dots \cap a_m$ – наименьший, а $a_1 \cup \dots \cup a_m$ – наибольший элементы.

Пусть \mathfrak{B} – конечная булева алгебра. Покажем, что $h(\mathfrak{B}) = \mathcal{P}(U)$. Если $\{F_1, \dots, F_t\}$ – произвольное подмножество множества U , а a_1, \dots, a_t – наименьшие элементы фильтров F_1, \dots, F_t , то нетрудно показать, что

$$h(a_1 \cup \dots \cup a_t) = \{F_1, \dots, F_t\}.$$

□

4.3. Псевдобулевы алгебры

Булевы алгебры – важный и полезный инструмент исследования классических логических исчислений – **Исчисления Высказываний** и **Исчисления Предикатов**. Для исследования неклассических логических исчислений требуются более общие алгебраические структуры. В частности, адекватным алгебраическим инструментом для изучения **Интуиционистского Исчисления Высказываний** являются **Псевдобулевы алгебры** или **алгебры Брауэра**.

Определение 4.3.1. *Решеткой* называется непустое частично упорядоченное множество $\mathcal{B} = \langle B, \leq \rangle$, в котором для любых двух элементов a и b из основного множества B существуют **точная верхняя** $\sup(a, b)$ и **точная нижняя** $\inf(a, b)$ **границы** двуэлементного множества $\{a, b\}$.

Напомним, что **точная верхняя грань** $\sup(a, b)$ (**точная нижняя грань** $\inf(a, b)$) двуэлементного множества $\{a, b\}$ – это элемент множества B , удовлетворяющий условиям:

$$\begin{aligned} 1) a &\leq \sup(a, b), \quad 2) b \leq \sup(a, b), \\ 3) (\forall x)((a &\leq x \& b \leq x) \rightarrow \sup(a, b) \leq x) \end{aligned}$$

(соответственно условиям

$$\begin{aligned} 1) \inf(a, b) &\leq a, \quad 2) \inf(a, b) \leq b, \\ 3) (\forall x)((x &\leq a \& x \leq b) \rightarrow x \leq \inf(a, b)). \end{aligned}$$

Традиционно элемент $\sup(a, b)$ обозначается через $a \cup b$, а элемент $\inf(a, b)$ – через $a \cap b$.

Теория решеток достаточно хорошо разработана и имеет многочисленные применения как в самой математике, так и в ее приложениях. Мы не будем углубляться в общую теорию решеток, а рассмотрим лишь наиболее важные для нас с точки зрения предполагаемых приложений подклассы решеток.

Для произвольной решетки $\mathcal{B} = \langle B, \leq \rangle$ выполняются следующие свойства:

1. ассоциативность:

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. коммутативность:

для любых элементов a и b из множества B выполняются равенства

$$a \cap b = b \cap a, \quad a \cup b = b \cup a.$$

Определение 4.3.2. Решетка называется $\mathcal{B} = \langle B, \leq \rangle$ **дистрибутивной**, если для любых элементов a, b и c из множества B выполняются равенства

$$a \cap (b \cup c) = (a \cap b) \cup (a \cap c), \quad a \cup (b \cap c) = (a \cup b) \cap (a \cup c).$$

Булевы алгебры – это важный пример дистрибутивных решеток.

Если в решетке $\mathcal{B} = \langle B, \leq \rangle$ имеется **наибольший** (**наименьший**) элемент 1 (0), то он называется **единичным** (**нулевым**) элементом решетки \mathcal{B} . Напомним, это означает, что для любого элемента a из множества B выполняется неравенство $a \leq 1$ ($0 \leq a$). Заметим, что эти неравенства можно заменить равенствами $a \cap 1 = a$ или $a \cup 1 = 1$ ($a \cap 0 = 0$ или $a \cup 0 = a$).

Булевы алгебры – это дистрибутивные решетки с нулевым и единичным элементами, удовлетворяющие условию:

Аксиома дополнения:

для любого элемента a из множества B существует элемент \bar{a} , для которого выполняются равенства

$$a \cap \bar{a} = 0, \quad a \cup \bar{a} = 1.$$

Для введения понятия **псевдобулевой алгебры** потребуется несколько обобщить понятие дополнения элемента.

Определение 4.3.3. Элемент c решетки $\mathcal{B} = \langle B, \leq \rangle$ называется **псевдодополнением** элемента a **относительно** b , если c – наибольший элемент, удовлетворяющий неравенству $a \cap c \leq b$.

Псевдодополнение элемента a относительно b , если оно существует, обозначается через $a \Rightarrow b$. Из определения псевдодополнения следует, что для любого элемента x их множества B выполняется эквивалентность:

$$a \cap x \leq b \text{ тогда и только тогда, когда } x \leq (a \Rightarrow b).$$

Нетрудно показать, что если решетка $\mathcal{B} = \langle B, \leq \rangle$ является булевой алгеброй, то **псевдодополнение** $a \Rightarrow b$ элемента a **относительно** b всегда существует и оно равно $\bar{a} \cup b$.

Определение 4.3.4. Дистрибутивная решетка $\mathcal{B} = \langle B, \leq \rangle$ с единичным и нулевым элементами, в которой для любых элементов a и b существует псевдодополнение $a \Rightarrow b$ элемента a **относительно** b , называется **псевдобулевой алгеброй**.

Можно показать, что свойство дистрибутивности решетки на самом деле следует из остальных свойств решетки, входящих в определение псевдобулевой алгебры. Однако мы сознательно включили требование дистрибутивности решетки в это определение. В противном случае нам пришлось бы вводить промежуточное для преследуемых нами целей понятие импликативной решетки.

Примерами псевдобулевых алгебр, естественно, служат булевы алгебры. Другой важный класс псевдобулевых алгебр образуют *решетки открытых подмножеств* произвольного топологического пространства U относительно отношения включения \subseteq , если положить

$$(A \Rightarrow B) = I((U \setminus A) \cup B),$$

где $I(C)$ – это *внутренность* множества C .

В произвольной псевдобулевой алгебре $\mathcal{B} = \langle B, \leq \rangle$ для любого элемента a определено понятие *псевдодополнения* \tilde{a} равенством $\tilde{a} = a \Rightarrow 0$. Наряду с обозначением \tilde{a} мы будем использовать и обозначение $\sim a$.

Каждую псевдобулеву алгебру $\mathcal{B} = \langle B, \leq \rangle$ можно рассматривать как алгебраическую систему

$$\mathcal{B} = \langle B, \leq, \cap, \cup, \Rightarrow, \sim \rangle$$

с одним двуместным отношением \leq , с тремя двуместными операциями \cap , \cup и \Rightarrow и одной одноместной операцией \sim или как алгебраическую систему

$$\mathcal{B} = \langle B, \cap, \cup, \Rightarrow, \sim \rangle$$

с тремя двуместными операциями \cap , \cup и \Rightarrow и одной одноместной операцией \sim .

Основные, необходимые для дальнейшего, свойства псевдобулевых алгебр собраны в следующей теореме.

Теорема 4.3.1. *В любой псевдобулевой алгебре*

$$\mathcal{B} = \langle B, \leq, \cap, \cup, \Rightarrow, \sim \rangle$$

выполняются следующие эквивалентности, равенства и неравенства

- 1) $(a \Rightarrow b) = 1$ тогда и только тогда, когда $a \leq b$,
- 2) $a = b$ тогда и только тогда, когда $(a \Rightarrow b) = 1 \ \& \ (b \Rightarrow a) = 1$,
- 3) $(a \Rightarrow a) = 1$,
- 4) $(a \Rightarrow 1) = 1$,
- 5) $(1 \Rightarrow b) = b$,
- 6) $(a \Rightarrow a) \cap b = b$,
- 7) $a \cap (a \Rightarrow b) \leq b$,
- 8) если $a_1 \leq a_2$, то $(a_2 \Rightarrow b) \leq (a_1 \Rightarrow b)$,
- 9) если $b_1 \leq b_2$, то $(a \Rightarrow b_1) \leq (a \Rightarrow b_2)$,
- 10) $b \leq (a \Rightarrow b)$,
- 11) $a \cap (a \Rightarrow b) = a \cap b$,
- 12) $(a \Rightarrow b) \cap b = b$,

- 13) $(a \Rightarrow b) \cap (a \Rightarrow c) = (a \Rightarrow (b \cap c))$,
- 14) $(a \Rightarrow c) \cap (b \Rightarrow c) = ((a \cup b) \Rightarrow c)$,
- 15) $((a \Rightarrow (b \Rightarrow c)) = ((a \cap b) \Rightarrow c) = ((b \Rightarrow (a \Rightarrow c)))$,
- 16) $(c \Rightarrow a) \leq ((c \Rightarrow (a \Rightarrow b)) \Rightarrow (c \Rightarrow b))$,
- 17) $(a \Rightarrow b) \cap (b \Rightarrow c) \leq (a \Rightarrow c)$,
- 18) $(a \Rightarrow b) \leq ((b \Rightarrow c) \Rightarrow (a \Rightarrow c))$,
- 19) $a \leq (b \Rightarrow (a \cap b))$,
- 20) $(a \Rightarrow (b \Rightarrow c)) \leq ((a \Rightarrow b) \Rightarrow (a \Rightarrow c))$,
- 21) $(c \cap ((c \cap a) \Rightarrow (c \cap b)) = (c \cap (a \Rightarrow b))$,
- 22) если $a \leq b$, то $\tilde{b} \leq \tilde{a}$,
- 23) $\tilde{0} = 1, \tilde{1} = 0$,
- 24) $a \cap \tilde{a} = 0$,
- 25) $\sim (a \cap \tilde{a}) = 1$,
- 26) $a \leq \sim (\sim a)$,
- 27) $\sim (\sim (\sim a)) = \sim a$,
- 28) $\sim (a \cup b) = \sim a \cap \sim b$,
- 29) $\sim a \cup \sim b \leq \sim (a \cap b)$,
- 30) $\sim a \cup b \leq (a \Rightarrow b)$,
- 31) $(a \Rightarrow b) \leq (\sim b \Rightarrow \sim a)$,
- 32) $(a \Rightarrow \sim b) = \sim (a \cap b) = (\Rightarrow \sim a)$,
- 33) $(a \Rightarrow \sim b) = \sim \sim (a \Rightarrow \sim b)$,
- 34) $\sim \sim (a \Rightarrow b) \leq (a \Rightarrow \sim \sim b)$,
- 35) $(0 \Rightarrow a) = 1$.

Подмножество $C \subseteq B$ основного множества B псевдобулевой алгебры

$$B = \langle B \mid \{0, 1\}, \cap, \cup, \Rightarrow, \sim \rangle$$

называется *подалгеброй* псевдобулевой алгебры B , если оно замкнуто относительно операций псевдобулевой алгебры B , т. е. $0, 1 \in C$, и если $a, b \in C$, то $a \cap b \in C$, $a \cup b \in C$, $a \Rightarrow b \in C$ и $\sim a \in C$. Подалгебра C псевдобулевой алгебры B сама является псевдобулевой алгеброй относительно ограничений на ней операций псевдобулевой алгебры B .

Так как *пересечение произвольного семейства подалгебр псевдобулевой алгебры само является подалгеброй*, то для произвольного подмножества $X \subseteq B$ существует единственная минимальная относительно включения \subseteq подалгебра псевдобулевой алгебры B , содержащая это подмножество X . Эта подалгебра обозначается через $B(X)$ и называется *подалгеброй псевдобулевой алгебры B , порожденной подмножеством X* .

Для псевдобулевых алгебр имеет место следующая теорема, подобная аналогичной теореме 4.1.3 для булевых алгебр.

Теорема 4.3.2. *Если $X \subseteq B$ – конечное подмножество основного множества B псевдобулевой алгебры B , состоящее из n элементов, то порожденная им подалгебра $B(X)$ содержит не более чем 2^{2^n} элементов.*

Доказательство этой теоремы требует более подробного изучения псевдобулевых алгебр, в частности, их связи с топологическими булевыми алгебрами, что увело бы нас слишком в сторону от основной "классической" тематики пособия. Желающие могут изучить доказательство этой теоремы по замечательной книге Расева Е., Сикорский Р. "Математика метаматематики". М.: Наука. 1972 [32].

4.4. Из истории математики и логики

4.4.1. Из истории математики

Математика, как и искусство, – это особый способ описания и познания мира.

По мнению ряда специалистов по истории математики, есть достаточно убедительные основания считать, что достаточно развитая математика существовала в доэллинический период, почти за 3000 лет до н. э. математическими фактами владели египетские и вавилонские плотники и землемеры.

Важными источниками сведений, касающихся "доисторического" периода развития математики, служат **математические папирусы** и **клинописные математические тексты**. Математические папирусы – это древнейшие из дошедших до нас математических текстов. Они служили учебниками (справочниками) для писцов, которые были государственными служащими в Древнем Египте, в чьи обязанности входили подсчет налогов, определение расходов при проведении строителств и т. д.

Математические папирусы относятся к периоду Среднего царства (приблизительно XXI – XVIII вв. до н. э.). Это выдающиеся математические памятники Древнего Египта. Из них наиболее известны – **папирус Ринда**, названный так по имени его владельца, египтолога Г. Ринда. Папирус составлен писцом по имени Ахмес около 2000 – 1550 гг. до н. э., поэтому нередко сам папирус называют **папирусом Ахмеса**. Ряд исследователей считает, что папирус Ринда был создан на основе более древних источников. Основная часть папируса Ринда хранится в Британском музее (Лондон). Этот свиток представляет собой справочник землемера для решения практических задач. Впервые папирус подробно изучен и издан на немецком языке А. Эйзенлором в 1877 г. Папирус дает представление о состоянии математических знаний в Древнем Египте. Он включает в себя решения 84 задач прикладного характера. Задачи весьма разнообразные: это и нахождение площади поля, имеющего форму прямоугольника, треугольника, трапеции и круга, и вычисление объема прямоугольного параллелепипеда и цилиндра. 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.

Есть в папирусе и арифметические задачи на действия с дробями, на пропорциональное деление и даже одна задача (79-я) приводит к необходимости нахождения суммы геометрической прогрессии.

Московский папирус, хранящийся в Музее изобразительных искусств имени А. С. Пушкина (Москва), подробно изучался отечественными египтологами Б. А. Тураевым в 1917 г. и В. В. Струве в 1927 г. Он полностью издан на немецком языке в 1930 г. Собранные в **Московском папирусе** 25 задач носят схожий характер с задачами из **папируса Ринда**. Интересно отметить, что решение одной задачи основано на формуле для вычисления объема усеченной пирамиды, в основании которой квадрат, а в другой задаче вычисляется площадь боковой поверхности полуцилиндра. Это первый из дошедших до нас примеров вычисления площади криволинейной поверхности.

Клинописные математические тексты написаны клинописью на глиняных пластинах. Они охватывают период с 2-го тыс. до н. э. и до начала н. э. Это математические тексты Древней Вавилонии и Ассирии. Они включают математические таблицы – таблицы умножения, таблицы квадратов и кубов, таблицы обратных величин, позволяющие в вычислениях заменить деление умножением. Ряд **клинописных математических текстов** представляет собой специальные математические тексты, содержащие задачи с решениями. Известно более сотни специальных математических текстов, которые относятся в основном ко II тыс. до н. э. В **клинописных математических текстах** впервые встречаются квадратные уравнения и позиционная система счисления (шестидесятеричная). Квадратные уравнения, по-видимому, появились у вавилонян в связи с землемерной практикой, что отразилось в терминологии: неизвестные назывались "длина" и "ширина".

Хотя в **математических папирусах** и в **клинописных математических текстах** нет еще "общих правил" и каких-нибудь "теоретических обобщений", однако можно уже говорить о элементах геометрического и даже алгебраического мышления, особенно, в **клинописных математических текстах**, в которых, как утверждает Д. В. Аносов, фактически решались квадратные уравнения и даже отдельные уравнения более высоких степеней.

Как отмечает академик Д. В. Аносов, традиционно считается, что "*наука как единая система знаний, не обязательно непосредственно связанных с практической деятельностью, и как отдельная сфера человеческой деятельности, имеющей своей целью получение новых знаний, возникла в Древней Греции*". За предшествующий период развития цивилизаций были накоплены немалые научные сведения, но, считается, что науки в современном понимании этого слова еще не было. Д. В. Аносов предлагает называть то, что было до греков, "протонаукой". Несколько иную точку зрения по этому вопросу в ряде своих работ высказывает академик В. И. Арнольд, утверждающий со ссылкой на ряд исследователей, что уровень развития науки в Древнем Египте был существенно выше, чем это традиционно считается.

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. К середине V века до н. э. уже устанавливается некоторый канон математического стиля изложения, который получил завершение в работах великих греческих классиков Архимеда, Апполония и Евклида. Понимание математического доказательства в их работах уже практически не отличается от современного. В качестве яркого примера, подтверждающего это утверждение, может служить евклидово доказательство бесконечности множества всех простых чисел, которое ничем существенным не отличается от современных доказательств. Удивление вызывает и сама постановка вопроса о бесконечности множества простых чисел. Как пишет Н. Бурбаки во введении одной из книг своего трактата "Начала математики": "Теории множеств" - "Со времен греков говорить "математика" – значит, говорить "доказательство". В Древней Греции "*протонаука*" завершила превращение в науку, причем это произошло с философией, астрономией, географией, биологией, математикой и с некоторыми частями физики. Как полагают некоторые исследователи, тому, что это произошло именно в Древней Греции способствовали особенности устройства греческого общества. Считается, что именно в Древней Греции впервые в человеческой истории получили общественное признание все виды продуктивной духовной деятельности, в том числе и лишённые непосредственного утилитарного значения. Это вызывает особое удивление и восхищение, если вспомнить, что в современной России начала XXI века, т. е. почти через две с половиной тысячи лет на государственном уровне фактически восторжествовало догреческое мировоззрение. Вновь подтверждается тезис, что история учит тому, что она ничему не учит. Как свидетельствуют историки, в Древней Греции общественная и культурная обстановка способствовала тому, что широкую известность получали авторы даже открытий, не имевших непосредственного практического значения. Дух соревновательности был присущ греческому обществу, главным была сама победа, а не материальные блага, с ней связанные. Так было в спорте, достаточно вспомнить об Олимпиадах, в искусстве, философии и науке, что не могло не создавать стимулов для творческих поисков в различных сферах интеллектуального творчества. И вновь наши взоры обращаются к современной России, но лучше воздержаться от комментариев по поводу того, насколько мы ушли назад, и от прогнозов к чему это может привести. Некому слышать такие прогнозы. Имеющий уши, да услышит! А если Бог не дал ушей? В Древней Греции дедуктивное построение математических теорий приобрело особый общественный статус. Особым достижением математики того периода было систематическое дедуктивное построение геометрии, к которой фактически сводилась основная часть древнегреческой математики.

На протяжении всей 4-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 выступает 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 выражаем 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* (2000 – 1550 гг. 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 ”Ars 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. Не только в мир этнических арабов, но и вообще в исламский мир. Арабский язык, язык Корана, стал на определенный

период развития цивилизации фактически международным языком, на котором писались научные труды и который должен был знать каждый образованный мусульманин.

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 степеней (С. Ферро (1465 – 1526), Н. Тарталья (1500 – 1557), И. Кардано (1501 – 1576), Л. Феррари (1522 – 1565)). В это же время было начато использование и 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 обращались с расплывчатыми понятиями *бесконечно малой* и *бесконечно большой* величин, оперировали с бесконечными суммами слагаемых по правилам, известным 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 рассматри-

вать 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 завершенного, 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 неравномощности 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 π и решение знаме-

нитой 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 предметом математики могло быть лишь то, что могло быть получено за конечное число шагов из натуральных чисел. Сама идея рассматривать бес-

конечность 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, лейбницевским 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 общеупотребительнейшие 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: в 1890 году Дж. Пеано при доказательстве своей теоремы о существовании решения дифференциального уравнения заметил, что он естественным образом пришел к "применению бесконечно много раз произвольного закона, который каждому классу ставит в соответствие индивид этого класса". Но тут же Дж. Пеано отметил, что такое доказательство для него не является приемлемым. Б. Леви в 1902 году утверждал, что подобное рассуждение в неявной форме использовал Ф. Бернштейн в доказательстве одной теоремы, относящейся к кардинальным числам. Еще раньше **Аксиому выбора** в неявном виде использовал Г. Кантор.

Приведем яркое высказывание Бертрانا 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 необ-

ходимость 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 осуществляла 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 исчисления 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 века, которое продолжалось и в XX веке, 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. Козна (1934 – 2007) 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.

По мнению ряда математиков, движущие силы развития математики – это *решение прикладных задач, включая использование математики и ее методов в других науках, решение математических проблем и разработка новых математических теорий.*

Трудно удержаться от комментариев по вопросу преподавания математики, особенно в школе. 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. Фрейдентала (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.

4.4.2. Из истории логики

С одной стороны, логика как наука о приемлемых способах рассуждений, как анализ методов рассуждений существует почти две с половиной тысячи лет, а с другой стороны, наиболее значительные результаты в ней были получены за последние 100 – 150 лет. Само слово "логика" весьма многозначно. Та часть логики, в которой интересуются прежде всего формой, а не содержанием рассуждений, обычно называется **формальной логикой**. Ее истоки можно обнаружить в дошедших до нашего времени зачастую отрывочных философских текстах. Если в VII – VI вв. до н. э. только *утверждают* или *прорицают*, приводя лишь в отдельных случаях туманные доводы, основанные на столь же туманной аналогии, то в греческих философских текстах V в. до н. э. уже прослеживается осознанное стремление распространить на многие области человеческой мысли приемы проведения рассуждений, которые к тому времени весьма успешно применяли математики и риторика. В этом можно видеть первые попытки создания формальной логики. Уже с Парменида и Зенона философы начинают *аргументировать*, выделяют некоторые общие положения, которые кладут в основу своих рассуждений. Именно у Парменида впервые формулируется **закон исключенного третьего**. Зенон успешно применял *доказательства методом приведения к противоречию*.

Особое место в истории развития логики занимает древнегреческий философ Аристотель (384 – 322 гг. до н. э.). Он родился в Стагире. В 367 году в Афинах стал учеником Платона и 20 лет, вплоть до смерти Платона в 347 году, был членом Платоновской Академии. В 343 году приглашен царем Македонии Филиппом в качестве воспитателя его сына Александра. В 335 году вернулся в Афины и создал там свою школу. Умер Аристотель в Халкиде на Эвбее, куда был вынужден бежать от преследования по обвинению в преступлении против религии.

Аристотель охватил почти все отрасли знания его времени. Дошедшие до нас сочинения Аристотеля делятся по содержанию на семь групп. Логические трактаты Аристотеля объединены в свод "Органон": "Категории", "Об истолковании", "Аналитики первая и вторая" и "Топика". Аристотель в сочинении "Топика" сформулировал основное правило исчисления высказываний - "Правило отделения заключения", с которым мы уже хорошо знакомы "Из A и $(A \rightarrow B)$ следует B ". Считается, что именно Аристотель был одним из создателей формальной логики, ему приписывается открытие возможности описания дедуктивных рассуждений через форму соответствующих высказываний. Аристотель обозначает понятия и высказывания буквами. Он систематизировал некоторые приемы рассуждений руководствуясь идеей, что каждое правильное рассуждение можно свести к применению небольшого числа правил, независимых от природы объектов, о которых идет речь. Аристотель оставался непревзойденным авторитетом в логике вплоть до XVII века.

В целом в период ранней античности логические идеи развивались и активно обсуждались в ряде философских школ. Особую роль в развитии логики

сыграл анализ языка, проведенный софистами в V в. до н. э., что было следствием высокой культуры ораторского искусства. Вклад поздней античности в историю логической мысли ограничивается лишь переводческой и комментаторской деятельностью. В качестве одного из семи свободных искусств логика становится необходимым элементом гуманитарного образования.

Раннее европейское средневековье (VII – XI вв.) не внесло весомого вклада в развитие логики, так как это был период освоения научного наследия античного мира под углом зрения христианского сознания. В Европе развивается в этот период лишь *схоластическая логика* – церковно-школьная дисциплина, направленная на обоснование и систематизацию христианского учения. Лишь в XII – XIII веках были канонизированы произведения Аристотеля и стала развиваться средневековая несхоластическая логика. В средние века логиками были открыты многие законы логики высказываний, в это же время *возникла идея механизации процесса логического вывода и сделаны первые попытки ее реализации*.

Два века эпохи Возрождения для дедуктивной логики были периодом застоя. Она воспринималась как опора схоластики, как искусственное мышление, освящающее схематизм умозаключений, посылки которых обоснованы авторитетом веры, а не познания. Лишь к середине XVII века интерес к дедуктивной логике, как рабочему инструменту всех наук, требующему строго формулировать мысли, вновь стал пробуждаться. И особую роль на этом этапе развития логики сыграл немецкий философ, математик, физик и изобретатель, юрист, историк и языковед Готфрид Вильгельм Лейбниц (1.07.1646, Лейпциг, – 14.11.1716, Ганновер). В логике Г. В. Лейбниц развил учение об анализе и синтезе, ему принадлежит принятая в современной логике формулировка закона тождества. В работе Г. В. Лейбница "Об искусстве комбинаторики", написанной в 1666 году, предвосхищены некоторые моменты современной математической логики. *Логика находилась в центре больших проектов Г. В. Лейбница по формализации языка и мышления. Г. В. Лейбниц выдвинул идею применения в логике математической символики и построений логических исчислений, поставил задачу логического обоснования математики, предложил использовать бинарную систему счисления для целей вычислительной математики. Г. В. Лейбниц одним из первых стал рассматривать логику как дисциплину, идеи и методы которой лежат в основе многих других наук.* Важнейшей заслугой Г. В. Лейбница является разработка (наряду с И. Ньютоном и независимо от него) дифференциального и интегрального исчислений.

Г. В. Лейбниц высказал мысль о создании "всеобщей символики", универсального символического языка, свободного от многозначностей естественных разговорных языков, который был бы способен точно и однозначно выражать мысли и понимался бы без перевода. Этот язык, по замыслу Г. В. Лейбница, должен был стать для человеческих мыслей тем же, чем алгебраические обозначения являются для алгебры. Этот искусственный язык выполнял бы роль международного языка, служил бы орудием получения новых истин из известных. Лейбниц фактически понимает *формализованный язык как просто комби-*

нацию знаков. Г. В. Лейбниц пришел к идее нахождения простейших исходных понятий, "алфавита человеческих мыслей", комбинируя которые по определенным правилам, можно получить все остальные точно определимые понятия. По мнению Г. В. Лейбница, это позволило бы *создать универсальный алгоритм, позволяющий доказать все истинные утверждения, решать все математические проблемы*. Г. В. Лейбниц предложил несколько подходов к арифметизации логики, один из которых ведет к геделевской нумерации. Под воздействием этих идей Г. В. Лейбниц разработал символику исчисления бесконечно малых. В сочинениях Г. В. Лейбница содержатся начала математической (дедуктивной) логики. Его идеи оказали влияние на развитие алгебрологических методов в логике. В течение всего XVIII века и начала XIX века интерес к формальной логике был незначительным, что частично объясняется влиянием с середины XVIII века Э. Канта, считавшего, что "нам не нужны никакие новые изобретения в логике", так как достаточно того, что сделал в логике Аристотель.

Хотя Леонард Эйлер (4(15).4.1707, Базель, Швейцария, – 7(18).9.1783, Петербург), математик, механик и физик, непосредственно не занимался вопросами логики, однако в силу разносторонности своего математического интеллекта он не мог не оказать влияния на ее развитие, в частности, Л. Эйлеру приписывается использование кругов для представления логических предложений.

Другим создателем графического аппарата для представления предложений логики, получившим название диаграмм Венна, был Джон Венн (4.8.1834, Драйпул, близ Халла, – 4.4.1923, Кембридж), английский логик, работавший в области логики классов.

В XIX веке появились первые попытки алгебраизации логики, построения логической теории алгебраического характера, что способствовало формированию алгебры логики. Создателем современной символической логики по праву считается Джордж Буль (2.11.1815, Линкольн, – 8.12.1864, Баллинтемпл близ Корка), английский математик и логик, одним из первых предпринявший попытки, достаточно успешные, алгебраизации логики. Не имея специального математического образования, в 1849 году стал профессором математики в Куинс-колледже в Корке (Ирландия), в котором преподавал до конца жизни. Дж. Буль интересовался логикой, математическим анализом, теорией вероятностей, этикой Спинозы, философскими работами Аристотеля и Цицерона. В работах "Математический анализ логики" (1847), "Логическое исчисление" (1848), "Исследование законов мышления" (1854) Дж. Буль заложил основы алгебрологического этапа в истории математической логики. Им разработана алгебра логики как некая алгебраическая система. Он обозначает пересечение множеств A и B через AB , объединение – через $A + B$ в случае, когда A и B не имеют общих элементов. Само понятие "алгебра логики" было введено позже Ч. С. Пирсом. Чарлз Сандерс Пирс (10.9.1839, Кембридж, Массачусетс, – 19.4.1914, Милфорд, Пенсильвания), американский философ, логик, математик и естествоиспытатель. Читал лекции по логике, истории и философии науки в Гарвардском университете, университете Дж. Хопкинса в Балтиморе. Им выполнены работы по классификации суждений и типов доказательств, по изу-

чению природы логики и ее взаимоотношения с математикой, по определению пределов и возможностей формализации. Им изучены некоторые минимальные системы логических операций, через которые выражаются остальные операции (стрелка Пирса). Дж. Буль стремился ввести в создаваемую им алгебру логики все основные арифметические операции. Однако оказалось трудным интерпретировать логически операции вычитания и деления. Дальнейшие усовершенствования внес У. С. Джевонсон, который распространил понятие объединения $A + B$ множеств A и B на общий случай. Уильям Стэнли Джевонсон (1.9.1835, Ливерпуль, – 13.8.1882, близ Гастингса), английский экономист, статистик и философ-логик. Был профессором логики, философии и политической экономии в Манчестере (1866 – 1876) и Лондоне (1876 – 1880). У. С. Джевонсон успешно продолжил работы Дж. Буля по алгебраизации логики, именно он построил алгебраическую систему, называемую теперь *булевой алгеброй*. Де Морган (27.06.1806 – 18.03.1871) в 1858 г. и Ч. С. Пирс в 1867 г. доказали законы двойственности

$$\mathbb{C}(A \cup B) = \mathbb{C}(A) \cap \mathbb{C}(B), \quad \mathbb{C}(A \cap B) = \mathbb{C}(A) \cup \mathbb{C}(B).$$

Платон Сергеевич Порецкий (3(15).10.1846, Елизаветград, ныне Кировоград, – 9(22).8.1907, село Жоведь, ныне Черниговской области), русский математик, астроном, логик. П. С. Порецкий внес значительный вклад в развитие математической логики, которую он определял как *”логика по предмету, математика по методам”*. Он первым из русских ученых читал лекции по математической логике и ее приложениям к теории вероятностей. П. С. Порецкий развивал идущие от Дж. Буля, У. С. Джевонса и Э. Шредера (25.11.1841 – 16.06.1902) идеи в области алгебры логики, понимаемой им как *”исчисление логических равенств”*. Он наряду со Шредером развил методы решения логических уравнений.

В конце XIX века благодаря работам Дж. Пеано, Ч.С. Пирса, Г. Фреге, Б. Рассела, А. Н. Уайтхеда и Д. Гильберта в математической (дедуктивной) логике произошли революционные изменения. С этого времени начался современный этап истории математической логики.

Джузеппе Пеано (27.8.1858, Кунео – 20.4.1932, Турин), итальянский математик. С 1890 г. профессор Туринского университета. Много внимания уделил вопросам формально-логического обоснования математики, издал *”Формуляр математики”*, написанный формализованным языком, который содержал, кроме математической логики, немало значительных результатов из многих разделов математики. Введенная Дж. Пеано символика близка к применяемой в повседневной математической практике, вводит многочисленные и хорошо подобранные символы-сокращения. Вот несколько примеров введенных Дж. Пеано знаков \in , \supset , \cup и \cap . В работах Г. Фреге и Дж. Пеано были разработаны основные положения формализованных языков, которыми пользуются и в настоящее время. В 1889 году Дж. Пеано предложил систему аксиом для арифметики натуральных чисел в терминах функции следования $S(x) = x + 1$. Сходная система аксиом была предложена несколько ранее, в 1888 году, Р. Дедекиндом.

Дж. Пеано много занимался вопросами выражения математических теорем в логических символизмах.

Готлоб Фреге (8.11.1848, Висмар, – 26.7.1925, Бад-Клейнен), немецкий логик, в 1879 – 1918 гг. профессор университета в Йене. Главный труд Г. Фреге "Основные законы арифметики" (1893 – 1903), в котором он предложил систему формализованной арифметики на основе разработанного им расширенного исчисления предикатов. Работы Г. Фреге отличаются чрезвычайной точностью и подробностью анализа понятий.

Бертран Рассел (18.5.1872, Треллек, Уэльс, – 2.2.1970, Пенриндайдрайт, Уэльс), английский философ, логик, математик, социолог, общественный деятель, был профессором различных университетов Великобритании и США. Большое место в его работах занимает разработка философских вопросов математики. Им открыт один из парадоксов теории множеств, получивший название парадокса Рассела. Совместно с А. Н. Уайтхедом – основатель логистической школы в философии математики. Ими создан трехтомный капитальный труд "Принципы математики" ("Principia Mathematica"), в котором было систематизировано и развито дедуктивно-аксиоматическое построение логики, имевшее целью логическое обоснование математического анализа. В этой работе точность Г. Фреге удачно сочетается с удобством системы Дж. Пеано. Этот язык стал наиболее распространенным, большинство современных формализованных языков отличается от него лишь второстепенными изменениями, направленными на упрощение применения.

Альфред Норт Уайтхед (15.2.1861, Рамсгит, Кент, – 30.12.1947, Кембридж, Массачусетс), английский математик, логик и философ. Совместно с Б. Расселом – основатель логистической школы в философии математики.

Давид Гильберт (23.1.1862, Велау, близ Кенигсберга, – 14.2.1943, Геттинген), немецкий математик, исследования которого оказали большое влияние на развитие многих разделов математики XX века. Деятельность Д. Гильберта в Геттингенском университете, по мнению А. Н. Колмогорова, в значительной мере содействовала тому, что Геттинген в первой трети XX века являлся одним из основных мировых центров математической мысли (до прихода гитлеровцев к власти в Германии в 1933 году).

Андрей Николаевич Колмогоров (12(25).4.1903, Тамбов, – 20.10.1987, Москва), советский математик, внес выдающийся вклад во многие разделы современной математики – теорию функций действительного переменного, конструктивную логику, топологию, механику, теорию дифференциальных уравнений, функциональный анализ, теорию вероятностей, теорию информации.

К 1922 году у Д. Гильберта сложился обширный план обоснования всей математики путем ее полной формализации с последующим метаматематическим доказательством непротиворечивости формализованной математики. Д. Гильбертом совместно с П. Бернайсом написаны и изданы в 1934 и 1939 гг. два тома "Оснований математики", в которых подробно излагалась эта концепция обоснования математики. Надежды Д. Гильберта не оправдались – как показал К. Гедель, проблема непротиворечивости формализованных теорий оказалась

намного глубже и труднее.

Курт Гедель (28.4.1906, Брюнн (Брно), – 14.1.1978, Принстон, Нью Джерси), американский математик и логик австрийского происхождения. С 1953 года профессор Института перспективных исследований в Принстоне. К. Гедель – один из величайших логиков не только XX века, но и почти всего более чем двухтысячелетнего периода развития логики. Ему принадлежат теоремы о полноте для исчисления предикатов и знаменитые теоремы о неполноте, являющиеся выдающимся явлением не только для математики, но и для всей науки и культуры.

Была преодолена ограниченность чисто алгебраического подхода к логике, осознано значение математической логики для математики в целом, началось ее применение в исследованиях по основаниям математики и теории множеств. Г. Фреге начиная с работы 1879 года "Исчисление понятий" выполнил строгое аксиоматическое построение исчислений высказываний и предикатов. Предложенная им формализация логики включала в себя все основные элементы логических исчислений: пропозициональные и предметные переменные, кванторы и предикаты. Он акцентировал внимание на различиях между логическим законом и правилом вывода, между константой и переменной. Г. Фреге на основе развитой им логики предикатов разработал системы формализованной арифметики. Предложенная Г. Фреге символика не утвердилась в логике. Используемая в современной математической логике символика ведет свое начало от Дж. Пеано.

Логицизм – одно из основных направлений исследований в области оснований математики. Основной постулат логицизма – это утверждение о возможности и необходимости "сведения математики к логике", т. е. определения всех неопределяемых математических понятий в чисто логических терминах и доказательство всех математических теорем чисто логическими средствами. При таком подходе математика становится частью логики. Идеи логицизма восходят к Г. Лейбницу. Доктрина логицизма была впервые четко сформулирована Г. Фреге, который предложил подход к сведению понятия натурального числа к логическим понятиям. Г. Фреге детально разработал логическую систему, средствами которой ему удалось доказать основные арифметические теоремы. Так как к тому времени была в основном завершена арифметизация математического анализа, геометрии и алгебры, то, по мнению Г. Фреге, можно было утверждать и о выполнимости в основном логицистической программы. Однако еще до завершения публикации двухтомного труда Г. Фреге Б. Рассел обнаружил в его системе противоречие (парадокс Б. Рассела). Б. Рассел совместно с А. Н. Уайтхедом предприняли попытку исправить систему Г. Фреге и спасти ее от противоречий. С этой целью они проделали большую работу по формализации логики, итогом которой стал их совместный трехтомный труд "Principia Mathematica" (1910 – 1913), в котором логика строится в виде ступенчатого исчисления РМ – теории типов, что позволяло избавиться от всех известных в то время парадоксов. Книга "Principia Mathematica" оказала огромное влияние на развитие символической логики. Однако, как показал К. Гедель системы типа

РМ существенно неполны, т. е. на их языке можно сформулировать математические утверждения, которые средствами этой системы нельзя ни доказать, ни опровергнуть. Логицистическая программа "чисто логического" обоснования математики оказалась невыполнимой. Позднее различные усовершенствования системы РМ были предложены рядом математикой, в том числе американским математиком У. ван О. Куайном (1908 – 2000).

Работы Г. Фреге, Б. Рассела, А. Н. Уайтхеда, У. ван О. Куайна и их единомышленников оказали большое влияние на развитие математической логики и математики, способствовали формированию и уточнению важнейших логико-математических идей, разработке необходимого математического аппарата.

Математический интуиционизм - одно из основных направлений исследований в области оснований математики. Основной постулат интуиционизма – "интуиция – единственный источник математики и главный критерий строгости ее построений". Интуиционистская идеология восходит к античной математике, ее основные положения в той или иной мере разделялись такими выдающимися математиками, как К. Ф. Гаусс, Л. Кронекер, А. Пуанкаре, А. Лебег, Э. Борель, Г. Вейль.

Карл Фридрих Гаусс (30.4.1777, Брауншвейг, – 23.2.1855, Геттинген), немецкий математик, внесший фундаментальный вклад во многие разделы математики. Отличительной чертой творчества К. Ф. Гаусса была необычайная широта проблематики его исследований как в области самой математики, так и в сфере ее приложений. В ряде областей математики работы К. Ф. Гаусса содействовали повышению требований к логической отчетливости доказательств, но сам К. Ф. Гаусс не принимал активного участия в проводившейся в то время работе по обоснованию математического анализа. Но именно К. Ф. Гаусс первым осознал необходимость точной формулировки теоремы об однозначном разложении натуральных чисел на простые множители, так называемой *основной теоремы арифметики*.

Леопольд Кронекер (7.12.1823, Лигниц, ныне Легница, Польша, – 29.12.1891, Берлин), немецкий математик, был сторонником "арифметизации" математики, которая, по его мнению, должна быть сведена к арифметике целых чисел. По мнению Л. Кронекера, только арифметика целых чисел обладает подлинной реальностью. Руководствуясь этим принципом, Л. Кронекер вел упорную борьбу с принципами теоретико-функциональной школы К. Вейерштрасса и теоретико-множественной школы Г. Кантора.

Георг Кантор (3.3.1845, Петербург, – 6.1.1918, Галле), немецкий математик, разработавший теорию бесконечных множеств и теорию трансфинитных чисел. В 1874 году доказал несчетность множества всех действительных чисел. В 1879 – 1884 гг. Г. Кантор в серии работ изложил основные принципы своего учения о бесконечности. Революционные идеи Г. Кантора встретили со стороны ряда его современников резкое неприятие, однако впоследствии они оказали огромное влияние на развитие многих разделов математики XX века.

В 1880-х годах Л. Кронекер утверждал, что процветавшие тогда методы К. Вейерштрасса, Р. Дедекинда и Г. Кантора ненадежны, что используемые

ими фундаментальные понятия – просто слова, так как они не дают возможность проверить, удовлетворяет ли рассматриваемый объект определению.

Жюль Анри Пуанкаре (29.4.1854, Нанси, – 17.7.1912, Париж), французский математик, труды которого, с одной стороны, завершают классическое направление в математике, а с другой стороны, открывают путь к развитию новой математики, в которой, в частности, наряду с количественными соотношениями важную роль играют и факты качественного характера. А. Пуанкаре считал, что математическая индукция – ни к чему более простому не сводимое орудие интуитивных математических рассуждений. Поэтому его рассматривают как одного из предшественников математического интуиционизма.

Анри Лебег (28.6.1875, Бове, департамент Уаза, – 26.7.1941, Париж), французский математик, один из основателей современной теории функций действительного переменного, создатель теории меры, ввел понятие измеримой функции и новое определение интеграла, позволившего чрезвычайно расширить класс интегрируемых функций.

Эмиль Борель (7.1.1871, Сент-Африк, – 3.2.1956, Париж), французский математик, создатель нескольких разделов современного математического анализа.

Герман Вейль (9.11.1885, Эльмсхорн, Шлезвиг-Гольштейн, – 8.12.1955, Цюрих), немецкий математик, с 1933 года работал в США в Принстоне в Институте перспективных исследований (Institute for Advanced Study). Наиболее важные результаты получил в области непрерывных групп и их представлений с применениями к геометрии и физике.

Но основным идеологом интуиционизма по праву считается Л. Э. Я. Брауэр, который в начале XX века выступил с развернутой критикой основных положений классической математики и радикальной интуиционистской программой перестройки математического здания.

Лейтзен Эгберт Ян Брауэр (27.2.1881, Оверсхи, – 2.12.1966, Амстердам), голландский математик, с 1908 года последовательно проводил критику так называемых чистых доказательств существования, опирающихся на закон исключенного третьего, что в итоге положило начало особому направлению в области оснований математики – **математическому интуиционизму**. Особую ценность имеет проведенный Л. Э. Я. Брауэром анализ математических доказательств существования объектов с точки зрения возможности построения соответствующих объектов.

В статье "Недостоверность логических принципов", опубликованной в 1908 году, Л. Э. Я. Брауэр поставил под сомнение абсолютную веру в правила классической логики, которые оставались неизменными со времен Аристотеля (384 – 322 гг. до н. э.). Г. Вейль так излагал точку зрения Л. Э. Я. Брауэра: *"Согласно его взглядам и пониманию истории, классическая логика была абстрагирована от математики конечных множеств и их подмножеств... Забывая об этом ограниченном происхождении, впоследствии эту логику приняли ошибочно за нечто высшее и первичное по отношению ко всей математике и в конце концов стали применять ее без какого-либо оправдания к математи-*

ке бесконечных множеств”. Можно привести простые примеры утверждений, истинных для конечных множеств натуральных чисел, но ложные для бесконечных. Формирование интуиционистской идеологии шло в достаточно острой полемике с возглавляемым Д. Гильбертом еще одним из основных направлений исследований в области оснований математики – **математическим формализмом**. Л. Э. Я. Брауэр не принимал теоретико-множественные основания математики, веру в актуальный характер бесконечных множеств, правомерность переноса в область бесконечного логических принципов, выработанных при работе с конечными множествами. В частности, им отвергался *закон исключенного третьего*. С точки зрения интуиционистов предметом исследования в математике являются *умственные построения*, которые рассматриваются ”безотносительно к таким вопросам о природе конструируемых объектов, как вопрос, существуют ли эти объекты независимо от нашего знания о них” (А. Гейтинг). Математические утверждения, по мнению интуиционистов, дают некоторую информацию о выполненных построениях. Классическая и интуиционистская математики придерживаются существенно разных точек зрения на бесконечные множества. Классическая математика рассматривает бесконечность как *актуальную, экзистенциальную или завершенную*. Бесконечные множества рассматриваются как завершенные объекты, с которыми можно выполнять дальнейшие построения, в частности, они могут быть элементами других множеств. Интуиционистская математика рассматривает бесконечность как *потенциальную или становящуюся*. Эта точка зрения на бесконечность восходит к Г. Ф. Гауссу, который утверждал: ”Я возражаю... против употребления бесконечной величины, как чего-либо завершенного, что никогда не позволительно в математике”. Г. Вейль считал, что ”Брауэр выяснил и, как мне кажется, не оставил сомнения в том, что не существует доводов, защищающих веру в экзистенциальный характер совокупности всех натуральных чисел... Этот ряд чисел, который растет, не останавливаясь ни на какой стадии, за счет перехода к следующему числу, представляет собой многообразие возможностей, открытых для бесконечности; он вечно остается в состоянии становления, а не является замкнутым царством вещей, существующих в себе. То, что мы слепо превращаем одно в другое, является истинным источником наших трудностей, в том числе антиномий, – источником более глубокой природы, чем указанный Расселом принцип порочного круга. Брауэр открыл нам глаза и показал, как далеко классическая математика, вскормленная превосходящей всякую человеческую способность реализации верой в ”абсолютное”, идет дальше таких утверждений, которые могут претендовать на реальный смысл и истинность, основанную на доказательствах”.

Интуиционистская и классическая математики несколько по-разному понимают (трактуют) логические связки. Например, с точки зрения интуиционистской математики доказательство утверждения ”существует объект a , обладающий свойством A ”, должно давать *метод (алгоритм) построения конкретного объекта a , обладающего свойством A* . Однако в классической математике достаточно широко распространены косвенные доказательства суще-

ствования, в которых из предположения $(\forall x)(\neg A)$ выводится противоречие, на основании чего делается вывод, что $\neg(\forall x)(\neg A)$, а затем получают, что $(\exists x)A$. Нередко из такого доказательства не видно, как построить конкретный объект a , обладающий свойством A . В качестве примера рассмотрим традиционное доказательство частного случая теоремы Л. Э. Я. Брауэра о неподвижной точке "Любое непрерывное отображение единичного круга D в себя имеет неподвижную точку". Пусть f – непрерывное отображение единичного круга D в себя. Предположим, что для любой точки u единичного круга D выполняется неравенство $f(u) \neq u$. Для произвольной точки u единичного круга D обозначим через $\varphi(u)$ точку пересечения с границей круга D , т. е. с единичной окружностью S , луча, идущего из точки $f(u)$ в u . Нетрудно убедиться в том, что отображение $\varphi : u \mapsto \varphi(u)$ отображает единичный круг D на его границу единичную окружность S , причем точки единичной окружности S при этом остаются на месте. Получили, что единичная окружность S является ретрактом единичного круга D . Используя алгебраические методы, например, понятие фундаментальной группы, можно доказать, что единичная окружность S не является ретрактом единичного круга D . Из полученного противоречия получаем, что наше предположение $(\forall x \in D)(f(x) \neq x)$ ложно, т. е. $\neg(\forall x \in D)\neg(f(x) = x)$. В "классической математике" отсюда следует $(\exists x \in D)f(x) = x$. Однако из предложенного доказательства трудно извлечь способ, позволяющий для произвольного непрерывного отображения f единичного круга D в себя находить его неподвижную точку, т. е. такую точку $u \in D$, для которой выполняется равенство $f(u) = u$. Подобное доказательство существования не принимается интуиционистской математикой.

Существует специфика и в понимании интуиционистами логической связки дизъюнкции \vee – их понимание дизъюнкции $A \vee B$ отличается от классического. Не претендуя на исчерпывающую полноту изложения, поясним на теперь хорошо известном примере эту специфику. Рассмотрим два доказательства утверждения "существуют два иррациональных числа α и β таких, что число α^β является рациональным".

Классическое доказательство. Если число $\sqrt{2}^{\sqrt{2}}$ является рациональным, то полагаем $\alpha = \sqrt{2}$ и $\beta = \sqrt{2}$.

Если число же $\sqrt{2}^{\sqrt{2}}$ является иррациональным, то полагаем $\alpha = \sqrt{2}^{\sqrt{2}}$ и $\beta = \sqrt{2}$.

С точки зрения классической математики теорема доказана. В интуиционистской же математике такое доказательство не считается приемлемым, так как оно не дает возможность ответить на вопрос, какая из двух рассмотренных возможностей на самом деле имеет место.

С точки зрения интуиционистской математики нами лишь доказана импликация вида $((A \vee \neg A) \rightarrow B)$, где через A обозначено утверждение "число $\sqrt{2}^{\sqrt{2}}$ является рациональным", а через B – утверждение "существуют два иррациональных числа α и β таких, что число α^β является рациональным". Но так как в интуиционистской математике не принимается закон исключенного

третьего $(A \vee \neg A)$, то из этой импликации мы не можем получить требуемое утверждение B .

Интуиционистское доказательство могло бы выглядеть следующим образом. А. О. Гельфондом в качестве ответа на вопрос Д. Гильберта из его седьмой проблемы получен замечательный результат, доказательство которого чрезвычайно сложно: "*число $2^{\sqrt{2}}$ является трансцендентным*". Поэтому число $\sqrt{2}^{\sqrt{2}}$ также трансцендентно, а значит, иррационально. Значит, имеет место первая альтернатива, но при условии, что доказательство А. О. Гельфонда удовлетворяет интуиционистским критериям истинности. Значит, доказываемому утверждению удовлетворяет пара чисел $\alpha = \sqrt{2}$ и $\beta = \sqrt{2}$.

Заметим, что классическое доказательство выглядит существенно короче, однако оно менее информативно, чем интуиционистское.

Л. Э. Я. Брауэр и его единомышленники в серии работ начиная с 1918 года выполнили построение основных разделов интуиционистской математики – теории множеств, геометрии, топологии, математического анализа. В теории чисел неинтуиционистские методы не играют существенной роли, так как во многих случаях неконструктивные доказательства существования можно заменить конструктивными, хотя, как правило, существенно более длинными. В то же время в математическом анализе неинтуиционистские методы играют очень важную роль, начиная с построения действительных чисел, которые трактуются как бесконечные множества рациональных чисел. Т. е. уже на начальном этапе используется актуальная бесконечность. **Закон исключенного третьего** также играет существенную роль при определении отношения порядка для действительных чисел. К концу XX века интуиционистская математика была уже достаточно глубоко разработана. Отказ от рассмотрения в качестве объекта исследования бесконечных множеств как актуально заданных и требование эффективности всех осуществляемых построений привели к тому, что ряд интуиционистских вариантов традиционных разделов математики имеют с точки зрения классической математики достаточно своеобразный вид. Приведем в изложении Гейтинга некоторые взгляды Л. Э. Я. Брауэра "Согласно Брауэру, математика тождественна с точной частью нашего мышления... Никакая наука – в частности, ни философия, ни логика – не может служить предпосылкой для математики. Было бы порочным кругом применять в качестве средств для доказательства какие-либо философские или логические принципы, потому что в формулировке этих принципов уже предполагаются математические понятия". Для математики не остается "никакого другого источника, кроме интуиции, которая с непосредственной ясностью помещает перед нашими глазами математические понятия и выводы". Эта интуиция "является не чем иным, как способностью рассматривать в отдельности различные понятия и выводы, регулярно встречающиеся в обычном мышлении". "В интуиционистской математике выводы не извлекаются по фиксированным правилам, которые можно объединить в логику, а каждый вывод в отдельности непосредственно подтверждается своей очевидностью". Кроме того, "имеются общие правила, посредством которых из данных математических теорем можно интуитивно ясным

образом получать другие; теорию этих соотношений можно рассматривать в некоторой "математической логике", которая при этом является отраслью математики и не имеет ощутимых применений вне математики".

Л. Э. Я. Брауэр возражал против попыток формализации интуиционистской математики и логики, так как считал критерием верности построений прежде всего интуицию. Однако значительные успехи в изучении интуиционистской логики были достигнуты после того, как ее основные законы были сформулированы в виде соответствующих исчислений, которые были исследованы методами математической логики. Это позволило понять значение и особенности интуиционистской логики по сравнению с традиционной, что невозможно было сделать без точных формулировок. Л. Э. Я. Брауэр и его единомышленники в своих исследованиях выяснили, какая получается математика при последовательном проведении генетической точки зрения на образование математических понятий.

Математический формализм – одно из основных направлений исследований в области оснований математики, главным идеологом которого выступил Д. Гильберт. Основной постулат формализма *"каждый раздел математики может, а на определенном этапе своего развития и должен, быть полностью формализован"*, т. е. представлен в виде формальной системы или исчисления, которая будет развиваться по точно определенным правилам. При таком подходе обоснованием существования того или иного раздела математики становится не его интерпретация в терминах некоторой внешней по отношению к нему действительности, а лишь его *непротиворечивость*. Уже при переходе от "материальной" аксиоматики Евклида к "формальной" аксиоматике геометрии в монографии Д. Гильберта "Основания геометрии" (1899 г.) произошло существенное развитие и уточнение аксиоматического метода.

Д. Гильбертом была предложена программа вывода классической математики из кризиса, вызванного открытием парадоксов. Причем эта программа коренным образом отличалась от программы, провозглашенной Л. Э. Я. Брауэром и его единомышленниками.

Д. Гильберт исходил из признания того, что утверждения классической математики, содержащие актуальную бесконечность, не могут считаться интуитивно ясными. Однако он в отличие от Л. Э. Я. Брауэра был решительно против отказа от достижений классической математики. Он говорил: "Никто не сможет изгнать нас из рая, созданного для нас Кантором". Для спасения классической математики от интуиционистской критики им была предложена программа, суть которой кратко можно сформулировать следующим образом: *"переформулировать классическую математику в виде формальной аксиоматической теории и финитными методами доказать непротиворечивость этой теории"*.

Традиционный метод доказательства непротиворечивости аксиоматической теории до конца XIX века состоял в построении **модели** этой теории средствами другой теории. При таком подходе каждому объекту и первоначальному понятию рассматриваемой аксиоматической теории T сопоставляется объект

или понятие другой теории T^* . Тогда каждому утверждению \mathcal{A} аксиоматической теории T соответствует некоторое утверждение \mathcal{A}^* теории T^* , причем выполняются равенства

$$\begin{aligned}(\neg \mathcal{A})^* &= (\neg \mathcal{A}^*), & (\mathcal{A} \& \mathcal{B})^* &= (\mathcal{A}^* \& \mathcal{B}^*), & (\mathcal{A} \vee \mathcal{B})^* &= (\mathcal{A}^* \vee \mathcal{B}^*), \\ (\mathcal{A} \rightarrow \mathcal{B})^* &= (\mathcal{A}^* \rightarrow \mathcal{B}^*), & ((\forall x)\mathcal{A})^* &= (\forall x)\mathcal{A}^*, & ((\exists x)\mathcal{A})^* &= (\exists x)\mathcal{A}^*.\end{aligned}$$

Причем теория T^* подбирается таким образом, чтобы для каждой аксиомы \mathcal{A} аксиоматической теории T утверждение \mathcal{A}^* было теоремой теории T^* .

Если бы аксиоматическая теория T оказалась противоречивой, т. е. в ней выводимы две формулы \mathcal{A} и $(\neg \mathcal{A})$, то в теории T^* оказались бы выводимы соответствующие формулы \mathcal{A}^* и $(\neg \mathcal{A}^*)$. Таким образом вопрос о непротиворечивости аксиоматической теории T сводится к вопросу о непротиворечивости теории T^* .

Например, аналитическая геометрия, т. е. использование координат для представления геометрических объектов, позволяет свести вопрос о непротиворечивости геометрических теорий к вопросу о непротиворечивости теории действительных чисел.

Построенные А. Пуанкаре модели плоской геометрии Н. И. Лобачевского в круге и в верхней полуплоскости и построенная Ф. Клейном модель в круге сводят *вопрос о непротиворечивости плоской геометрии Н. И. Лобачевского к аналогичному вопросу для евклидовой геометрии плоскости*. Напомним основные этапы построения модели А. Пуанкаре плоскости Лобачевского в верхней евклидовой полуплоскости. Фиксируем на евклидовой плоскости ортогональную декартову систему координат. "Точками плоскости Лобачевского" будем считать точки верхней евклидовой полуплоскости, определяемой осью OX , которую будем называть *граничной прямой*, т. е. "точки плоскости Лобачевского", – это точки евклидовой плоскости с координатами (x, y) , где $y > 0$, а граничная прямая состоит из всех точек с координатами $(x, 0)$. При этом точку A с координатами (a, b) будем отождествлять с комплексным числом $z = a + bi$. "Прямые плоскости Лобачевского" – это полуокружности, расположенные в верхней евклидовой полуплоскости и ортогональные ее граничной прямой, включая полуокружности "бесконечного радиуса", т. е. лучи, расположенные в этой верхней евклидовой полуплоскости и ортогональные ее граничной прямой. *Метрика* $\rho(x, y)$ в этой модели определяется следующим образом: если A и B – две точки верхней полуплоскости, S – полуокружность, проходящая через точки A и B , расположенная в верхней полуплоскости и ортогональная ее граничной прямой, а X и Y – точки пересечения полуокружности S с граничной прямой, то

$$\rho(A, B) = c |\ln |[A, B, X, Y]| |, \quad \text{где}$$

$$[A, B, X, Y] \text{ — двойное отношение, т. е. } \frac{X - A}{X - B} : \frac{Y - A}{Y - B}.$$

В этой формуле c – некоторая константа. *Движения* в рассматриваемой модели плоскости Лобачевского – *дробно-линейные преобразования, переводящие верхнюю полуплоскость в себя.*

Отобразив дробно-линейным преобразованием верхнюю полуплоскость на единичный круг, получим модель А. Пуанкаре в круге плоскости Лобачевского.

В модели Ф. Клейна "точками плоскости Лобачевского" служат внутренние точки некоторого фиксированного круга, а "прямыми плоскости Лобачевского" – хорды этого круга.

Метод доказательства непротиворечивости одной теории путем построения ее модели средствами другой теории является относительным, так как сводит вопрос о непротиворечивости исходной теории к аналогичному вопросу для теории, средствами которой строится модель. Для доказательства непротиворечивости теории множеств, математического анализа и арифметики этот метод мало пригоден, так как не видно "более надежных" и "более простых" математических теорий для построения моделей указанных теорий.

Д. Гильбертом был предложен новый прямой подход к доказательству непротиворечивости. Так как непротиворечивость теории T означает, что для нее невозможна ситуация, когда доказано некоторое утверждение A и его отрицание $\neg A$, то Д. Гильберт и предложил изучить все доказательства теории T и установить, что такая ситуация не может возникнуть. Д. Гильберту принадлежит идея метода *формализации доказательств*.

Таким образом, сама теория T , система всех ее доказательств становится объектом изучения некоторой новой математической теории, которую Д. Гильберт назвал "*метаматематикой*" или "*теорией доказательств*".

Особый интерес представляет учение Д. Гильберта о "*действительных*" и "*идеальных*" утверждениях классической математики. По Д. Гильберту, "*действительные утверждения*" – утверждения, имеющие содержательный смысл, а "*идеальные утверждения*" – это утверждения, которые не рассматриваются как имеющие содержательный смысл. Например, утверждения с использованием актуальной бесконечности можно рассматривать как идеальные. По Д. Гильберту, в классической математике к действительным утверждениям присоединяются идеальные, что позволяет при работе с бесконечными множествами пользоваться простыми законами аристотелевой логики. Добавление "идеальных элементов" для пополнения структуры системы и упрощение ее теории широко распространено в математике. Например, присоединение к евклидовой плоскости бесконечно удаленных точек и бесконечно удаленной прямой ведет к проективной геометрии, в которой отношение инцидентности между точками и прямыми становится проще, чем в евклидовом случае. Другие примеры расширения системы объектов с целью некоторого упрощения теории дают расширения числовых систем - переход от натуральных чисел к целым упрощает теорию сложения, так обратная операция, вычитание, становится всегда выполнимой, переход к рациональным числам делает всегда выполнимым деление, кроме деления на нуль, переход к действительным числам упрощает теорию длин, площадей и объемов, а переход к комплексным числам упрощает

теорию алгебраических уравнений.

Против подхода Д. Гильберта решительно возражали Л. Э. Я. Брауэр и его единомышленники. Приведем высказывание Л. Э. Я. Брауэра на этот счет "Неправильная теория, не наткнувшись на противоречие, не становится от этого менее неправильной, подобно тому как преступное поведение, не остановленное правосудием, не становится от этого менее преступным". С последней частью высказывания Л. Э. Я. Брауэра можно и не согласиться, так как "преступное поведение" становится таковым, лишь когда это будет признано судом, а значит, в той или иной мере остановлено. Д. Гильберт возражал "Отнять у математиков закон исключенного третьего – это то же, что забрать у астрономов телескоп или запретить боксерам пользоваться кулаками". Д. Гильберт в одной из своих статей утверждал, что не закон исключенного третьего, а недопустимые и бессмысленные образования понятий повинны в парадоксах теории множеств. Кроме того, он вполне оправданно считал, что его "игра формулами" содействует изучению "техники нашего мышления". Классическая математика может рассматриваться как простая и изящная *систематизирующая схема*, с помощью которой совокупность казавшихся разнородными и не связанными друг с другом утверждений, объединяются в виде следствий из "идеальных" теорем этой теории. Например, методы аналитической теории чисел, не имеющие приемлемого для интуиционистов смысла, позволяют обосновать некоторые приемлемые с интуиционистской точки зрения теоретико-числовые результаты, для которых либо вообще не известны неаналитические "элементарные" доказательства, либо известные "элементарные" доказательства существенно более сложные (существенно более длинные и запутанные, что делает их более трудными для восприятия).

В каждой математической теории изучается некоторая система математических объектов. Формализация теории превращает саму математическую теорию в объект математического исследования. Для этого прежде всего строится соответствующий символический язык, лишенный недостатков естественных разговорных языков. С этой целью фиксируется соответствующий алфавит, включающий пропозициональные связки, кванторы, технические символы, функциональные и предикатные символы. Во множестве всех слов в этом алфавите с помощью точных определений выделяются подмножества "правильно построенных выражений", обычно таковыми являются множество термов и множество формул. Как правило, существуют простые алгоритмы, позволяющие по любому слову определить, является ли оно термом или формулой. Логические принципы, используемые в традиционной математике при выводе теорем, определялись неявно через значения обычных терминов. При последовательной формализации теории точно определяется, какими логическими принципами можно пользоваться при выводах. Это делается частично через указание соответствующих аксиом, а частично путем точной формулировки правил вывода одних утверждений из других. Так как в итоге происходит полное абстрагирование от содержания или сущности, а внимание уделяется лишь форме, то говорят о *формализации* теории. После формализации теория из си-

системы осмысленных утверждений превращается в систему формальных слов, из которых только по форме некоторые являются правильно построенными, некоторые – аксиомами. Лишь форма слов свидетельствует о том, следует ли данное слово по данному правилу вывода из данной системы слов. Формализация сводит все к форме и правилу. Она устраняет неопределенность в вопросах, что такое утверждение теории и что такое доказательство в теории. В итоге длительного периода истории развития человеческого интеллекта было установлено, что значительная часть математических теорий допускает такую формализацию. Пифагору (VI век до н. э.) приписывается открытие или создание аксиоматико-дедуктивного метода изложения математических теорий. До нас этот метод дошел во многом благодаря "Началам" Евклида.

Формальная теория становится предметом изучения специальной математической дисциплины – *метаматематики* или *теории доказательств*, которая включает в себя описание формальных систем и исследование их свойств. Сама изучаемая предметная теория для метатеории выступает как система слов в некотором алфавите. Метатеория принадлежит обычной неформальной математике, она выражается на обычном языке с использованием математической символики. Традиционно в метатеории используются финитные методы, интуитивно представляемые объекты и осуществимые процессы. Доказательства существования, как правило, дают и метод построения объекта, существование которого доказывается. Эти ограничения вызваны той целью, которую преследовал Д. Гильберт при формулировке своей метаматематической программы. Вопрос о том, не приводят ли к противоречию методы формализуемой теории, изучается в метатеории формализованной теории методами, которые не подвержены тем же сомнениям, что и методы исходной теории, которая была формализована. Критерием допустимости данного метода в метаматематике выступает в конечном счете его интуитивная убедительность.

Особый этап в развитии аксиоматического метода связан с именем Никола Бурбаки (Nicolas Bourbaki). Под этим общим псевдонимом группа математиков, в большинстве французских, предприняла попытку, развивая программу Д. Гильберта, изложить различные математические дисциплины с позиций формального аксиоматического метода. Группа образовалась в 1937 году в основном из выпускников Высшей нормальной школы. Численность и состав группы никогда не объявлялись. В далеко еще не завершенном многотомном трактате Н. Бурбаки "Элементы математики", выходящем с 1939 года, последовательно развивается формальная аксиоматическая система, которая по замыслу авторов должна охватить все основные разделы математики как "частные аспекты общей концепции". Первая книга тракта "Теория множеств". В ней закладывается фундамент всего трактата, состоящий из наиболее общих принципов. Изложение носит очень абстрактный и формализованный характер. Последовательно выдерживается способ изложения – от общего к частному. Во Франции вышло уже достаточно много томов трактата, которые вызвали большой интерес среди математиков как новизной изложения, так и высоким научным

уровнем. Часть книг переведена на русский язык и доступна российскому читателю.

О современном этапе истории математической логики.

В XIX веке исследования в области математической логики активизировались, чему в немалой мере способствовало открытие неевклидовых геометрий и исследования по обоснованию математического анализа. Еще в большей мере активизации исследований в области математической логики способствовало обнаружение (открытие) в конце XIX века парадоксов или антиномий. Это считается началом "Великого кризиса оснований", попытки преодоления которого привели к активизации исследований в области оснований математики, что в свою очередь имело далеко идущие последствия.

Парадокс Г. Кантора (1899 г.) По теореме Г. Кантора для любого множества M выполняется неравенство $\overline{\overline{M}} < \overline{\overline{\mathcal{P}(M)}}$. Обозначим через W множество всех множеств, т. е. элементами W являются всевозможные множества и только они. Тогда каждый элемент из $\mathcal{P}(W)$, будучи множеством, принадлежит W , поэтому $\mathcal{P}(W) \subseteq W$. Значит, $\overline{\overline{\mathcal{P}(W)}} \leq \overline{\overline{W}}$, что вместе с неравенством $\overline{\overline{W}} < \overline{\overline{\mathcal{P}(W)}}$ приводит к противоречию $\overline{\overline{\mathcal{P}(W)}} < \overline{\overline{\mathcal{P}(W)}}$.

Парадокс Б. Рассела (1902 г.) Обозначим через S множество

$$\{x | \neg(x \in x)\}.$$

Заметим, что $x \in S$ тогда и только тогда, когда $\neg(x \in x)$.

Предположим, что $S \in S$. Тогда по предыдущей эквивалентности $\neg(S \in S)$. Значит, $S \in S$ и $\neg(S \in S)$. Из полученного противоречия получаем, что наше предположение $S \in S$ неверно, поэтому $\neg(S \in S)$. Итак, мы доказали, что $\neg(S \in S)$. Отсюда в силу определения множества S получаем, что $S \in S$.

Значит, для множества S мы доказали $S \in S$ и $\neg(S \in S)$. Полученное противоречие и носит название парадокса Б. Рассела.

Популяризируя этот парадокс, Б. Рассел предлагает рассмотреть деревенского парикмахера, который *бреет всех тех деревенских жителей, которые не бреются сами, и не бреет всех тех деревенских жителей, которые бреются сами*. К парадоксальной ситуации приводит вопрос "Бреет ли этот парикмахер самого себя?"

Логическим вариантом парадокса Б. Рассела служит следующий парадокс, который приписывается Б. Расселу и К. Греллингу. Прилагательное называется "предикабельным", если свойство, которое оно обозначает, присуще ему самому. В противном случае прилагательное называется "импредикабельным". Примеры "предикабельных" прилагательных "абстрактное", "многосложное", "русский". Примеры "импредикабельных" прилагательных "конкретно", "односложное", "красное". К парадоксальной ситуации приводит вопрос "Каким является прилагательное "импредикабельное"?"

Парадокс Дж. Ришара (1905 г.) Некоторые тексты на русском языке задают действительные числа. Так как алфавит русского языка конечен (в него мы включаем строчные и прописные буквы, знаки препинания и символ

пробела), то можно занумеровать все тексты на русском языке. Удалив из этого пересчета тексты, не задающие действительных чисел, мы получим пересчет T_1, \dots, T_k, \dots всех тестов на русском языке, задающих действительные числа. При этом действительное число, заданное текстом T_k , называется *к-ым числом Ришара*. Получаем пересчет всех чисел Ришара $\alpha_1, \dots, \alpha_k, \dots$. Рассмотрим текст T :

”действительное число, у которого к-ый десятичный знак равен единице, если у к-ого числа Ришара к-ый десятичный знак не равен единице, и равен двум, если у к-ого числа Ришара к-ый десятичный знак равен единице”. Этот текст T определяет некоторое число Ришара a . Пусть $a = \alpha_k$. Тогда по построению a получаем: a и α_k отличаются k -ым десятичным знаком. Полученное противоречие и носит название парадокса Ришара.

Парадокс Ришара представляет особый интерес, поскольку ведущие к нему рассуждения схожи с канторовским доказательством несчетности множества всех действительных чисел.

Парадокс Г. Берри (1906 г.) В русском языке существует лишь конечное число слогов, поэтому конечным является множество текстов на русском языке, содержащих не более пятидесяти слогов, значит, с их помощью можно задать лишь конечное число натуральных чисел. Пусть a – *”наименьшее из натуральных чисел, которые нельзя задать текстом на русском языке, содержащим не более пятидесяти слогов”*. Текст, напечатанный курсивом, задает число a и содержит не более пятидесяти слогов, что противоречит смыслу этого текста.

Парадокс лжеца. Некоторое лицо говорит *”Я лгу”*. Если он действительно лжет, то сказанное им есть ложь, и, значит, он не лжет. Если же он не лжет, то сказанное им есть правда, поэтому он лжет. Т. е. он лжет и не лжет одновременно.

Можно несколько видоизменить этот парадокс. Пусть некоторое лицо произносит фразу *”высказывание, которое я сейчас произношу, ложно”*. Высказывание, напечатанное курсивом, нельзя считать ни истинным, ни ложным. Парадокс лжеца приписывают Эвбулиду (IV век до н. э.), он был хорошо известен в древности.

Обнаружение парадоксов привлекло внимание к вопросам оснований математики многих выдающихся математиков конца XIX – начала XX в. (Д. Гильберт, А. Пуанкаре, Г. Вейль, Л. Брауэр). Многие математики внесли вклад в поиск выхода из сождавшейся критической ситуации.

К середине XX века математическая логика достигла немалых успехов в постановке и решении принципиально новых математических проблем. Она действительно стала, как говорил П. С. Порецкий, логикой по предмету, математикой по методу. В рамках математической логики было предложено точное математическое определение понятия *”доказательство”*, что позволило поставить вопросы о доказуемости и недоказуемости тех или иных математических утверждений. Были разработаны и методы установления недоказуемости. Это позволило, в частности, К. Геделю и П. Дж. Коэну (1934 – 2007) доказать, что знаменитая **континуум-гипотеза** Г. Кантора не зависит от остальных ак-

сиом общепринятых на сегодняшний день вариантов *аксиоматической теории множеств*.

Приведем мнения ряда авторитетных математиков о роли математической логики в конце XX века.

Дж. Шенфильд ("Математическая логика". М.: Наука, 1975): "... математическая логика является не собранием разрозненных результатов, а действенным методом изучения некоторых наиболее интересных проблем, стоящих перед математиками".

Э. Мендельсон ("Введение в математическую логику". М.: Наука, 1971. Введение): "*Глубокие и опустошительные результаты Геделя, Тарского, Черча, Россера, Клини и многих других были богатой наградой за вложенный труд и завоевали для математической логики положение независимой ветви математики*".

Приведем некоторые, конечно, весьма неполные сведения, ибо "Никто не объятного объять не может", о тех исследователях, кто, кроме упомянутых выше внесли существенный вклад в развитие математической логики в уже прошлом XX веке.

Ян Лукасевич (21.12.1878, Львов, – 13.11.1956, Дублин), польский логик, профессор университетов во Львове (1906 – 1915) и Варшаве (1915 – 1939). После Второй мировой войны профессор Королевской ирландской академии в Дублине. Я. Лукасевич построил первую систему многозначной логики, а на ее основе – систему модальной логики. Ввел бескомбочную форму записи логических и математических выражений.

Эмиль Леон Пост (11.2.1897, Августов, Польша, – 21.4.1954, Нью-Йорк), американский математик и логик. Читал лекции по математике и логике в Колумбийском и Нью-Йоркском университетах. Им дано одно из наиболее часто используемых определений понятий *непротиворечивости* и *полноты* формальных систем, получено доказательство теорем о функциональной и дедуктивной полноте для логики и исчисления высказываний. Э. Постом предложено одно из первых (независимо от А. Тьюринга) математических уточнений интуитивного понятия алгоритма в терминах *абстрактной вычислительной машины*, получившей название *машины Поста*, сформулирован основной тезис теории алгоритмов о возможности реализации любого алгоритма на подходящей машине Поста. Э. Посту и А. А. Маркову принадлежат первые доказательства алгоритмической неразрешимости ряда проблем алгебры.

Алонзо Черч (14.6.1903, Вашингтон, – 11.8.1995, Hudson, Ohio), американский логик, математик. Профессор Принстонского университета (1947 – 1967). С 1967 г. профессор математики и философии Калифорнийского университета (Лос-Анджелес). А. Черч внес вклад в различные разделы логики. В 1936 году А. Черч сформулировал основную гипотезу теории алгоритмов, получившую название *Тезис Черча*: каждая вычислимая функция является частично рекурсивной. В 1936 году А. Черч доказал алгоритмическую неразрешимость исчисления предикатов.

Стивен Коул Клини (5.1.1909, Хартфорд, штат Коннектикут, – 25.1.1994,

Мэдисон, штат Висконсин), американский математик и логик. Основные работы С. Клини посвящены теории алгоритмов и рекурсивных функций, проблемам интуиционистской логики и математики, теории языков и автоматов. С. Клини – автор ряда широко известных монографий по математической логике, основаниям математики и теории рекурсивных функций.

Алан Матисон Тьюринг (23.6.1912, Лондон, – 7.6.1954, Уилмслоу, близ Манчестера), английский математик и логик. В 1936 – 1937 гг. А. Тьюринг предложил одно из первых (независимо от Э. Поста) математических уточнений интуитивного понятия алгоритма в терминах *абстрактной вычислительной машины*, получившей название *машины Тьюринга*, сформулировал основной тезис теории алгоритмов о возможности реализации любого алгоритма на подходящей машине Тьюринга. А. Тьюринг активно участвовал в создании первого компьютера "Colossus", который был разработан в Англии для решения задач дешифрования германской шифрмашин "Enigma" в самом начале Второй мировой войны.

Альфред Тарский (14.1.1902, Варшава, – 26.10.1983, Беркли, Калифорния), американский логик и математик польского происхождения. Основные его работы посвящены теории моделей, теории множеств, булевым и псевдобулевым алгебрам, логикам с формулами бесконечной длины и другим разделам математической логики и оснований математики.

Жак Эрбран (12.2.1908, Париж, – 27.7.1931, Ла-Берард, Изер), французский математик и логик. Основные работы относятся к математической логике – исчислению предикатов, теории рекурсивных функций, конструктивной логике.

Петр Сергеевич Новиков (15(28).8.1901, Москва, – 9.01.1975, Москва), советский математик, внес выдающийся вклад в теорию множеств, математическую логику, теорию алгоритмов и теорию групп. Доказал алгоритмическую неразрешимость проблем тождества, сопряженности и изоморфизма в теории групп. С 1957 года и до конца жизни руководил отделом математической логики Математического института имени В. А. Стеклова АН СССР, создал школу математической логики в СССР.

Анатолий Иванович Мальцев (14(27).11.1909, ныне поселок Мишеронский Шатурского района Московской области, – 7.7.1967, Новосибирск), советский математик, внес выдающийся вклад в алгебру и математическую логику. А. И. Мальцев – один из создателей общей теории алгебраических систем и теории моделей.

Андрей Андреевич Марков (9(22).9.1903, Петербург, – 11.10.1979, Москва), советский математик, с 1959 года заведовал кафедрой математической логики Московского государственного университета имени М. В. Ломоносова. А. А. Марков внес выдающийся вклад в теорию алгоритмов и математическую логику – создал школу конструктивной математики и логики в СССР.

Пол Джозеф Коэн (2.04.1934, Лонг-Бренч, Нью-Джерси – 23.03.2007, Стэнфорд, Калифорния), американский математик, профессор Стэнфордского университета. П. Дж. Коэн достиг выдающихся успехов в различных разделах математики. В 1963 году П. Дж. Коэн опубликовал выдающийся резуль-

тат в области теории множеств и математической логики – *доказательство невозможности вывода **Континуум-гипотезы** Г. Кантора в аксиоматической теории множеств. Тем самым завершив начатые в 40-е годы XX века исследования К. Геделя, доказавшего в 1940 году невозможность опровержения **Континуум-гипотезы** Г. Кантора в рамках аксиоматической теории множеств, т. е. невозможность вывода в аксиоматической теории множеств отрицания **Континуум-гипотезы** Г. Кантора.* За этот выдающийся результат Полу Джозефу Козну на Международном математическом конгрессе, проходившем в 1966 году в Москве, была присуждена Филдсовская медаль, в определенном смысле высшая в то время международная математическая награда (позже появились и другие международные математические награды – премия Неванлины в 1982 году и премия Абеля в 2002 году).

ПОСЛЕСЛОВИЕ

В планах автора написание продолжения пособия, в котором предполагается рассмотреть дополнительные вопросы логики и исчисления предикатов с равенством, включая фундаментальную теорему К. Геделя о неполноте, изложить основы теории рекурсивных функций, необходимые для доказательства этой теоремы, вне их связи с подходом к уточнению понятия алгоритма, привести некоторые сведения о формальной арифметике и некоторых других формализованных теориях, включая нестандартный, или неархимедов, анализ. Особое внимание планируется уделить вопросу о сложности разрешающих алгоритмов для некоторых известных формальных теорий.

Литература

- [1] Адян С. И., Дурнев В. Г. Алгоритмические проблемы для групп и полугрупп // Успехи матем. наук. 2000. Том 55. 2. С. 3–94.
- [2] Архангельский А. В. Канторовская теория множеств. М.: Изд-во МГУ, 1988.
- [3] Булос Дж., Джеффри Р. Вычислимость и логика. М.: Мир, 1994.
- [4] Бурбаки Н. Начала математики. Первая часть. Основные структуры анализа. Книга первая. Теория множеств. М.: Мир, 1965.
- [5] Верещагин Н. К., Шень А. Начала теории множеств. М.: Изд-во МЦНМО, 1999.
- [6] Верещагин Н. К., Шень А. Языки и исчисления. М.: Изд-во МЦНМО, 2000.
- [7] Гордон Е. И., Полотовский Г. М. Мощность бесконечных множеств. Нижний Новгород: Изд-во НГУ, 1998.
- [8] Девис М. Прикладной нестандартный анализ. М.: Мир, 1980.
- [9] Дурнев В. Г. Элементы теории множеств и математической логики. Ярославль: ЯрГУ, 1978.
- [10] Дурнев В. Г. Введение в математическую логику. Ярославль: ЯрГУ, 2005.
- [11] Дурнев В. Г. Элементы математической логики. Ярославль: ЯрГУ, 2006.
- [12] Дурнев В. Г. Элементы теории алгоритмов. Ярославль: ЯрГУ, 2008.
- [13] Ершов Ю. Л., Палютин Е. А. Математическая логика. М.: Наука, 1979.
- [14] Ивс Г., Ньюсом К.В. О математической логике и философии математики. М.: Изд-во Знание, 1968.
- [15] 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.

- [16] Столл Р. Множества, логика, аксиоматические теории. М.: Просвещение, 1968.
- [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] Коэн П. Дж. 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] Манин Ю. И. Доказуемое и недоказуемое. М.: Советское радио, 1979.
- [26] Манин Ю. И. Вычислимое и невычислимое. М.: Советское радио, 1979.
- [27] Марков А. А. Элементы математической логики. М.: Изд-во МГУ, 1984.
- [28] Мендельсон Э. Введение в математическую логику. М.: Наука, 1976.
- [29] Натансон И. П. Теория функций вещественной переменной. М.: Наука, 1974.
- [30] Новиков П. С. Элементы математической логики. М.: Наука, 1973.
- [31] Плиско В. Е. Математическая логика. М.: Изд-во МГУ, 2000.
- [32] Расева Е., Сикорский Р. "Математика метаматематики". М.: Наука, 1972.
- [33] Серпинский В. О теории множеств. М.: Просвещение, 1966.
- [34] Успенский В. А. Нестандартный, или неархимедов, анализ. М.: Знание, 1983.
- [35] Успенский В. А. Нестандартный, или неархимедов, анализ. М.: Наука, 1988.
- [36] Феферман С. Числовые системы. М.: Наука, 1971.
- [37] Френкель А., Бар-Хиллел И. Основания теории множеств. М.: Мир, 1966.

- [38] Шенфилд Дж. Математическая логика. М.: Наука, 1975.
- [39] Чень Ч., Ли Р. Математическая логика и автоматическое доказательство теорем. М.: Наука, 1983.
- [40] Черч А. Введение в математическую логику. Т. 1. М.: ИЛ, 1960.
- [41] Jech T. the Axiom of Choice. Amsterdam: North-Holland, 1973.
- [42] Churh A. An unsolvable problem of elementary number theory // Amer. J. Math. 1936. Vol. 58. 2. P. 345–363.
- [43] Churh A. A note on the Entscheidungsproblem // J. Symbolic Logic. 1936. Vol. 1. 1. P. 40–41.
- [44] Post E. L. *Intoduction to a general theory of elementary propositions* // Amer. J. Math. 1921. Vol. 43.
- [45] Post E. L. *Finite combinatory processes – formulation 1* // Journal of Symbolic Logic. 1936. Vol. 1, № 3. P. 103 – 105.
- [46] Post E. L. *A variant of a recursively unsolvable problem* // Bull. Amer. Math. Soc. 1946. Vol. 52. P. 264 – 268.
- [47] Post E. L. *Recursive unsolvability of a problem of Thue* // J. Symbol Log. 1947. Vol. 12, № 1. P. 1 – 11.
- [48] Thue A. *Problem üder Veränderungen von Zeichenreihen nach gegebenen Regeln* // Vid. Skr. Math.-natur. KI, 1914. № 10.
- [49] Turing A. M. On computable numbers, with an application to the Entscheidungsproblem // Proceedings of London Mathematical Society. Ser. 2. 1936. Vol. 42. № 3, 4. P. 230 – 265.

Учебное издание

Дурнев Валерий Георгиевич

ЭЛЕМЕНТЫ ТЕОРИИ МНОЖЕСТВ И МАТЕМАТИЧЕСКОЙ ЛОГИКИ

Учебное пособие

Редактор, корректор М. В. Никулина

Компьютерная верстка В. Г. Дурнев, М. А. Башкин

Подписано в печать ...0..09. Формат 60 × 84 1/8.

Бум. офсетная. Гарнитура "Times NewRoman"

Усл. печ. л. 52,52. Уч.-изд. л. 23,0. Тираж 120 экз.

Заказ

Редакционно-издательский отдел

Ярославского государственного университета

имени П. Г. Демидова

150000, г. 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