# МАТЕМАТИКА как ИНОСТРАННЫЙ

архитектура математической мысли

Н. И. Казимиров

# МАТЕМАТИКА
## КАК
# ИНОСТРАННЫЙ

или архитектура математической мысли

**Н. И. Казимиров**

**Москва, 2026**

УДК 510.6
ББК 22.12
К14

**Казимиров Н. И.**
К14 Математика как иностранный, или архитектура математической мысли — М., 2026. — 353 с.

Книга представляет собой попытку автора написать пособие по изучению математического языка так, как принято изучать иностранный язык. Целью книги является научить читателя правильно и легко воспринимать математический текст, понимать его закономерности, структуру, возможности и ограничения. Ориентированная на изучение математического текста как такового, книга в основном апеллирует к формальным системам, которые изучаются в математической логике и примерам классических формальных теорий. В то же время в ней постоянно подчеркивается многоуровневый взгляд на математический язык, включающий метатеорию и семантику формальных конструкций.

**Ключевые слова**: язык, формулы, логика, формальные теории, основания математики, теория множеств.

# СОДЕРЖАНИЕ

# Ключевые теоремы

# ПРЕДИСЛОВИЕ

Дорогой читатель,

Данная книга представляет собой целостное и структурированное собрание материалов, разработанных мною для курса по изучению математики как иностранного языка. Эти наработки поначалу нашли свое место в моем блоге на Youtube, а затем были положены в основу данного издания.

Отметим сразу же несколько особенностей книги, которые существенно отличают ее как от учебников по математике, так и от учебников иностранных языков.

Во-первых, цель книги состоит не в том, чтобы научить читателя именно математике или математической логике, хотя она изобилует примерами именно из этих дисциплин. Напротив, цель состоит в том, чтобы показать, насколько прозрачным и понятным может быть *lingua franca* современных точных наук, если пройти определенный курс адаптации — путешествие, в котором эта книга призвана стать вашим проводником.

Особенно актуальным это становится сегодня, когда на наших глазах появляется новый исторический актор, для которого математический язык является родным, — *искусственный интеллект*. Алгоритмы, управляющие роботами, нейронные сети, анализирующие данные, и большие языковые модели строят свои «мысли» и «решения» на строгих законах логики и алгебры, которые и составляют грамматику языка математики. Понять их — значит заглянуть в будущее коммуникации не только с машинами, но и с самой формализованной мыслью.

Во-вторых, эта работа задумана прежде всего как книга для дополнительного чтения, а не как традиционный учебник. Язык математики глубоко отличается от любого разговорного языка, и уровни владения им определяются критериями, отличными от стандартных шкал языковой компетенции. Поэтому эту книгу лучше всего использовать, чтобы перекинуть мост между интуитивным пониманием и строгим формализмом, дополняя стандартные курсы логики, теории множеств или алгебры.

В-третьих, книга не претендует на точное научное описание лингвистических особенностей и явлений, которые так или иначе проявляются в математическом языке и которые могут иметь соответствующую коннотацию и терминологию в лингвистике. Поэтому те места, где изложение материала выходит за рамки математики и логики, следует считать скорее сопутствующим художественным описанием, чем выверенным научным текстом. Однако я как автор был бы признателен, если бы опытный лингвист или филолог помог мне в будущем разобраться в правильном употреблении терминологии и необходимых отсылках к научным источникам.

В-четвертых, особое внимание уделяется *анатомии доказательств*. Текст предлагает уровень детализации, часто опускаемый в стандартных учебниках, где технические нюансы нередко оставляются читателю. Например, доказательство возведения ординалов в степень через функции с конечным носителем представлено с исчерпывающей тщательностью. Более того, мы явно анализируем связь между различными определениями ординальных арифметических операций — рекурсивными и основанными на упорядоченных суммах, произведениях и степенях. Эта двойственность подходов редко представлена столь полно в учебной литературе, однако она необходима для глубокого понимания того, как строятся математические структуры. Подобно тому как беглость в иностранном языке требует овладения тонкостями грамматики, беглость в математике требует видения микроскопических деталей её логических оснований.

Необходимо также сказать о глубине изложения. Хотя мы стремимся к строгости, главная цель этой книги — продемонстрировать *архитектуру* математической мысли. Вследствие этого, для некоторых монументальных результатов — таких как теоремы Гёделя о неполноте, теорема Морли о категоричности или результаты о независимости в теории множеств — мы ограничиваемся **концептуальным обсуждением** их значения и последствий, а не приводим формальные выводы. И наоборот, мы уделяем скрупулезное внимание «микроскопическим» основам, часто опускаемым в стандартных текстах: например, строгий вывод элементарных арифметических свойств из аксиом Пеано представлен во всех деталях. Кроме того, мы делаем акцент на теоретико-модельном подходе к доказательствам в логике предикатов, подчеркивая семантическую связь между языком и его моделями.

Структура книги имитирует этапы изучения языка, что отражено в названиях глав. Её содержание дополняет стандартную математическую литературу, фокусируясь на описательном аспекте математики, выраженном через формализмы и модели.

Текст книги разделен на две части, в первой из которых превалирует «лирика», т. е. некоторые общие рассуждения и факты без доказательств, а во второй, «брутальной» части внимание читателя сконцентрировано на прямом применении изучаемого языка в конкретных примерах, где преобладает математическая логика. Соответственно, в первой части книги, по крайней мере в начале, очень мало формул и довольно много нестрогих ассоциативных рассуждений, а во второй, наоборот, страницы усеяны формальными выкладками, напоминая своим видом текст компьютерной программы, и почти отсутствуют общие рассуждения.

Кроме того, первая часть книги разделена на блоки, условно соответствующие уровням сложности математического языка. Традиционно, это уровни **A1**, **A2**, **B1**, **B2**, **C1**, каждый из которых затем делится на еще более детальные разделы или модули, сложность которых внутри одного уровня никак не ранжируется. Материал часто рассматривается повторно на разных уровнях с возрастающей строгостью, отражая «спиральный подход» к изучению языка. Уровень профессионального владения **C2** опущен, так как такое мастерство характеризует «носителей языка» — людей с профессиональным математическим образованием, которым эта книга по определению не нужна.

Эта модульная структура допускает нелинейный подход к чтению. Подобно тому как используют учебник иностранного языка — выбирая подходящий уровень сложности и пропуская уже освоенные уровни, — читателю предлагается пропустить элементарные разделы, если они кажутся тривиальными, и переходить непосредственно к более продвинутым темам. Вы вольны выбирать отправную точку, соответствующую вашему текущему уровню «владения языком», возвращаясь к ранним главам только за конкретными разъяснениями.

Часть II не следует уровневой структуре. Она организована по ключевым темам — Язык, Логика, Арифметика и Теория множеств — для удобного закрепления необходимых утверждений и определений, на которые ссылается Часть I.

С самого начала текста предполагается, что читатель уже в некоторой степени знаком с математической символикой хотя бы из первых 6–7 лет общеобразовательной школы, так что здесь мы не занимаемся изучением цифр, не учим таблицы сложения и умножения, не объясняем аксиомы планиметрии и суть координатного метода Декарта, относя все эти простейшие вещи к уровню **A0**, который еще называется Beginner или Starter.

Тем не менее, начинаем мы наше пособие, как и положено, с изучения алфавита, поскольку все дальнейшие рассуждения существенным образом опираются на этот при-

митивный базис любого письменного языка. Собственно, весь раздел **A1** в значительной мере посвящен тому, чтобы рассказать, как же на самом простом уровне устроен математический текст, т. е. каким образом и по каким правилам складываются те замысловатые формулы, которые так часто отпугивают непосвященных. Еще не понимая полностью смысла текста, записанного на математическом языке, вы уже сможете его читать и понимать его внутреннюю структуру. Иначе говоря, в этом разделе мы рассматриваем синтаксическую структуру математического языка. С моей точки зрения, отсутствие «правил чтения» математического языка в учебниках математики является одним из огромных пробелов современного естественно-научного образования. Уровень **A1** по аналогии с обычными учебниками иностранных языков я бы назвал *уровнем выживания* или Elementary.

На уровне **A2** мы затрагиваем базовые понятия логики в том виде, в каком ее ранее преподавали как отдельный предмет. И хотя теперь считается, что логика есть часть математики, мы будем придерживаться той парадигмы, что существует некая общая научная логика, присущая человеческому разуму как некоторый базовый код, позволяющая строить выводы и прогнозы вне зависимости от знаний математики, а есть логика (точнее, много разных логик) формальная, анализом которой как раз и занимается математика, и которая лежит в основе формальных математических и компьютерных систем. Вместе с логикой мы привносим в наш язык некоторую семантику, т. е. смысловую окраску тех бесчисленных закорючек, которые мы уже научились писать и читать. На этом уровне мы уже существенно продвигаемся в освоении языка, изучаем такие базовые вещи, как рассуждения и вывод, вводим начальную терминологию и обозначения из теории множеств, даем определения различных видов отношений и функций, вводим обозначения логических операций и кванторов. Уровень **A2** можно обозначить как *предпороговый* или Pre-Intermediate.

На уровне **B1** мы переходим уже к формальной логике, детализируем ее описание, выделяем несколько слоев логики — исчисление нулевого порядка (логика высказываний), исчисление первого порядка (логика предикатов), формальные аксиоматические теории первого порядка. Некоторое внимание уделяется также теории моделей и интерпретаций формального языка и формальных теорий, понятию непротиворечивости, полноты, логического следования. Язык вместе с тем становится более строгим, определения более точными. Немало места уделяется значимости понятия равенства и такого его определяющего свойства, как конгруэнтность. Вместе с тем мы продолжаем использовать «наивные» понятия множеств, отношений и функций, откладывая анализ формальной теории множеств на более высокий уровень. Здесь нашим главным достижением в изучении математического языка будет полное представление о том, что такое теория, аксиома, формальное доказательство и как все это можно «приземлить» на теоретико-множественную модель. Иначе говоря, здесь выученный ранее язык из простого умения говорить превращается в способ думать и грамотно излагать свои мысли. Уровень **B1** по аналогии с разговорными языками можно назвать Intermediate или *пороговый уровень*. На этом уровне количество готовится перейти в качество.

С началом уровня **B2** мы все больше вынуждены писать формулы вместо слов, поскольку начинаем преодолевать значительный с точки зрения восприятия порог сложности математического языка. А именно, мы знакомимся с формализмом первопорядковой арифметики Пеано, обсуждаем ее аксиоматику и некоторые следствия. Важными вехами на этом пути будут приобретаемые навыки обращения с формальными конструкциями, умение воплощать в формализме некоторые общие понятия и понимать границы применимости формализмов в плане способности выразить те или иные кон-

цепции. Здесь мы также вводим язык теории множеств, фокусируясь на финитной математике и представлении множеств в виде деревьев, подведя под аксиоматику некоторую философскую мотивацию. Описание теории наследственно конечных множеств будет той вишенкой на торте, которая увенчает уровень **B2** и подготовит к штурму аксиоматической теории множеств Цермело-Френкеля. Уровень **B2** мы можем сравнить с Upper-Intermediate или *продвинутым пороговым уровнем* в освоении математического языка как иностранного.

Уровень **C1** предлагает тщательный анализ языка теории множеств. Здесь мы дадим окончательно строгие определения таким понятиям, как отношение и функция, детально проанализируем аксиому выбора в различных ее формах и ее место в математике, коснемся роли аксиомы регулярности в систематизации универсума множеств по фон Нейману, поговорим о способах построения структур и разберем их на конкретных примерах числовых структур. Здесь мы совершаем фазовый переход от простого формализма к языку высокого уровня, способному выражать современные математические концепции.

Если вы успешно пройдете этот путь и проберетесь через чащи формул во Второй части, я уверен, что любые опасения перед математическими текстами исчезнут. Вы приобретете навыки самостоятельного создания таких текстов и формулирования мыслей на уникальном языке, на котором, по выражению Галилео Галилея, написана книга природы.

По всему тексту ключевые понятия и обозначения при первом упоминании выделены **жирным шрифтом**. Следуя спиральному подходу к освоению языка, первоначальные объяснения в Части I опираются на интуицию и контекст, в то время как строгие математические определения приводятся по мере продвижения изложения к более высоким уровням или закрепляются в Части II.

Чтобы облегчить переход от пассивного понимания к активному владению материалом, в книгу включено около 190 упражнений различной степени сложности — от задач на вычисления до построения нетривиальных доказательств. Ответы приведены в конце книги.

## Цифровое приложение

Чтобы помочь читателям ориентироваться в сложной сети математических понятий, я разработал интерактивный инструмент 3D-визуализации — **MathLogic Nexus**. Это веб-приложение позволяет пользователям исследовать логические зависимости между определениями, теоремами и теориями. В то время как книга фокусируется на фундаментальных лингвистических и логических основах, *MathLogic Nexus* помещает эти понятия в более широкий математический контекст, визуализируя их связи с теорией моделей, топологией и теорией вычислимости. Оно служит динамической картой «архитектуры» математической мысли. Инструмент доступен онлайн по адресу: `https://nexus.mathem.at/`, а его краткий обзор — на моем Youtube-канале.

Наконец, для удобства навигации в конце книги размещены подробный Предметный указатель и Список обозначений.

# Благодарности

Эта книга — результат долгого личного путешествия по ландшафту математической логики, пути, который я по большей части прошел как независимый исследователь. Однако ни одно путешествие не бывает по-настоящему одиночным, и я в долгу перед теми, кто сформировал мое математическое мировоззрение.

Хочу выразить глубочайшее уважение и благодарность моему научному руководителю, профессору Юрию Леонидовичу Павлову, чье руководство в годы моей аспирантуры, посвященной случайным лесам и графам, привило мне дисциплину математической мысли.

Хотя мне не выпала честь быть его непосредственным учеником, я глубоко благодарен академику Льву Дмитриевичу Беклемишеву. Его блестящие лекции, опубликованные кафедрой математической логики МГУ, стали для меня главными вратами в современную теорию доказательств. Ясность его изложения служила ориентиром для моих собственных попыток объяснять сложные понятия.

Я также благодарен моим рецензентам за конструктивную критику. Их настойчивое пожелание расширить практическую составляющую книги побудило меня добавить упражнения в Часть II, что значительно повысило ее учебную ценность.

### Примечание об издании

Данная книга изначально задумывалась и писалась на русском языке, однако её международная версия была принята к публикации издательством Springer под названием Mathematics as a Foreign Language. Настоящее русское издание представляет собой оригинальную авторскую версию, свободную от ограничений перевода и сохраняющую все стилистические особенности родного языка.

Москва, Россия
2026

YouTube

Telegram

mathem.at

# Часть I

# Восхождение

УРОВЕНЬ A1

# Выживание

*Самое непостижимое в этом мире — это то, что он постижим.*

— Альберт Эйнштейн

## A1.1. Иллюстративная сказка

Представим себе, что Математика — это некая экзопланета, довольно-таки непривычно устроенная и населенная странными существами, назовем их *математянами*, средством общения которых являются замысловатые фигурные закорючки, которые они умеют чертить прямо в воздухе, благо состав атмосферы им это позволяет. Но в отличие от сюжета известного фильма «Прибытие» Дени Вильнёва, эти, с позволения сказать, «тексты» намного сложнее выглядят и одновременно имеют очень строгую логическую структуру. И вот на эту планету высаживается земной бот, оснащенный ИИ, и пытается наладить контакт с местными жителями. Для этого ему, конечно же, требуется найти с ними общий язык, т.е. по сути разобраться в их странном языке и научиться на нем что-то «говорить». Слово «говорить» мы берем в кавычки, потому что этому процессу не сопутствуют колебания воздуха, которые мы могли бы назвать звуком, а сам процесс имеет чисто визуальное сопровождение.

«Разумный» бот начинает применять свои сложные алгоритмы по анализу структур, помогающие распознать этот язык по какому-либо известному землянам шаблону. Первое, что он понимает: язык является и алфавитным, и иероглифическим одновременно, поскольку значительная часть элементов языка повторяется многократно, в то время как другая часть элементов встречается сравнительно редко.

С одной стороны, это проблема, поскольку не совсем понятно, какими лингвистическими методами пытаться разобрать этот язык на составляющие. С другой стороны, довольно быстро выясняется, что почти все иероглифические знаки коррелируют с алфавитными последовательностями, т.е., проще говоря, их можно расшифровать с помощью более длинного, но более простого текста. Это обнадеживает.

Следующая фундаментальная особенность языка математян состоит в том, что всякий отдельно взятый графический образ, выражающий какое-то абстрактное понятие, имеет определенную внутреннюю структуру в виде дерева-матрешки, т.е. складывается при помощи подстановки простых графем в некоторые шаблоны, разнообразие видов которых весьма ограничено. Тем самым становится понятно, как генерировать новые «слова» и «фразы» на местном языке.

Разобравшись с базисом и структурой языка, наш бот пытается искать правила, по которым одни конструкции допустимы, т.е. встречаются в замеченных им «разговорах» довольно часто, а какие категорически недопустимы (не встречаются) или допускаются крайне редко, что можно соотнести с их негативной или вульгарной коннотацией. Методом случайных деревьев решений (`decision trees`) или еще каким-то более продвинутым методом анализа структур ИИ нашего бота распознает ряд простых правил,

позволяющих строить правильные тексты и при этом как можно реже оскорблять чувства местного населения (как в песне Высоцкого про тау-китян).

Итак, синтаксис языка стал более-менее понятным, и теперь самое время для распознавания некоторой семантики языка, т.е. придания ему смысла. Для чего нужно пробовать полностью или фрагментарно интерпретировать корректно построенные тексты в какой-то уже известной нам семантической реальности. Например, отыскать в земных текстах такие фрагменты, которые очень похожим образом соотносятся друг с другом. Иначе говоря, если в языке математян всегда за одним конкретным выражением следует другое не менее конкретное, то и в земной интерпретации конкретные аналоги этих выражений тоже должны располагаться друг за другом в том же порядке с очень высокой долей вероятности.

Тут важно понимать, что интерпретации могут быть простыми и сложными. Простые интерпретации чаще всего довольно нелепы, однако они позволяют оценить саму возможность произвести интерпретацию чужого языка (и его относительную непротиворечивость). Вспоминается рассказ А. Азимова «Логика», в котором робот нового поколения, обслуживающий некое устройство трансляции энергии на спутнике, придумал религию, очень просто объясняющую необходимость держать луч в фокусе ретранслятора — он стал поклоняться устройству, называя его Господином, отмел всяческую возможность существования космоса, Земли и луча энергии, но зато как «отче наш» старался сделать так, чтобы стрелки приборов не отклонялись от нужных значений ни на волосок. При этом категорически отпала необходимость в людях, и он отстранил их от управления спутником, назвался пророком Господина, а из роботов-помощников сделал адептов этой религии. Что характерно, такая упрощенная метафизическая концепция позволяла очень точно и надежно исполнять то, что было предписано роботам изначально, совершенно не задумываясь о пользе народному хозяйству и какой-то там Земле. Он просто выбрал простой самодостаточный фрагмент языка управления транслятором и проинтерпретировал его еще более простым способом. Интепретация была абсолютно ложной с точки зрения людей, но непротиворечивой и вполне работоспособной.

Итак, наш бот начинает придумывать интерпретации или, говоря более научно, строить модели того языка, который он открыл. Построение разнообразных моделей, имеющих вполне конкретный смысл для землян, позволяет хотя бы примерно оценить семантику математян, а также попытаться построить переводчик с нашего языка на их, и наоборот.

После этого можно смело утверждать, что земной бот, а вместе с ним и поджидающие его на орбите земляне нашли общий язык с аборигенами планеты Математика, и могут приступать к культурному обмену. Если, конечно, стандартная модель изученного языка не окажется настолько примитивной, что наши корреспонденты сочтут нас полными кретинами и прекратят общение.

## A1.2. Принцип матрешки

Итак, в целом мы уже начертили путь, по которому нам предстоит пройти. Попробуем представить себя создателями того самого бота с ИИ, который изучает инопланетный язык, и применим наши наработки к изучению не такого уж инопланетного, но подчас более сложного и непонятного языка, каковым является язык математики.

Во-первых, для краткости будем обозначать этот язык буквой $\mathfrak{Math}$. Сразу же стоит оговориться, что $\mathfrak{Math}$ включает в себя на самом деле целое родовое дерево языков и диалектов, которые в каждой конкретной ситуации определяются некоторым более строгим образом. Пока же для нас язык $\mathfrak{Math}$ — это математический язык вообще, в самом общем понимании.

Во-вторых, заметим, что этот язык обладает многими признаками естественных языков, такими как: коммуникативность (поскольку обеспечивает возможность ученым из разных наук и стран обмениваться знаниями), наличие встроенного метаязыка (инструментов, позволяющих описывать себя самого), эстетические функции (выражающиеся во внутренней красоте универсальности и согласованности понятий), индикативность (указание принадлежности своих пользователей к определенным группам профессий), неограниченная семантическая мощность (поскольку математические понятия могут одинаково хорошо работать при совершенно различной семантике), эволютивность (математический язык быстро и плодотворно развивается, адаптируясь к новым реалиям науки и культуры).

В то же время по понятным причинам математический язык нельзя отнести к естественным языкам, поскольку он не имеет привязки к какой-либо этнической группе или языковой семье, а кроме того, он включает огромное семейство формальных языков, зачастую напоминающих языки программирования, что, конечно, резко отличает его от языков разговорных.

В-третьих, язык $\mathfrak{Math}$ — это чисто письменный язык. Безусловно, в этом языке есть «озвучка», т.е. текст мы можем так или иначе прочесть вслух, но толку для слушателя от этого фонирования не будет никакого, поскольку математические формулы крайне трудно воспринимаются на слух, за исключением каких-то совсем уж простейших выражений. Эта особенность языка $\mathfrak{Math}$ на первый взгляд должна упростить его изучение, ведь мы сразу же можем отбросить такие известные компоненты изучения языков как аудирование и говорение, оставив только чтение и письмо. Однако, следуя принципам диалектики, не стоит упускать из виду антагонистическую составляющую упрощения — схлопывание каналов восприятия, ведь теперь мы начисто отвергаем слуховую память и полагаемся только на зрение и логику (в отдельных случаях может помочь память микромоторики, но в математике она может сыграть злую шутку).

Как и любой другой письменный язык, наш язык $\mathfrak{Math}$ начинается с **алфавита**. При этом нужно понимать, что алфавит языка $\mathfrak{Math}$ намного шире, чем стандартный алфавит любого европейского языка (латинский, греческий или кириллица), поскольку помимо обычных букв он включает в себя цифры и огромное количество специальных знаков, чем-то напоминающих иероглифы. Однако у этих символов, как правило, вполне логичное происхождение и точная контекстная семантика.

Например, символ отношения принадлежности ($\in$), предложенный Джузеппе Пеано, происходит от первой буквы греческого слова *ἐστί* («быть», т.е. быть частью, быть в заданном объеме понятия), аналогичное происхождение у обозначения дифференциала ($d$), предложенного Готфридом фон Лейбницем, и квадратного корня (от первой буквы слова *radix*), введенного Кристофом Рудольфом. Чуть более сложная история происхождения символа сложения ($+$): считается, что он произошел как сокращение латинского союза *et* («и»). Также можно вспомнить, что символы кванторов всеобщности ($\forall$) и существования ($\exists$) произведены от первых букв слов *Any* и *Exists* путем их отражения (авторство приписывается Г. Генцену и Ч. Пирсу).

Все символы алфавита мы относим к так называемым **графемам**, т.е. неделимым элементарным графическим символам. Предполагается, что эти символы человек уме-

ет легко различать с первого взгляда (исключением, пожалуй, является готический шрифт).

В дополнение к алфавиту мы также располагаем большим количеством *несамостоятельных графем*, которые служат для построения всевозможных выражений и сами по себе ничего не обозначают. К ним, например, относятся различные скобки, акценты, стрелки, операторные символы и т.д. и т.п. Характерным отличительным признаком несамостоятельных графем является наличие у них *подстановочных мест*, на практике часто обозначаемых переменными. Эти подстановочные места-переменные являются своего рода точками сборки более сложных лексических единиц нашего языка $\mathfrak{Math}$.

Кроме того, в математике и особенно в программировании часто встречаются многобуквенные обозначения каких-то функций, операций, констант, например, sin или arctan. Эти обозначения могут быть как стандартизованными, так и определяемыми «на лету» в рамках одной статьи или книги. Такие обозначения мы не относим к алфавиту, поскольку они составлены из алфавитных символов, но называем **жесткими графемами**, поскольку они выступают в роли неделимых символов. Восприятие жестких графем как единых символов определяется контекстом и может быть затруднено в ряде случаев. Жесткие графемы тоже могут быть как самостоятельными, так и несамостоятельными (т.е. сопровождаться подстановочными местами).

Более подробное определение алфавита и графем мы приводим во второй части книги (см. разделы D1.1 и D1.2).

Все графемы, несмотря на их огромное разнообразие, образуют некоторый конечный, слабо меняющийся со временем список значков. Они являются элементарными частицами текста на языке $\mathfrak{Math}$. Точно так же, как буквы обычного языка являются элементарными частицами, из которых состоят письменные слова и предложения. И точно так же, как в разговорном языке, из алфавитных символов и графем языка $\mathfrak{Math}$ складываются более сложные обозначения понятий, отношений, объектов.

Помимо смысловой нагрузки, уходящей корнями в различные разговорные языки и понятия, математические обозначения почти всегда несут функциональную нагрузку и подчиняются «**принципу матрешки**», который заключается в том, что все сложные слова математического языка $\mathfrak{Math}$ есть комбинация его графем по заранее заданным правилам.

Точнее, скажем, что **лексемой** языка $\mathfrak{Math}$ называется, во-первых, всякая самостоятельная графема (и в частности символы алфавита), а во-вторых, результат подстановки лексем в несамостоятельную графему на ее подстановочные места (или вместо переменных).[1] Мы специально здесь не выделяем переменные как особый синтаксический вид лексем, чтобы сделать изложение проще. Но в дальнейшем мы уделим переменным пристальное внимание.

Заметим, что в разговорном языке мы имеем похожую (хотя и не точно такую же) ситуацию: например, в английской грамматике имеет место строго определенный порядок членов предложения (определенные подстановочные места для подлежащего, сказуемого и т.д.), а в немецком и русском языках глагол часто определяет не только падеж зависимого слова, обозначающего объект действия (переходный глагол), но и предлог перед ним. Так что собирать предложения из слов мы можем только по строго определенным правилам.

[1] Более формальное и технически точное определение лексемы, основанное на понятии *производного шаблона*, будет дано во второй части книги (см. раздел D1.2). Однако на интуитивном уровне именно принцип рекурсивной сборки является ключевым.

Таким образом, принцип матрешки говорит нам буквально следующее: если у нас есть одна пустая матрешка и одна уже собранная матрешка, то мы можем вторую положить внутрь первой, и в результате получится более сложная собранная матрешка. Такая простая аналогия немедленно приводит к вопросу — что делать, если матрешки окажутся несовместимыми по размеру? Для этого существует *типизация* лексем и подстановочных мест. Проще говоря, всякое подстановочное место «признает» только лексемы своего типа, и при сборке лексем это нужно учитывать.

Например, в геометрии нельзя складывать две точки или находить их скалярное произведение, поскольку эти операции применимы только к векторам, в линейной алгебре нельзя брать детерминант у неквадратной матрицы, а в теории вероятностей невозможно сложить вероятность с событием. Но в математике несовместимось типов — это скорее исключение, чем правило, т.к. мы все стараемся сводить к числовым типам или использовать естественную конвертацию типов «на лету». В программировании же, наоборот, типизация лексем играет огромную роль и ее непонимание часто приводит к ошибкам в коде программ.

Посмотрим на простейшем примере, как происходит процесс лексемостроения. Символ сложения (+) является несамостоятельной графемой, имеющей два подстановочных места — слева и справа, причем как подстановочные места, так и сам результат подстановки принадлежат к одному типу — числам. На эти места мы можем подставить, например, алфавитные символы $a$ и $b$, получив лексему $a + b$. Аналогично действуем в случае умножения: $c \cdot d$. А теперь мы можем вновь взять символ сложения, и на его подстановочные места подставить уже полученные нами лексемы: $a + b + c \cdot d$. Обычно подстановочные места принято заключать в скобки, чтобы сохранять структуру лексемы, так что правильнее было бы записать ее так: $(a + b) + (c \cdot d)$.

Здесь мы действуем строго по определению, подставляя «старые» лексемы в несамостоятельную графему, т.е. надстраиваем имеющиеся конструкции одним шагом «вверх».

Более привычным способом является обратная процедура — наращивание лексемы вниз путем подстановки готовых лексем вместо переменных другой готовой лексемы. Например, имея лексему $a + (b \cdot c)$, мы можем осуществить подстановку лексемы $a + b$ вместо переменной $c$, в результате чего получим лексему $a + (b \cdot (a + b))$. Такая генерация лексемы произведена не по определению, однако можно доказать, что и она приводит к правильно построенным лексемам, т.е. лексему $a + (b \cdot (a + b))$, на самом деле, можно собрать «снизу вверх», строго следуя определению. Подобного рода структурные теоремы обычно доказываются индукцией: предполагая, что лексема получается корректной независимо от способа сборки для лексем длины меньше $n$, мы далее доказываем, что это будет верно и для лексемы длины $n$.

В итоге получается, что лексемы можно собирать почти как угодно: достраивать их «вверх» путем подстановки в несамостоятельные графемы, выращивать их «вниз», заменяя переменные более сложными лексемами, или же комбинировать оба подхода сразу.

Кроме того, процесс сборки лексем никак не ограничен по сложности, в результате чего можно собирать бесконечно много сложных математических выражений. Мы вправе, например, строить многоэтажные башни степеней:

$$5^{4^{3^{2^{1}}}}$$

или изобразить что-нибудь этакое:[2]

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{2}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{2}\right)^3}}. \qquad \text{(A1.1)}$$

Следует, однако, понимать, что математики — тоже люди, и им не хочется громоздить необозримые многоэтажные выражения с огромным количеством символов, поэтому обычно вводятся дополнительные обозначения, позволяющие локально (в рамках одной статьи или книги, например) присвоить часть сложного выражения некоторому более простому выражению (например, одной букве) и в дальнейшем пользоваться им как сокращением. Аналогичного принципа мы придерживаемся и в языках программирования, когда вводим обозначения для функций и переменных.

Вышеупомянутую формулу (A1.1) можно декомпозировать на три более простых выражения, например, так:

$$x = \sqrt[3]{A + \sqrt{B}} + \sqrt[3]{A - \sqrt{B}},$$

где мы ввели временные обозначения:

$$A \overset{\text{def}}{\rightleftharpoons} -\frac{q}{2}, \quad B \overset{\text{def}}{\rightleftharpoons} \left(\frac{q}{2}\right)^2 + \left(\frac{p}{2}\right)^3,$$

символ $\overset{\text{def}}{\rightleftharpoons}$ означает равенство по определению или *присваивание*. Он часто используется для введения обозначений и сокращений в математических текстах. Этот символ ни в коем случае нельзя путать с равенством, поскольку он отражает не смысловое, а графическое равенство, т.е. переобозначение.

Такая инвариантность результата относительно порядка сборки (и декомпозиции) лексемы иллюстрируется с помощью следующей полезной конструкции, которая называется **деревом разбора**. Чтобы было проще, покажем дерево разбора на примере формулы Кардано (см. рис. A1.1). Кроме того, проиллюстрируем использование временных обозначений $A$ и $B$ в той же самой формуле соответствующими деревьями разбора (см. рис. A1.2)

Дерево разбора однозначно восстанавливается по формуле за исключением тех случаев, когда не указан приоритет выполнения операций. Так, формула $a + b + c$ может быть разобрана двумя способами в зависимости от расстановки приоритетов двух операций сложения: $(a+b)+c$ или $a+(b+c)$. Поэтому обычно дерево разбора применяется только к таким выражениям, где проставлены все формально требуемые скобки и тем самым приоритет выполнения операций определен однозначно.

Дерево разбора по сути представляет собой запись алгоритма построения формулы, в котором указано, как из самостоятельных и несамостоятельных графем собирается конкретная формула. Порядок ветвей в этом дереве важен, поскольку получаемый с его помощью текст имеет направленность. Только в том случае, когда мы наделяем текст математической семантикой (например, под знаком + понимаем сложение), можно, следуя свойствам этой семантики, пренебречь порядком ветвей, но в таком случае дерево разбора становится не *синтаксическим*, а *семантическим*.

Из дерева разбора хорошо видно, что построение формулы можно начинать с любого места, тем более, что в нем есть одинаковые ветви. Мы можем построить сначала

[2] Формула Кардано для решения приведенного кубического уравнения $x^3 + px + q = 0$.

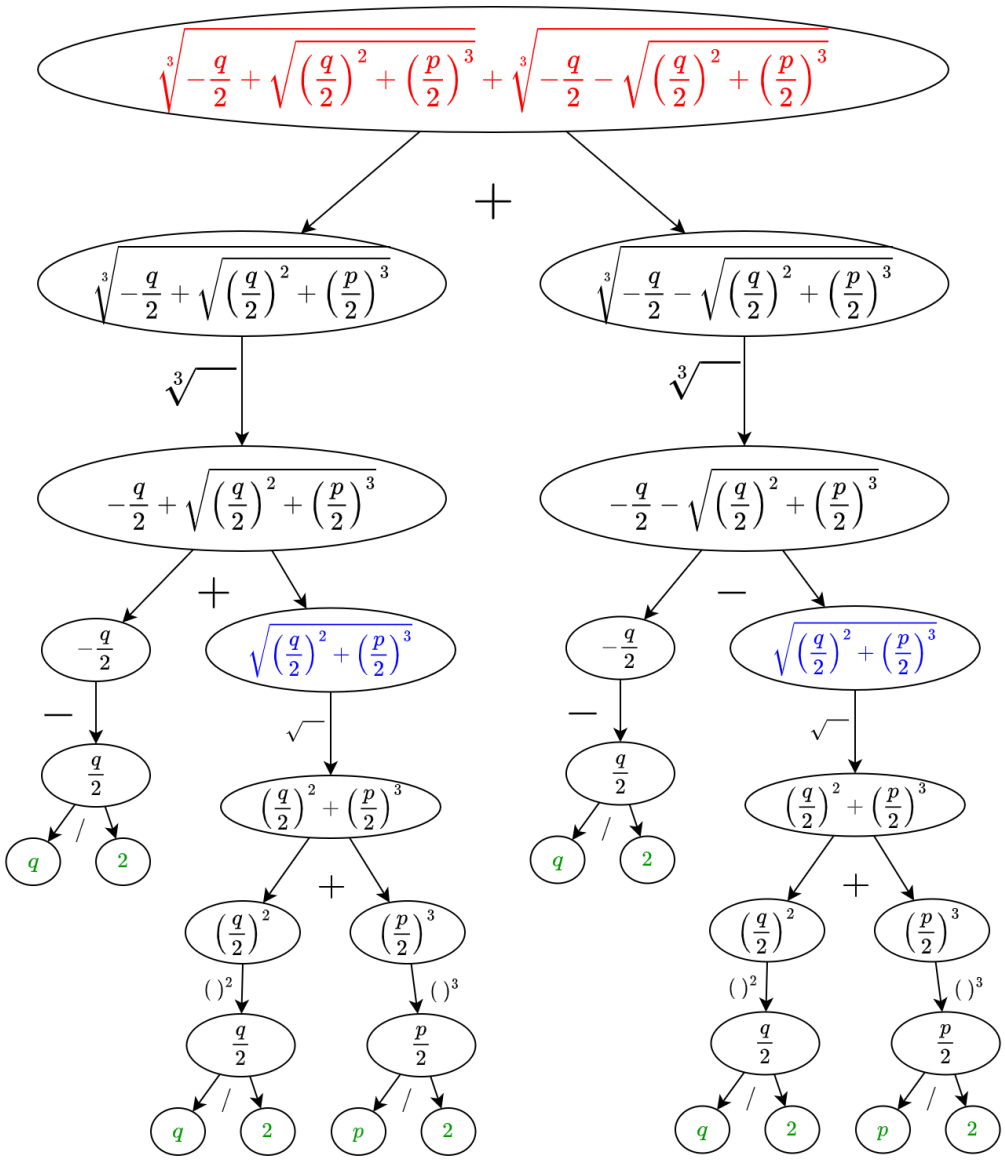


Рис. А1.1. Дерево разбора для формулы Кардано.

подкоренные выражения, потом отложить их в сторону и построить формулу с корнями, под которыми будут пустые подстановочные места, а затем в эти подстановочные места вставить заранее заготовленные подкоренные выражения. Главное здесь — не путать порядок используемых подстановочных мест. Если сложение нам еще может простить такую путаницу, то вычитание и деление не простят, формула станет неверной.

Отметим также, что дерево разбора всегда заканчивается какими-то простейшими графемами, например, символами алфавита или временными обозначениями (которые, как правило, тоже являются алфавитными). Дерево можно модифицировать тремя способами: заменять ветвь на какой-то алфавитный символ (редуцирование), присоединять новую ветвь вместо листа (конечной вершины) дерева (наращивание вниз) и, обратно, само дерево подставлять вместо листа другого дерева (наращивание вверх). При этих манипуляциях мы получаем новые лексемы, соответствующие строгому определению лексем.

Понятие дерева разбора, которое мы используем для анализа структуры формул, не

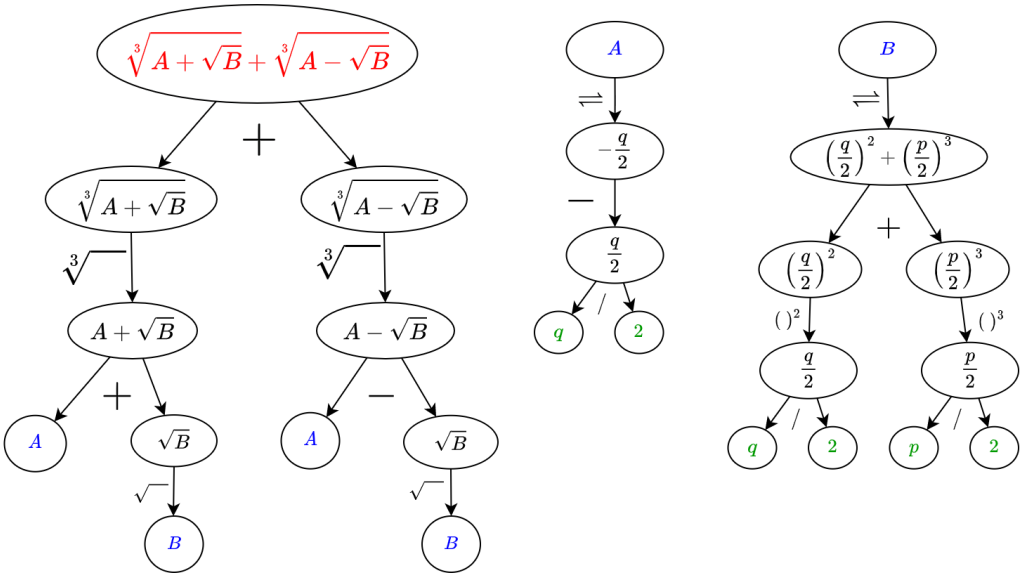


Рис. A1.2. Использование временных обозначений $A$ и $B$

является лишь удобной визуализацией. Это — фундаментальный инструмент, на котором построены языки программирования и системы искусственного интеллекта. Когда компилятор переводит программу, написанную человеком, в машинный код, он первым делом строит именно такое синтаксическое дерево, чтобы понять структуру команд.

Современные системы ИИ, такие как большие языковые модели, не пытаются восстановить грамматическую структуру текста путем явного построения синтаксических деревьев. Вместо этого они улавливают колоссальный объем статистических закономерностей. Поразительно то, что выученные ими неявные структуры настолько точно соответствуют правилам языка, что классические деревья разбора превратились из средства анализа в мощный инструмент для верификации, позволяющий нам убедиться, что машина действительно «поняла» синтаксис.

Глядя на столь красивую законченную идею построения лексем, можно предположить, что любые конструкции, возведенные по принципу матрешки, являются математическими выражениями. На самом деле это не так, и в каждом конкретном формальном фрагменте языка $\mathfrak{Math}$ задаются определенные правила, которые можно применять для сборки выражений путем наращивания дерева разбора. И дело тут не только в типизации лексем, но также и в ограниченном наборе используемых символов. Иначе говоря, конкретный формализм оперирует конкретными графемами. Но других ограничений при этом нет.

Отметим, что сама идея представления сложных выражений через структурированную сборку из более простых элементов имеет глубокие корни. Еще в XVII веке Готфрид Лейбниц мечтал о создании 'characteristica universalis' — универсального символического языка, который позволил бы формализовать человеческие рассуждения. Хотя его проект не был полностью реализован, стремление к точности и структурности в символических записях проложило путь к современной математической нотации, где «принцип матрешки» и анализ структуры выражений (подобный построению дерева разбора) являются неотъемлемой частью.

## A1.3. Семантика vs Синтаксис

Может показаться, что синтаксис языка при построении математической теории первичен, но это не совсем так. На самом деле, прежде чем синтаксис будет полностью определен, необходимо разобраться с тем, насколько богатым должен быть язык, который мы хотим использовать, какие классы объектов он должен описывать, какие взаимосвязи, имеющие место в изучаемой предметной области, он должен выделить как существенные и зафиксировать в своей системе обозначений.

Поэтому первичной для языка, безусловно, является семантика. Но, однажды родившись, формальный язык и построенные на его основе математические теории могут «забыть» исходную семантику и применяться в самых разных областях знаний там, где это «технически» возможно. Следуя Давиду Гильберту, можно заметить, что формальная система работает одинаково хорошо независимо от того, что мы понимаем под обозначенными в ней предметами — будь то точки, прямые и плоскости, либо же столы, стулья и пивные кружки.[3]

*Давид Гильберт*

При этом, однако, не стоит забывать о том, что если точки мы назвали столами, то такую подмену понятий мы производим тотально, т.е. абсолютно все формулы нашего языка отныне будут говорить про столы там, где раньше они говорили про точки, и в то же самое время нельзя подразумевать столы в тех местах, где ранее мы использовали прямые или плоскости, т.е. смешивать исходно различные понятия. Иначе говоря, если уж производить замену понятий (*выбирать интерпретацию*), то это нужно делать согласованно и тотально, поскольку если сама по себе семантическая природа описываемых сущностей не играет роли для формализма, то все отношения между сущностями должны быть адекватно перенесены из одной области в другую. Грубо говоря, если в геометрии у нас имеется формула, выражающая отношение «лежать между» для трех точек, то и в предметной области столов и стульев у нас также будет работать формула, означающая свойство «лежать между», только уже для трех столов.

В контексте современных достижений искусственного интеллекта, эта способность формальных систем «забывать» исходную семантику приобретает новое измерение. ИИ-системы, обучаясь на огромных корпусах данных, *компактифицируют* знания, выявляя наиболее вероятные связи и закономерности. Они не обязательно оперируют с пониманием истинности или ложности в человеческом смысле, но способны вычислить «правильность» или «допустимость» конструкций, основываясь на статистических корреляциях и паттернах, извлеченных из обучающих данных. Это позволяет им, например, генерировать тексты или формулы, которые формально безупречны и даже кажутся осмысленными, даже если внутренняя «семантическая реальность», на которой базируется их генерация, может быть совершенно иной, чем человеческая. Это подчеркивает, как математический язык, благодаря своей строгой структуре, позволяет отделить синтаксис от семантики, создавая универсальный инструмент, применимый даже в тех случаях, когда его пользователи не обладают полным интуитивным пониманием его глубинных смыслов.

Пожалуй, самым ярким примером разброса семантических реализаций математических теорий можно считать теорию групп, которая, как известно, широко используется не только внутри самой математики в рамках более частных теорий, но также в физике,

[3] Неточная цитата из книги К. Рид «Гильберт» [13].

химии, кристаллографии, информатике и даже в некоторых гуманитарных направлениях.

Другой хороший пример различного применения одной и той же теории — это теория линейных операторов, которая применяется, например, в квантовой механике и в алгоритмах машинного анализа текстов, и много где еще.

Попробуем, не вдаваясь глубоко в искусство построения формализмов, пощупать тот механизм, который приводит нас к математическим формулам, на примере логических выражений обычного (разговорного) языка. Прежде всего нам потребуется отделить друг от друга два понятия: объекты (субъекты) и отношения. Как и в разговорном письменной языке, мы будем различать лексемы, соответствующие этим понятиям. **Предикатами**[4] называются лексемы, обозначающие отношение между объектами и/или субъектами, они обычно имеют логический тип семантики. **Термами** называются лексемы, обозначающие объекты исследуемой предметной области.

Так, приведенный выше пример формулы Кардано (A1.1) представляет собой предикат равенства, выражающий тождество корня $x$ и некоторого арифметического выражения. А само это выражение, для которого мы привели дерево разбора на рис. A1.1, представляет собой терм, выражающий описание некоторого объекта (числа). Следуя этому описанию, отправляясь от конкретных значений $p$ и $q$, можно вычислить конкретное значение $x$.

Другой пример предиката: отношение $<$ на целых числах.

Наряду с предикатами используется также более общее понятие — **формула**. Формула, как и предикат, является записью отношения между объектами с помощью предикатов и логических символов. Иначе говоря, формула — это логически выстроенное описание отношения.

Подчеркнем, что предикат иногда может быть определен довольно сложной формулой, т.е. не все предикаты в рамках данного языка имеют элементарный вид с точки зрения определения.

Забегая вперед, воспользуемся некоторыми логическими и математическими спецсимволами: $\forall$ — «для любого», $K \cap M$ — пересечение двух множеств, $k \in K$ — $k$ есть элемент множества $K$.

Предположим, что нашей предметной областью являются животные, т.е. мы выступаем в роли зоологов. Пусть $K$ — множество всех крокодилов, $M$ — множество всех животных в Москве-реке. Любое животное имеет вполне конкретную характеристику — цвет (чтобы не усложнять модель, будем считать, что имеется в виду некоторый один главный цвет). Пусть предикат $\mathscr{A}(k, c)$ принимает истинное значение тогда и только тогда, когда животное $k$ имеет цвет $c$. Пользуясь такими обозначениями запишем следующее утверждение: «Все крокодилы в Москве-реке красные». Получим:

$$\forall k \in K \cap M : \ \mathscr{A}(k, \text{«красный»}). \tag{A1.2}$$

Разберем, как это получилось. Во-первых, мы решили ограничить предметную область только животными. Поэтому любая переменная (в нашем случае $k$) автоматически обозначает у нас произвольное животное. Во-вторых, мы выделили в генеральной совокупности животных два подмножества: «живущие в Москве-реке» и «крокодилы», при этом мы никак не определили эти классы явным образом, так что на самом деле неважно, какие слова для их обозначения мы используем. В-третьих, мы ввели еще один сорт объектов, который назвали цветами (опять же, совершенно неважно, что на

[4] От лат. *praedicatum* — заявленное, упомянутое, сказанное.

самом деле скрывается за этим словом). Наконец, мы добавили в теорию обозначение $\mathscr{A}$ для формулы, которая умеет связывать два вида объектов: животных и цвета. Семантика этого обозначения такова, что мы понимаем под ним соответствие животного и его цвета (в логике это называется *предикатом*, а в разговорном языке роль предиката обычно выполняет глагол). После этого мы написали формулу (A1.2), которая буквально расшифровывается так:

> для любого $k$, который одновременно принадлежит множеству $K$ и множеству $M$, выполняется предикат $\mathscr{A}(k, \text{«красный»})$.

Одновременная принадлежность двум множествам у нас реализована формулой $k \in K \cap M$, которая означает, что $k$ входит в пересечение множеств $K$ и $M$, т.е. является элементом и того, и другого множества одновременно. Иначе эту же формулу можно было бы записать так: $(k \in K) \wedge (k \in M)$, т.е. вместо операции пересечения множеств воспользоваться логической операцией *конъюнкции* ($\wedge$).

Попутно пронаблюдаем, как в формуле $k \in K \cap M$ реализуется «принцип матрешки». Сначала мы взяли алфавитный символ пересечения $\cap$, который имеет два подстановочных места (слева и справа), куда разрешено подставлять только множества, и подставили алфавитные символы $K$ и $M$, получили более сложную лексему $K \cap M$. Затем мы взяли символ принадлежности $\in$, который также имеет два подстановочных места, и подставили, соответственно, переменную $k$ и только что собранную лексему $K \cap M$. Таким образом, лексема $k \in K \cap M$ представляет собой двухуровневую матрешку из двух символов, имеющих подстановочные места (операторные символы), и трех символов без таковых мест (переменные).

Наконец, вспомним про «столы, стулья и пивные кружки». Пусть теперь мы имеем дело не с животными, а со звездами всей Вселенной. Пусть также $K$ есть совокупность всех нейтронных звезд, $M$ — совокупность всех звезд нашей галактики «Млечный путь», $C$ — множество названий цветов, а выражение $\mathscr{A}(k, c)$ говорит нам, что звезда $k$ имеет спектральный класс с преобладающим цветом $c$. В таком случае та же самая формула (A1.2) на сей раз будет иметь следующую семантику:

> всякая нейтронная звезда галактики «Млечный путь» имеет красный спектр

Как видим, мы полностью изменили семантику нашей небольшой теории, но формула (A1.2) при этом не претерпела никаких изменений: формализм остался прежним.

Стоит отметить, что формальная теория становится теорией только тогда, когда помимо языка мы также предъявляем механизм определения того, какие формулы, написанные на этом языке, истинные, а какие ложные. Для этого теория снабжается *аксиомами*, из которых по общим логическим правилам выводятся истинные (относительно данных аксиом) утверждения, называемые *теоремами*.

Добавление аксиом может существенно сузить спектр применения формальной теории, поскольку теория будет иметь ценность только в том случае, когда при наделении ее определенной семантикой из заданной предметной области аксиомы теории будут истинными в данной семантике. Иначе говоря, если мы рассматриваем геометрию Эвклида про точки, прямые и плоскости со всеми пятью постулатами, а потом заменяем их на столы, стулья и пивные кружки, то мы ожидаем, что переписанные в этом новом языке постулаты Эвклида окажутся истинными. В этом случае и все теоремы геометрии будут истинными для столов, стульев и кружек, и теория будет полезной в данной предметной области. Любое же мельчайшее несоответствие аксиом или теорем свойствам

реальных объектов, к которым мы пытаемся применить формальную теорию, означает невозможность ее использования в данном случае.

Подводя промежуточный итог, отметим, что язык математики достаточно гибок для того, чтобы описывать на нем самые разные предметные области. Кроме того, он достаточно абстрактен для того, чтобы имелась возможность один и тот же язык использовать в совершенно различных ситуациях, т.е. математический язык, будучи порожденным какой-то конкретной семантикой, почти мгновенно отрывается от нее, следуя только своей внутренней архитектуре и правилам, никак не связанным с предметной областью.

Эта универсальность языка дает гарантию надежности всех результатов, полученных в нем: если язык удалось адекватно сопоставить с какой-то областью, и в этой области верны некоторые аксиомы, то в ней верны также и все теоремы, доказанные чисто логически из данных аксиом. Такое свойство математических теорий позволяет рассматривать их сами по себе, в отрыве от конкретных реализаций, и получать универсальные абсолютно точные теоремы.

Нужно отметить также, что и внутри самой математики существуют различные уровни абстракции и соответствующие им формальные языки и теории. Так, язык логики первого порядка (исчисление предикатов) является наиболее абстрактным и работает практически во всей математике без ограничений. Он и является тем самым рафинированным остовом аристотелевской логики, который мы называем формальной логикой.

Язык теории множеств является «овеществлением» логики в терминах множеств и элементов, он позволяет строить абсолютно все математические конструкции в виде конкретных множеств (или их классов). Однако сама по себе теория множеств страдает неполнотой в отличие от логики предикатов, что приводит к различным интересным «парадоксам». Следующей теорией по силе абстракции, видимо, следует считать теорию групп и колец, которая, как мы уже отмечали, имеет массу конкретных реализаций в самых разных областях исследований как в самой математике, так и за ее пределами.

С другой стороны, применение теорий в конкретных ситуациях следует производить с осторожностью: не путать, не менять и не дополнять введенные понятия, проверять истинность используемых аксиом в данной предметной области, не вводить в язык новые понятия, имеющие какой-либо внешний контекст, без строгого их определения в рамках самой формальной теории.

Наконец, нужно отметить, что в силе математических теорий заложена и некоторая их слабость, а именно: все результаты теории являются обезличенными, они не могут «почувствовать» тонкости, отличающие одну реализацию теории от другой. Неформально говоря, математическая теория «не видит» разницы между теми своими реализациями, которые являются корректными.

## A1.4. Рефлексия

Очень важным свойством языка $\mathfrak{Math}$, как, в общем-то, любого достаточно развитого разговорного языка, является способность к *рефлексии*, т.е. возможность на этом языке описывать и анализировать внутренние закономерности самого себя.

Для этого обычно в языке выделяется специальный корпус графем, заточенный под описание элементов и конструкций самого себя. Эта специальная часть языка становится самостоятельным языком со своими особенностями, но в целом следует правилам

более общего, изучаемого ею языка. Обычно язык, используемый для описания других языков, называют **метаязыком**. В языке, способном к рефлексии, метаязык является его собственной частью.

Отметим, что инкапсуляция метаязыка в исходный язык Math позволяет, на самом деле, и метаязыку описывать самого себя, как часть языка Math. И здесь мы можем привести иллюстрацию из разговорного языка. В любом развитом языке, в частности, в русском, есть прилагательные, которые качественно характеризуют какие-либо предметы и явления. В частности, мы можем рассмотреть прилагательные, которые описывают свойства прилагательных. Например, любое прилагательное можно охарактеризовать как сложное или простое в зависимости от того, как оно устроено (скажем, «красный» — простое прилагательное, а «сложносоставной» — сложное, т.к. включает два образующих корня). Таким образом, среди всех прилагательных разговорного языка можно выделить класс прилагательных, которые могут быть использованы для описания всех прилагательных. Это и будет простейший метаязык внутри разговорного (русского) языка.

На рефлексии основаны различные «неудобные» логические парадоксы. Во-первых, это всем известный парадокс лжеца (или брадобрея), который мы не будем здесь повторять. Во-вторых, с прилагательными тоже можно придумать парадокс. Коль скоро прилагательные умеют что-то говорить про самих себя, разделим их на два класса: *самоприменимые* и *несамоприменимые*. Например, прилагательное «сложносоставной» является самоприменимым, т.к. оно действительно является сложносоставным (происходит от двух основ), а прилагательное «несложносоставной» явно не является самоприменимым.

Теперь зададим вопрос: а к какому классу относится прилагательное «несамоприменимое»? С одной стороны, если оно сампримениmo, то оно является несамоприменимым (ибо оно нам об этом говорит), с другой стороны, если оно несамоприменимое, то оно именно таким свойством и обладает, т.е. является самоприменимым. Получается неразрешимый логический парадокс.

Чтобы не впадать в подобные ловушки, обычно требуют ограничить *самореферирующие* определения, т.е. определения, ссылающиеся на самих себя, а то и вовсе их запретить. Так что метаязык обычно обособляется от остального языка и сам про себя ничего не говорит.

Аналогичным трюком воспользовался Гёдель для получения своей самой знаменитой теоремы о неполноте формальной арифметики. Дело в том, что арифметика способна сама себя анализировать, если определенным способом научиться нумеровать арифметические формулы (т.е. лексемы языка арифметики), и в ней тоже можно найти утверждение, которое будет заявлять нечто о самом себе. Но в арифметике этот парадокс разрешается тем, что мы отделяем понятие истинности от доказуемости, выводя тем самым «нехорошие» высказывания в серую зону понятия доказуемости (они становятся ни доказуемыми, ни опровержимыми). С одной стороны, это спасает математику от противоречий, с другой стороны, дает повод усомниться в ее всесильности.

Что касается языка Math, которым мы здесь занимаемся, то, как уже было сказано, мы просто не будем применять метаязык к анализу самого себя, считая его понятия и лексемы некой надстройкой более высокого порядка. С одной стороны, мы избегаем логических парадоксов, с другой стороны — получаем в руки более-менее стандартные языковые средства, позволяющие рассуждать в целом о языке Math некоторым формализованным образом, по возможности избегая средств разговорного языка (на котором до сих пор излагается эта книга).

В целом, нужно отметить, что такой дуализм языка в математике скорее правило, чем исключение. Математик всегда работает одновременно на двух уровнях языка: конкретном и абстрактном. Конкретный язык описывает исследуемые предметы и явления формально (например, линейные операторы и их свойства), абстрактный язык обслуживает процесс оперирования конкретным языком и наполнением его смыслом (например, для введения определений и пояснения целей формальных выкладок).

Наиболее отчетливо такой дуализм наблюдается в математической логике, где мы исследуем какую-то формальную систему (например, арифметику Пеано) с помощью более абстрактных инструментов логики и теории множеств. Более того, над этой метатеорией множеств мы также имеем в виду и мета-метатеорию, которая описывает общую канву исследований данной формальной системы.

На заметку: у любого художественного произведения тоже есть несколько смысловых уровней: то, что автор описал буквально; то, что он имел в виду (скрытый смысл, управляемый автором); а также непроизвольное проявление личности самого автора в данном произведении.

## A1.5. Термины

Связь языка $\mathfrak{Math}$ с разговорным (в нашем случае — русским) языком остается весьма прочной прежде всего через такое понятие как **те́рмин** (не путать с *термом*!). Дело в том, что лексемы сами по себе, как синтаксические единицы, не наделены смыслом, но для того, чтобы придать им определенную семантику (как тот самый робот из рассказа Азимова), мы должны так или иначе закрепить за лексемами какие-то понятия. Например, лексема sin служит для обозначения функции синуса. В этом есть определенный смысл выбранного обозначения: во-первых, график синуса похож на вогнутый берег, который называется заливом, во-вторых, по латыни залив — *sinus*, откуда и взялось обозначение. Таким образом придумываются в науке большинство (если не все) словесных обозначений понятий. Но ведь слово разговорного языка, записанное на бумаге, («sinus» или «синус») — это лексема данного слова в данном разговорном языке.

Отсюда возникает определение: **термином** мы называем лексему разговорного языка, закрепленную за данным понятием и имеющую соответствующую лексему в языке $\mathfrak{Math}$.

Итак, есть понятие функции синуса, за которым закреплен термин «синус» и лексема sin (языка $\mathfrak{Math}$).

Термины очень удобны, когда мы хотим определить какое-то понятие (локально в данной статье/тексте или глобально для всей науки), для которого нет устоявшейся лексемы, а само определение достаточно длинное, чтобы его каждый раз выписывать. Например, термин «функция» выделяет строго определенное понятие в математике, имеющее нетривиальное определение. Более того, сам по себе разговорный термин несет в себе определенную коннотацию, которая (так же, как в случае с заливом и синусом) перебрасывает мостик между смысловым наполнением разговорного термина и строго определенным формальным математическим понятием. Это практично, экономично и органично.

Таким образом, наличие терминов, взятых из разговорного языка и сопровождающих понятия и лексемы языка $\mathfrak{Math}$, обеспечивает нам некоторую базовую семантику, позволяющую а) лучше запоминать лексику языка $\mathfrak{Math}$, б) легче читать тексты на

языке $\mathfrak{Math}$ и в) быстрее усваивать новые понятия и связи между ними, что является немаловажным гуманитарным фактором при работе с языком $\mathfrak{Math}$.

Ведь, как говорили древние греки, мерой всех вещей является человек!

При этом не стоит забывать, что семантика разговорного языка, проявляющаяся в терминах, является вспомогательной, иллюстративной (как картинки и графики), она не может служить доказательной базой внутри самого языка $\mathfrak{Math}$.

## A1.6. Переменные и свертки

Проводя аналогию с разговорным языком, под **переменными** мы можем подразумевать достаточно простые лексемы, которым отведена роль обозначать произвольный элемент некоторого класса. Например, в разговорном языке под словом «человек» понимается какой-то человек (не какой-то конкретный человек и не все люди в целом, а просто произвольный представитель множества людей). Так и в языке $\mathfrak{Math}$, когда мы хотим что-либо сообщить о произвольном объекте данного рода, мы его обозначаем некоторой переменной, например, $x$ или $y$, и далее пользуемся этой переменной в формулах. По сути переменная — это тоже временное обозначение, но не для конкретной формулы, а для произвольного объекта из того класса объектов, которые мы описываем в нашем языке.

Нужно отметить, что несмотря на достаточно простое определение переменной, само по себе это понятие — достаточно сложное с точки зрения семантики. Если вспомнить языки программирования (которые можно считать реализациями языка $\mathfrak{Math}$), то переменные бывают нескольких типов, например, строковые или числовые. Это значит, что за переменной закрепляется некоторый *тип*, который ограничивает возможности использования этой переменной. С одной стороны, это заставляет нас производить согласование типов, когда мы составляем какие-либо сложные лексемы, чтобы, например, случайно не подставить буквы вместо числовой переменной, с другой стороны, это сильно упрощает синтаксис, поскольку не нужно на протяжении всего текста (например, статьи по математике или листинга программы) явно указывать, какие значения может принимать та или иная переменная. Достаточно при определении переменной сказать что-то вроде «пусть $x$ — произвольное натуральное число».

Вторая проблема, связанная с понятием переменной, — это, собственно, определение данного понятия. Чисто синтаксически понятно, что если есть переменная некоторого типа, то вместо нее можно подставлять любую лексему того же типа. Но это как минимум означает, что мы должны распределить все лексемы по типам, т.е. навязать им некоторую классификацию несинтаксического свойства. В формальных математических теориях так и поступают. При определении того фрагмента языка $\mathfrak{Math}$, который будет использоваться в конкретной теории, мы оговариваем сразу, как должны выглядеть лексемы того или иного типа, либо же постулируем отсутствие типов. В последнем случае все намного проще, поскольку переменные могут пробегать все возможные объекты, описываемые этой теорией, без каких-либо ограничений.

Неформально можно представлять себе переменную как некоторую ячейку определенной формы, в которую можно положить только совместимые по форме предметы (в треугольную ячейку — треугольные призмы, в круглую — цилиндры, и т.д.). Подходящие по форме предметы — это реализации данной переменной внутри своего типа. В разговорном языке аналогами переменных являются имена нарицательные. Например,

слово «дом» в каждом конкретном контексте может обозначать какой-то конкретный дом или разновидность домов, но не может применяться к человеку или животному.


*Тип*

В математике выделение классов объектов из общего разнообразия достигается написанием определяющей *формулы* и введением *термина*. При этом, как уже говорилось, сам по себе термин не относится к языку $\mathfrak{Math}$, он просто подменяет собой определение, выраженное на языке $\mathfrak{Math}$, каким-то говорящим словом. Например, «функция», «целое число», «квадратичная форма», «замкнутое множество» — это термины, за которыми не закреплены обозначения переменных. С другой стороны, есть термин «ординал», за которым иногда закрепляются переменные из начала греческого алфавита (если это текст из оснований математики), чтобы всегда под $\alpha$, $\beta$, $\gamma$ понимать произвольные ординалы. При этом мы часто определяем обозначение для класса, которое можно считать обозначением константы, т.е. именем собственным. Например, класс всех ординалов обозначается Ord, класс всех целых чисел — $\mathbb{Z}$ и т.д. В разговорном языке классы однородных предметов обычно именуются словами во множественном числе, например, «дома», «люди» и т.д. Это означает, что «дом» есть элемент класса «дома». Сравните: $\alpha$ есть элемент класса Ord (ординал есть элемент класса ординалов).

Однако большинство имен нарицательных в разговорном языке — это обозначение довольно узких классов вещей. Тот же «дом» — это очень специальный класс предметов, имеющий сравнительно небольшой объем по сравнению с объемом вообще всех вещей, описываемых языком.

В то же время, в математике (и программировании) переменная обычно пробегает достаточно общий класс (по модулю рассматриваемой реализации языка $\mathfrak{Math}$). А значит, сравнение переменных только с именами нарицательными из обычного языка не вполне корректно. И тут нам на помощь приходят местоимения. Ведь такие слова, как «он», «она», «оно», «этот», «эта» и т.д., применимы в разговорном языке к очень широким классам объектов, т.к. разделяют их только по родовому признаку. Поэтому переменные можно сравнивать как с именами нарицательными, так и с местоимениями (но помнить, что любая аналогия неполна).

Как видим, и само понятие переменной, и ее соотнесение с понятиями из разговорного языка вызывает определенные затруднения и не является однозначным. Это значит, что параллели между математическим и разговорным языками нужно проводить с осторожностью.

Переменные позволяют нам выделить один особенный класс лексем языка $\mathfrak{Math}$ под общим названием **свертки**. Под сверткой мы будем понимать такие лексемы, в которых переменные (одна или больше) играют роль итератора, по которому производится некоторое действие или берется предикат, в результате чего эта лексема обозначает объект, не зависящий от переменных, по которым производится итерирование. Эти итерируемые переменные называются *связанными* (данной сверткой), и их можно заменять на другие переменные того же типа, но нельзя заменять никакими другими лексемами. Свертка уменьшает число свободных параметров исходного выражения, которым она определяется.

Приведем примеры лексем-сверток (отделены друг от друга запятыми):

$$\int_0^1 e^{-x}dx, \quad \sum_{n=1}^{100} 2^n, \quad \{x \mid x^2 > 2\}, \quad \forall x\ (x = x), \quad \exists x\ (x > 0).$$

Здесь переменные $x$ и $n$ — те самые связанные переменные, по которым производится итерирование некоторой операции (в случае интеграла и суммы — суммирование, в случае множества и кванторов — проверка истинности соответствующего предиката). В конкретной математической семантике у каждой из этих лексем-сверток мы получаем конкретное значение, которое не зависит от $x$ и $n$.

Часто лексема-свертка содержит переменные, которые она не связывает. Такие переменные называются *свободными переменными* или *параметрами*. Покажем это на примерах.

▶ **Свертка функций.** Свертка $(f * g)(t)$ обычно определяется интегралом:[5]

$$(f * g)(t) \stackrel{\text{def}}{=\!=} \int_{-\infty}^{+\infty} f(\tau) g(t - \tau) d\tau.$$

Здесь $\tau$ — связанная переменная (итератор), которая «поглощается» интегралом. В отличие от нее, $t$ — это свободная переменная (параметр) внутри связывающей лексемы. Результирующая лексема является записью функции от $t$, т.к. ее значение меняется при варьировании параметра $t$.

▶ **Свертывание множества с параметром.** Рассмотрим множество всех вещественных чисел, строго меньших некоторого числа $c$:

$$M_c \stackrel{\text{def}}{=\!=} \{x \mid (x \in \mathbb{R}) \wedge (x < c)\}.$$

Переменная $x$ связана фигурными скобками (нотацией построения множества) и служит лишь для описания элементов. Переменная $c$ является параметром; изменение $c$ меняет само множество (например, $M_0$ — это множество отрицательных чисел, тогда как $M_{10}$ — более широкое множество).

▶ **Кванторы с параметрами.** Формула $\exists x\ (x^2 = a)$ содержит связанную переменную $x$ и параметр $a$. Эта формула утверждает, что $a$ имеет квадратный корень. Истинность этого утверждения полностью зависит от значения параметра $a$ (в области вещественных чисел оно истинно для $a \geqslant 0$ и ложно для $a < 0$).

Таким образом, свободные переменные действуют как «входной интерфейс» лексемы, связывая ее с внешним контекстом, тогда как связанные переменные обеспечивают внутреннюю работу механизма свертывания.

Является ли эта концепция свертки чисто математическим изобретением? Вовсе нет. На самом деле, естественный язык активно использует очень похожий механизм, хотя он и менее строго формализован. Когда мы используем обобщающие конструкции, мы, по сути, создаем свертку. Хороший пример — знаменитая фраза, которая, по легенде, была начертана над входом в Академию Платона:

«***Тот, кто*** *не знает геометрии, да не войдет сюда.*»

Синтаксически это явная структура связывания через квантор. Фраза «Тот, кто» по существу играет роль квантора всеобщности ($\forall$) в сочетании со связанной переменной. Она не относится к конкретному человеку; скорее, она создает временный заполнитель

[5] Здесь слово «свертка» относится не только к синтаксическому объекту (лексема-свертка), но и непосредственно к математическому объекту — функции. Это — термин из функционального анализа.

(placeholder) для произвольного человека, назовем его $x$. Если этот произвольный человек $x$ подходит под описание, то запрет распространяется на $x$.

В этой конкретной фразе слова «геометрия» и «сюда» выступают как **константы** (конкретные значения). Они определяют конкретный экземпляр правила. Однако мы легко можем представить общий логический *шаблон*, стоящий за этой фразой:

«***Тот, кто*** *не знает Предмета, да не войдет в Место.*»

В этом шаблоне «Предмет» и «Место» становятся **параметрами** (свободными переменными). Присваивая этим параметрам различные значения, мы меняем область действия правила, не меняя его внутренней логики связывания. Например, если мы положим Предмет $\overset{\text{def}}{\rightleftharpoons}$ «пароль», а Место $\overset{\text{def}}{\rightleftharpoons}$ «серверная», мы получим стандартный протокол безопасности. Это полностью аналогично **свертке с параметрами**, такой как выражение $\exists x(x^2 = a)$, которое мы обсуждали ранее. Логическая структура (связывание переменной $x$) остается прежней, но конкретное утверждение зависит от значения, присвоенного свободному параметру $a$.

Математика просто берет эту естественную языковую способность к обобщению и накладывает строгие правила на *область действия* переменной (где она начинается и заканчивается) и ее *тип*, предотвращая двусмысленности, часто встречающиеся в обычной речи.

## A1.7. Особенности математического языка

Настало время подвести некоторый промежуточный итог нашим изысканиям. В этом разделе мы отметим основные черты языка $\mathfrak{Math}$, которые в совокупности делают его, с одной стороны, уникальным с точки зрения наших знаний о языках вообще, а с другой стороны, подчеркивают и некоторую общность с ними:

1. Горизонтальная направленность текста.
2. Принцип матрешки и однозначность разбора лексем.
3. Синонимы и редукции.
4. Финитность конструкций.
5. Строгая детерминированность переменных.
6. Изъявительная форма повествования.
7. Отсутствие обычных спряжений и склонений.

**Горизонтальную направленность текста** вряд ли можно назвать отличительной чертой языка $\mathfrak{Math}$, поскольку она свойственна и разговорным языкам. Однако и в математике, и в языках программирования общее правило чтения лексем слева направо часто встраивается в некоторый структурный порядок текста, где, с одной стороны, внутри лексем допускаются самые разные направления (вспомните хотя бы обозначение определенного интеграла или матрицы) и порядок чтения зависит от семантики конкретного шаблона, а с другой стороны, общая логика текста подразумевает скорее вертикальную ориентацию сверху вниз, что в общем тоже согласуется с разговорными

языками, но лишь отчасти. Особенно это заметно в структуре листинга программ, когда переход на новую строку определяется не столько шириной носителя текста, сколько правилами обработки (чтения) данного текста. То же самое можно заметить и в отношении отступов в начале строки: часто они имеют значение не только для красоты и удобства чтения вложенных блоков программ, но и несут определенный функциональный смысл (как, например, в языке Python).

**Принцип матрешки** — пожалуй, главное отличительное свойство языка 𝔐𝔞𝔱𝔥, поскольку он является определяющим для понятия лексемы нашего языка. Этот принцип, с одной стороны, позволяет потенциально бесконечно генерировать новые лексемы, с другой стороны, появляется возможность разобрать каждую лексему на составляющие части (построить дерево разбора) и понять, как она была сконструирована. Причем, как правило, такой разбор производится однозначно (даже если существуют альтернативные варианты разбора, то они в некотором смысле эквивалентны).

Данная особенность языка 𝔐𝔞𝔱𝔥 резко выделяет его на фоне разговорных языков. Конечно, некоторую рекурсивность или структурность можно усмотреть и в разговорных языках: все мы с детства помним, что предложение можно разложить на подлежащее, сказуемое и второстепенные члены, которые, в свою очередь, можно представить различными видами частей речи (существительное, глагол, прилагательное, наречие и т.д.), те уже представляются конкретными словами, а слова — морфемами и, в конце концов, буквами. Однако мы сразу же видим, во-первых, ограниченность такой иерархии, поскольку сложность структуры речи мы не можем наращивать неограниченно, а во-вторых, изначально заложенную типизацию элементов на каждом уровне «сборки» текста (например, в качестве сказуемого нужно всегда использовать глагол или, реже, составное (именное или глагольное) сказуемое). Это тот самый случай типизации, который мы обсуждали выше в связи с переменными, однако в разговорном языке типизация больше привязана к структуре речи, чем к семантике, в то время как в математике типизация прямо указывает на семантику объектов, описываемых лексемами того или иного типа.

Справедливости ради, стоит привести пример исключения, которое лишь подтверждает правило: в разговорном языке можно придумывать сколь угодно много уровней вложенности, если рассматривать цепочку придаточных предложений:

Вот два петуха,
Которые будят того пастуха,
Который бранится с коровницей строгою,
Которая доит корову безрогую,
Лягнувшую старого пса без хвоста,
Который за шиворот треплет кота,
Который пугает и ловит синицу,
Которая часто ворует пшеницу,
Которая в тёмном чулане хранится
В доме, который построил Джек.

И здесь мы можем видеть что-то вроде башни степеней из арифметики. Примечательно, что хотя обе конструкции (как в данном стихе, так и в случае башни степеней) никак не ограничивают нас в творчестве, чрезмерное увлечение ими приводит к полной нечитабельности текста.

Кроме того, большинство разговорных языков не являются аналитическими, т.е. те лексемы, которые используются при построении текста разговорного языка, могут

иметь т.н. начальную форму и различные вариации, образованные с помощью зависимых морфем (окончаний, суффиксов, приставок и т.п.), которые видоизменяются в зависимости от контекста. Язык 𝔐𝔞𝔱𝔥, если не относить к нему термины, взятые из разговорных языков, наоборот, предельно аналитичен именно в силу природы его лексем. Действительно, трудно представить себе математические лексемы, части которых обладали бы склонностью к изменениям в зависимости от окружающих их графем. Обычно такого рода изменения реализуются функциями и условными операторами, которые сами по себе также предельно аналитичны.

Собственно говоря, аналитичность языка и возможность построить дерево разбора чисто синтаксическими методами (например, анализируя скобки в тексте) — две стороны одной медали.

На полях отметим, что несмотря на всю сложность и неаналитичность разговорных языков, математика предлагает ряд методов их изучения с помощью неклассических логик, например, к таковым относятся субструктурные логики Ламбека, формализующие определенным образом (через некоммутативные алгебры) синтаксическую структуру предложений разговорного языка.

В языке 𝔐𝔞𝔱𝔥, как и в разговорных языках можно обнаружить такие явления как **синонимы** и **редукции**.

**Редукции** в математике распространены не менее щедро, чем в разговорных языках, хотя, как правило, они имеют строго регламентированную природу. Прежде всего это касается скобок. Например, по правилам построения арифметических лексем мы должны записывать выражение $a+bc$ как $(a+(bc))$, однако такое обилие скобок вызывает сложности в восприятии текста, и поэтому существуют стандартные приоритеты операций (как в математике, так и в программировании), позволяющие произвести однозначный синтаксический разбор данной лексемы, предварительно восстановив редуцированные скобки.

В разговорных языках редукции также имеют место, например, типичное французское сокращение *du* для сочетания *de le*, а также немецкое *im* для *in dem*. В отличие от математических редукций разговорные не имеют какой-то общей системы правил и просто сами по себе являются уникальными правилами. Впрочем, и в математике бывают такие частные редукции, которые вводятся скорее как переобозначения «на лету» для удобства локально производимых выкладок, с тем чтобы по завершении этих выкладок забыть о введенном переобозначении.

Термин *синоним* требует отдельного уточнения. Обычно под синонимами понимают два слова, обозначающие одно и то же понятие, либо очень близкие понятия. Например, «кавалерия» и «конница» суть синонимы. Однако, когда мы обсуждаем язык 𝔐𝔞𝔱𝔥, мы еще не в состоянии оперировать термином «равенство» и уж тем более термином «близкий» или «похожий», поскольку для этого нам нужно научиться давать определения, а также ввести определенную аксиоматику (хотя бы для равенства). Единственное равенство, которое мы в состоянии предъявить на уровне лексем — это посимвольное тождество лексем. Но в таком случае синонимами у нас могут быть лишь полностью совпадающие лексемы, т.е. синонимов как таковых и нет. Тем не менее, если вспомнить о редукциях и сопутствующих им соглашениях о приоритетах, то мы уже можем построить целый класс синонимичных лексем, считая синонимами те лексемы, которые получаются друг из друга редукцией скобок.

Более того, если привлечь на помощь семантику языка, то можно дать косвенное определение синонимов как *таких лексем, которые имеют одинаковую семантику в рамках конкретной реализации языка* 𝔐𝔞𝔱𝔥. Например, если речь идет о языке арифме-

тики, то синонимами могут быть лексемы 10 и 010, поскольку ведущий ноль в числах обычно игнорируется, но в ряде случаев может быть полезен для синтаксических разборов. Или, например, буквы E и M могут использоваться как синонимы для обозначения математического ожидания, а дробь как правило имеет два равнозначных представления: $a/b$ и $\frac{a}{b}$. Однако такого рода синонимы все-таки редки в математике, а «настоящее» проявление синонимов возможно только после введения равенства в язык, когда принципиально разные по виду лексемы оказываются эквивалентными в силу каких-то логических свойств рассматриваемого языка.

Немного хуже дело обстоит с многозначностью лексем, т.е. тех случаев, когда одна и та же лексема в зависимости от контекста может иметь различную семантику. Достаточно вспомнить букву $\omega$, которая может обозначать и первый бесконечный ординал, и период маятника, и число Эйзенштейна $(-1+i\sqrt{3})/2$; другой пример — буква $i$, которая часто выступает как индекс суммирования и как мнимая единица. Здесь мы наблюдаем полную аналогию с разговорными языками, где одно слово может иметь множество смысловых оттенков в зависимости от контекста, а нередко и просто обозначать совершенно разные вещи (например, омографы «за́мок» и «замо́к», омоформы «мой» (местоимение) и «мой» (глагол повелительного наклонения) и т.д.).

Заметим, что в программировании такие вещи обычно пресекаются интерпретатором, поскольку в данном случае интерпретатором является машина, в то время как в разговорных языках и в математике интерпретатором является человек, которому свойственно экономить на обозначениях в угоду вариациям контекста.

Мы в дальнейшем постараемся придерживаться *контекстно-свободных* лексем, чтобы не запутать читателя еще больше.

Говоря о **финитности конструкций**, мы подразумеваем то обстоятельство, что все лексемы языка $\mathfrak{Math}$ конечны по своей природе. Иначе говоря, каждая лексема изготавливается из конечного набора графем за конечное число шагов. В разговорном языке, разумеется, все конструкции также финитные. И хотя они используют такие неопределенные термины как «и т.д.», «и т.п.», это отсылка к потенциально бесконечному процессу, описываемому данным конечным текстом.[6]

Здесь мы имеем полную аналогию с математическим языком. Тем не менее, такую финитность нашего языка следует, по-видимому, считать, особенностью, поскольку сами математические объекты, которые этим языком описываются, часто имеют актуально бесконечную природу, причем разнообразие этих бесконечностей поражает воображение. И все же, именно в силу конечности самого языка на практике мы оперируем лишь конечным числом объектов или их типов, среди которых есть и самые разные бесконечности. Такой вот парадокс или, лучше сказать, антиномия.

Еще одна особенность языка $\mathfrak{Math}$, которую мы здесь отметим, — это **строгая детерминированность переменных**.

Под этим словосочетанием следует понимать, прежде всего, свойство «изотропности» переменных, т.е. если данной переменной присвоено какое-то значение (одно конкретное или тип), то во всех вхождениях ниже по тексту эта переменная имеет ровно такое же значение, пока она не будет явным образом переопределена. Иначе говоря, если мы где-то выполнили присвоение $a \overset{\text{def}}{\rightleftharpoons} 2$, то все вхождения $a$ далее имеют значе-

[6] В математике вместо и т.д. мы используем многоточие, но это скорее элемент метаязыка, чем какого-либо формализма. В формальных системах иногда допускаются бесконечные формулы или секвенции, например, $\omega$-правило в языке $\mathrm{PA}_\omega$, но все такие бесконечности имеют строго регулярную, конечно описываемую конструкцию.

ние 2, сколько бы раз эта переменная ни появилась в тексте вплоть до следующего переопределения (отметим, что здесь важную роль играет направленность текста). Это свойство переменных мы будем подразумевать в дальнейшем, записывая подстановки вида $[a/x]$ (это омограф дроби, а не дробь!), которые означают, что в данной формуле требуется все вхождения переменной $a$ (как подстроки) заменить на $x$.

Заметим, что в разговорных языках самые общие аналоги переменных, т.е. местоимения, не подчиняются такому свойству. Например, в тексте

«Она должна ехать на юг. Река здесь есть? — Она за лесом»

значение слова *она* меняется прямо «на лету», при этом читатель однозначно может восстановить это значение из контекста. В математике и программировании такие фокусы недопустимы.

Тем не менее, кое-какой аналог контекстного переопределения переменной имеется и в языке Math. Речь идет о **лексемах-свертках**. В свертке, во-первых, всегда присутствует переменная (хотя бы одна), а во-вторых, эта переменная имеет строго ограниченную область действия. Например, в лексеме $\forall x \in A \ (x = x^2)$ мы принудительно ограничиваем значения переменной множеством $A$ и для таких значений далее заявляем некое равенство, стоящее в скобках. При этом мы можем следом написать еще одну лексему вроде $\exists x > 0 \ (x^2 < 0)$, и будет понятно, что теперь область значений переменной $x$ сменилась с множества $A$ на множество положительных чисел, и эти области значений переменной $x$ актуальны только для формулы, стоящей следом в скобках. В программировании такое ограничение области действия переменной наблюдается, например, в циклах и функциях, где переменная имеет строго локальный контекст. Тем не менее, как видим, переопределение переменной «на лету» строго формализовано и не допускает разночтений.

Таким образом, свертка позволяет нам синтаксически обособить некоторый фрагмент текста и для него задать свои допустимые значения переменных. Более того, можно встретить иногда вложенные свертки, использующие одну и ту же переменную, например, такие:

$$\sum_{k=1}^{\infty} k^2 \left( \sum_{k=-10}^{10} k a_k \right)^3 + k^3 \left( \sum_{k=-100}^{100} k^2 b_k \right)^5 .$$

В принципе, понятно, что «внешнее» $k$ здесь не имеет никакого отношения к обоим «внутренним» $k$, которые тоже никак не связаны друг с другом, т.е. мы имеем дело со свертками внутри свертки, в каждой из которых переменная $k$ принимает разные, вообще говоря, значения. В этом можно усмотреть аналог той текстовой фразы с местоимением «она», которую мы приводили выше. Но нужно отметить, что лексемы такого вида хоть и законны, но как правило не используются. Дело в том, что они будут работать ровно до тех пор, пока не потребуется внешнюю переменную $k$ использовать совместно с внутренней в одной формуле. В самом деле, рассмотрим такую лексему:

$$\sum_k \int_0^{\infty} e^{itk - t^2} dt.$$

Здесь сверточные переменные $k$ и $t$ встречаются в общем арифметическом выражении $itk - t^2$. Что случится, если мы их обозначим одинаково? Получится такая лексема:

$$\sum_x \int_0^{\infty} e^{ixx - x^2} dx.$$

И здесь мы перестаем уже понимать, по какой части формулы надо интегрировать, а что является параметром суммы.

Поэтому общий подход к вложенным сверткам заключается в том, *чтобы все сверточные переменные были разными*. Более того, в современной логике вообще принято разделять переменные на два класса: *свободные* и *связанные*. Связанные переменные используются для формирования сверток, а свободные переменные обозначают внешние параметры. Такой подход позволяет избегать описанных выше коллизий с названиями переменных.

Наконец, отметим также, что в языке Math все повествование происходит в **изъявительном наклонении**, т.е. в математике мы описываем вещи как они есть. В тексте доказательств мы можем прибегать к использованию условного наклонения, например, при доказательстве методом от противного, когда нам нужно что-то предположить, а затем опровергнуть, но на формальном уровне это никак не проявляется.[7] Тем более в математике не используется повелительное наклонение иначе как при присваивании значений переменных. Мы можем сказать «пусть $x = 2$», и это выглядит как повелительное наклонение, однако на формальном уровне это записывается как посылка импликации.

Последнее, что стоит отметить как особенность математического языка, — это отсутствие изменений имен объектов (аналоги существительных) и операций (аналоги глаголов) по лицам, числам, родам, падежам, временам, видам. Здесь уместно вспомнить, что и для разговорных языков не все эти атрибуты обязательны, например, в английском языке нет родов и падежей, а также видов глаголов, зато есть большое число времен. В математике же таких категорий изменений объектов и суждений нет. Например, операция пересечения множеств ($\cap$) не может со временем состариться и перестать работать так, как мы ее определили. Или теорема Пифагора не может устареть в том смысле, что вчера она была верна, а завтра перестанет быть верной. Есть, конечно, изменения символики с течением времени (как, например, устаревшее обозначение импликации $\supset$), но это скорее эволюция языка, чем временные формы его единиц.

Однако же отсутствие времен и падежей — не повод облегченно вздыхать, поскольку в математике имеются свои собственные способы изменения имен и операций.

Чаще всего это связано с тем, что мы экономим на количестве используемых символов, чтобы текст не выглядел громоздким, и поэтому многие символы определяем в ходе изложения материала. Например, знак $\cong$ часто используется для обозначения изоморфизма, но какого конкретно — определяется в тексте. Символ $\omega$ может обозначать как первый бесконечный ординал, так и число Эйзенштейна, либо использоваться как обозначение дифференциальной формы и т.п. Все такие определения обозначений могут зависеть как от области математики, в которой мы работаем, так и от конкретной статьи или книги. Ну а такие ходовые буквы как $a, b, c, x, y, z$ переопределяются в ходе повествования регулярно. То же самое можно сказать и о таких обозначениях операторов, как штрих производной, «крышка», возведение в степень и т.д., смысл которых варьируется от книги к книге, от одной области математики к другой. И единых правил (вроде таблицы спряжений) для этих изменений нет.

В этом заключается абсолютная свобода математики, и часто это же служит препятствием для нематематиков к пониманию математических текстов. С другой стороны, любая статья или книга по математике не состоит из одного лишь формального текста, обычно не менее половины ее объема составляют лексемы разговорного языка, часть

[7] Точнее, в формальной логике мы используем правило контрапозиции: $((\mathscr{A} \to \mathscr{B}) \wedge \neg\mathscr{B}) \to \neg\mathscr{A}$.

из которых являются математическими терминами, а подавляющее большинство — обычными речевыми конструкциями разговорного языка, призванными пояснить то, что написано в формальной части. Это позволяет воспринимать чисто формальный материал через неформальные образы и понятия.

## A1.8. Вопросы для самоконтроля

**Q1** Что такое «принцип матрешки»? [стр. 20]

**Q2** Перечислите как минимум три признака естественных языков, которыми обладает математический язык (𝔐𝔞𝔱𝔥). [стр. 18]

**Q3** В чем заключается основное отличие математического языка от естественных языков? [стр. 18]

**Q4** Что такое графемы и жесткие графемы в математическом языке? Приведите примеры. [19]

**Q5** Объясните на примере формулы Кардано (A1.1), как используется «принцип матрешки» для упрощения сложных выражений.

**Q6** Что такое дерево разбора и какую роль оно играет в понимании структуры математических формул? [стр. 23]

**Q7** В чем разница между синтаксисом и семантикой математического языка? [стр. 25]

**Q8** Что такое предикаты и термы в математическом языке? Приведите примеры из текста. [стр. 26]

**Q9** Что такое лексема-свертка? [стр. 32]

## A1.9. Упражнения

**Ex1.** Постройте дерево разбора для формулы корней квадратного уравнения:

$$x = \frac{-b + \sqrt{b^2 - 4ac}}{2a}$$

Укажите иерархию используемых шаблонов (дробь, сложение, вычитание, квадратный корень, возведение в степень, умножение).

**Ex2.** В математике скобки часто опускаются на основе приоритета операций. Восстановите все опущенные скобки в следующих выражениях, чтобы сделать структуру однозначной:

1. $a \cdot b + c \cdot d$;
2. $x^2 + 2xy + y^2$;
3. $a/b/c$ (предполагая стандартную левоассоциативность);
4. $e^{x^2+y}$.

**Ex3.** Нарисуйте (или опишите) дерево разбора для тождества Эйлера, определив иерархию используемых шаблонов:

$$e^{i\pi} + 1 = 0$$

**Ex4.** Декомпозируйте следующее вложенное выражение по слоям. Что является самым внешним шаблоном, и каковы внутренние компоненты?

$$\sqrt{1 + \sqrt{1 + \sqrt{1 + x}}}$$

**Ex5.** В выражении ниже определите, какие символы выступают как объекты (существительные/переменные/константы), а какие как действия/отношения (глаголы/операторы):

$$\frac{d}{dx}(x^3 + 3x) = 3x^2 + 3$$

**Ex6.** Переведите следующие предложения естественного языка на язык логики предикатов, используя кванторы $(\forall, \exists)$, логические связки $(\wedge, \vee, \to, \neg)$ и подходящие предикаты. *Пример:* «Все французы говорят по-французски». Универсум: Все люди. Предикаты: $Fr(x)$ — «$x$ француз», $Speak(x, \text{French})$ — «$x$ говорит по-французски». Формула: $\forall x(Fr(x) \to Speak(x, \text{French}))$.

1. «Некоторые французы говорят по-английски».
2. «Ни один француз не говорит по-китайски». (Подсказка: перефразируйте как «Для любого человека, если он француз, то он не говорит по-китайски»).
3. «Есть физики, которые любят математику, но не любят квантовую механику».
4. «Любой, кто изучает математическую логику, должен знать теорию множеств».
5. «Существует физик, который предложил теорию, которую понимает каждый математик».
6. «У каждого человека есть ровно один биологический отец». (Подсказка: «существует ровно один» $\exists!$ можно записать как $\exists x(P(x) \wedge \forall y(P(y) \to y = x))$).
7. «Не все то золото, что блестит».
8. «Если физик не знает математики, он не поймет ни Общей теории относительности, ни Квантовой механики».
9. «Не существует теории, которая объясняет абсолютно всё».

**Ex7.** Переведите следующие формальные предложения на естественный русский язык (старайтесь, чтобы это звучало естественно, а не механически):

1. $A \subseteq B \wedge B \subseteq A \to A = B$;
2. $\forall x \in \mathbb{R} : x^2 \geqslant 0$;
3. $n, m \in \mathbb{Z} \wedge n \neq 0 \to \exists q, r : (m = nq + r \wedge 0 \leqslant r < |n|)$.

**Ex8.** Переведите следующие утверждения на язык $\mathfrak{Math}$:

1. Квадрат суммы $a$ и $b$ равен сумме их квадратов плюс удвоенное произведение.

2. Произведение любого числа на ноль равно нулю.
3. Для каждого положительного числа $\varepsilon$ существует положительное число $\delta$.

**Ex9.** Определите, какие из следующих строк являются синтаксически корректными математическими выражениями, а какие — «абракадаброй». Объясните почему.

1. $5 + (3 \cdot 2)$;
2. $5 + \cdot (3\ 2)$;
3. $\sin(x) = \cos$;
4. $\int_a^b f(x)dx$.

**Ex10.** В следующих выражениях определите *связанную* переменную (итератор) и *свободные* переменные (параметры):

1. $\sum_{k=1}^{n} k^3$;
2. $\lim_{x \to a}(x^2 - 3)$;
3. $\bigcup_{i \in I} A_i$.

**Ex11.** Рассмотрим выражение $\sum_{i=1}^{n}(i + \sum_{j=1}^{i} j)$. Почему запись $\sum_{i=1}^{n}(i + \sum_{i=1}^{i} i)$ была бы сбивающей с толку или некорректной?

**Ex12.** Выполните синтаксическую подстановку $[x/(a+b)]$ (замените $x$ на лексему $a+b$) в следующих выражениях. Будьте внимательны со скобками!

1. $3x$;
2. $x^2$;
3. $\sin(x)$.

**Ex13.** В формуле площади круга $S = \pi r^2$:

1. Какие символы являются константами?
2. Какие символы являются переменными?

**Ex14.** Восстановите скобки в выражении $2^{3^4}$ согласно стандартному математическому соглашению для степеней (сверху вниз / правоассоциативность). Вычислите значения $(2^3)^2$ и $2^{(3^2)}$, чтобы продемонстрировать разницу при расстановке скобок.

**Ex15.** Посмотрите на выражение $f^{-1}(x)$. В зависимости от контекста, синтаксически оно может означать две совершенно разные вещи. Что это за вещи? (Подсказка: обращение функции vs возведение в степень.)

**Ex16.** Классифицируйте следующие операторы как унарные (1 аргумент) или бинарные (2 аргумента):

1. $-$ в выражении $-5$;
2. $-$ в выражении $a - b$;
3. $!$ в выражении $n!$;
4. $\cup$ в выражении $A \cup B$.

# У чертога логики

> *Но тебе придется примириться с этим, — возразил Воланд, и усмешка искривила его рот, — не успел ты появиться на крыше, как уже сразу отвесил нелепость, и я тебе скажу, в чем она, — в твоих интонациях. Ты произнес свои слова так, как будто ты не признаешь теней, а также и зла. Не будешь ли ты так добр подумать над вопросом: что бы делало твое добро, если бы не существовало зла, и как бы выглядела земля, если бы с нее исчезли тени? Ведь тени получаются от предметов и людей. Вот тень от моей шпаги. Но бывают тени от деревьев и от живых существ. Не хочешь ли ты ободрать весь земной шар, снеся с него прочь все деревья и все живое из-за твоей фантазии наслаждаться голым светом?*
>
> — М. Булгаков, «Мастер и Маргарита»

Приведенная цитата из классика показывает нам важность дифференциации чего бы то ни было хотя бы на два класса. При этом мы не заостряем внимание на том, как именно называются эти классы, имеют ли эти названия какой-то смысловой подтекст или являются абракадаброй. Важно то, что если совокупность всего того, что мы в принципе могли бы описывать языком Math (или любым другим языком), нельзя было бы разделить на категории, то мы принципиально не смогли бы различать предметы, события, явления, а также видеть какие-либо отношения между ними. Вся вселенная у нас схлопнулась бы в одну точку.

По сути **логика** как таковая представляет собой *комплекс правил и методов, позволяющих некоторым регулярным способом отличать «свет» от «тьмы», обнаруживать сходства и различия, отделять существенное от несущественного, находить связи и структуры* в том объеме знаний, к которому мы применяем язык Math как описательное средство. В этом и следующем разделах мы поговорим о логике в общем виде, понимая ее как некоторое неотъемлемое свойство нашего разума, позволяющее выстраивать правильные суждения.

Первый же вопрос, который может возникнуть у читателя: зачем производить какое-то деление на классы, если они и так уже есть? Действительно, ведь при определении языка Math мы научились строить синтаксически правильные лексемы. Более того, мы предъявили вполне конкретный алгоритм, как это делать, отправляясь от некоторых предопределенных подстановочных шаблонов и алфавитных символов. Наконец, по любому тексту мы даже можем за конечное время распознать, является ли он правильно построенной лексемой или нет. Давайте тогда считать лексемы «истинными» текстами, а все остальные комбинации символов — «ложными» текстами.

Такой догматический подход таит в себе ряд проблем. Во-первых, мы тем самым построили не более чем *логику лексем*. То есть мы с помощью этой логики умеем опре-

делять правильные лексемы, и на этом ее способности заканчиваются. Такую логику можно назвать *синтаксической*.[1]

Во-вторых, если мы хотим применять язык Math к каким-то внешним сущностям (будь то математические абстракции или физические явления), то мы должны уметь описывать свойства этих сущностей в позитивном ключе, т.е. описывать их явным образом, а не с помощью отрицания или исключения других свойств. Кроме того, различия между лексемами-описаниями должны соответствовать действительным различиям описываемых сущностей. Если же мы не научимся различать правильно построенные лексемы, то не научимся анализировать те сущности, которые ими описываются — для нас весь мир распадется на бытие и небытие, поскольку неправильными текстами мы не сможем описывать конкретные элементы бытия (просто будет непонятно, как соотнести одно с другим).

В-третьих, знание о том, что является сущим, а что нет, не всегда дано нам в ощущениях, следовательно, мы должны иметь какую-то строгую схему, которая позволила бы последовательностью *правильных* манипуляций показать, обозначает ли данная лексема какую-то сущность из предметной области или же она, будучи корректной с точки зрения синтаксиса, некорректна с точки зрения семантики, т.е. не описывает реально существующие предметы.

Грубо говоря, правильные с точки зрения синтаксиса лексемы — это корректно заданные вопросы с вариантами ответа «Да» или «Нет». Сам же ответ определяется семантикой. Но именно для того, чтобы уметь вычислить разницу между «Да» и «Нет», тексты вопросов сами по себе должны быть грамотно (синтаксически верно) построены.

Поэтому корректное, работоспособное и удобное с практической точки зрения описание какой-либо предметной области разумно производить внутри уже определенного некоторым регулярным образом фрагмента нашего универсального языка Math, отбросив все синтаксически некорректные записи.

Определив такой фрагмент в каждом конкретном случае, мы получаем возможность записывать на нем алгоритмически строгим способом а) описания объектов из данной предметной области и б) предикаты, описывающие взаимное отношение этих объектов. По большому счету именно формализованное представление предикатов и является основной целью формализации предметной области.

Почему так? Дело в том, что любой предикат, описывающий отношение между объектами, в некотором смысле упрощает и обобщает ситуацию, переводя предметное знание в истинностную категорию. С одной стороны, этого вполне достаточно, поскольку с практической точки зрения нас всегда интересует фактология предметной области, а именно, ответ на вопрос о том, является ли в ней фактом то или иное соотношение между объектами, поскольку это позволяет предсказывать реакцию среды на наши действия в ней. С другой стороны, переход к предикатам переводит исследование в философскую истинностную категорию самого общего характера. Действительно, подстроив нужным образом формализм под описание объектов и предикатов предметной

[1] При желании синтаксическую логику можно развить, выделяя в имеющихся классах какие-то новые подклассы, определения которых будут завязаны на их синтаксис. Например, можно воспользоваться тем, что всякая правильно построенная лексема представляется в виде дерева разбора, а уж деревья можно классифицировать очень разнообразными способами, отталкиваясь от их высоты и характеристик ветвления. Однако и такая *разветвленная* логика будет не более чем профанацией с точки зрения логики вообще, ибо ничего, кроме синтаксического анализа текста, она не предоставит. Такие логики удобны в глубоко частных случаях, но не годятся как общий подход с целью выявления той самой семантики, о которой идет речь в приведенной цитате.

области, мы сводим ее изучение к некоторым универсальным для всего человечества инструментам — логическим выводам.

В свою очередь, применение абстрактного логического аппарата подразумевает оперирование такими понятиями, как Истина и Ложь, которые в контексте конкретной предметной области (семантики) определяются, соответственно, как выполнение или невыполнение каких-либо предикатов. Конкретнее, если какие-то объекты связаны некоторым предикатом (т.е. совместно соответствуют ему своими свойствами), то такой предикат считается истинным для данных объектов, а в противном случае — ложным.

Это конкретное определение пары Истина/Ложь для целей формализации предметной области и ложится в основу определения логики предметной области и соответствующей формальной системы.

Более точно скажем, что под **логикой** некоторой предметной области мы будем понимать *регуляризованную (формальную) схему определения относительной истинности формул в языке этой предметной области*. Относительность истины в данном случае означает, что истинность формул устанавливается не сама по себе, а при условии истинности других формул.

Поэтому стоит особенно отметить, что логика не являет собой установление истины в последней инстанции, но предъявляет некоторый строгий формализованный механизм получения новых знаний (истинных предикатов) из уже имеющихся. Ответственность за выбор стартовых истинных знаний (фактов) возлагается на исследователя (человека).

Таким образом задача формализации предметной области в языке $\mathfrak{Math}$ состоит из следующих этапов (табл. A2.1):

Таблица A2.1. Схема формализации

| | |
|---|---|
| **(1)** | построение фрагмента языка $\mathfrak{Math}$ с помощью описания начальных графем и правил их комбинирования; |
| **(2)** | определение в этом фрагменте лексем, соответствующих формулам и термам; |
| **(3)** | определение правил, по которым можно устанавливать истинность одних формул, предполагая истинность других (правила вывода); |
| **(4)** | задание стартовых истин (аксиом). |

Отметим, что если построение фрагмента языка (пункты 1 и 2) обычно заточено строго под конкретную предметную область, то определение правил вывода (пункт 3) имеет более универсальный характер и относится к области собственно логики.

Особым требованием к формализации является **корректность логики** относительно описываемой семантики (предметной области). Корректность означает, что из формул, соответствующих фактическим истинам, т.е. проверенным фактам, по правилам логики могут быть получены только (хоть и необязательно все) фактические истины, которые впоследствии могут быть верифицированы внешними средствами.

Заметим, что вышеупомянутая логика лексем является, с одной стороны, частным случаем логики в описанном нами смысле, если под предметной областью понимать именно лексемы языка $\mathfrak{Math}$, а с другой стороны, она же является тем базовыми пространством, внутри которого мы будем строить все остальные логики произвольных предметных областей. Аналогичная ситуация встречается и в самой математике, когда

синтаксически очень бедная формальная теория множеств способна описать всю математику.

## A2.1. Понятие

Вопрос о строгом определении понятий волновал философов и математиков с древности. Платон в своих диалогах часто ищет суть понятий через метод майевтики, а Аристотель в «Органоне» заложил основы классификации понятий и методов определения через род и видовое отличие. Стремление к точности определений — это вечный спутник развития математической мысли.

Строго говоря, «понятие» — это неопределимое в привычном смысле понятие (да-да, «понятие» — это тоже понятие!).

Всякое **понятие** предполагает наличие **объема понятия** и его **определения** (в книгах по логике вместо «определение» говорят «содержание», см. [16]). Кроме того, к понятию прикрепляется словесный **термин** (слово или словосочетание), чтобы это понятие в дальнейшем было удобно использовать. Часто к понятию еще прикрепляется **обозначение**, т.е. специальный символ (или группа символов), обозначающее данное понятие или его индивидуальных представителей.

Определение каждого конкретного понятия может быть либо *прямым*, когда мы, отправляясь от уже имеющегося терминологического аппарата, вводим новое понятие по формуле «А — это то-то и то-то», либо *косвенным*, когда два и более понятий вводятся одновременно через контекст их взаимосвязей (или, иначе, через перечисление свойств их взаимосвязей, выраженных предикатами).

Но в любом случае всякое понятие вводится предикативным способом, поскольку его определение записывается с помощью конечной или бесконечной серии формул в выбранном языке. Стоит особо отметить, что бесконечные определения в подавляющем большинстве случаев на самом деле представляют собой конечную схему, конкретные реализации которой жестко регламентированы.

Пример прямого определения понятия: «простое число — это число, имеющее ровно два делителя».

Пример косвенного определения понятия: *аксиомы арифметики Пеано*, определяющие логическую взаимосвязь понятий «число», «сложение», «умножение», «равенство», «последователь». Здесь сразу несколько понятий вводится одновременно при помощи конечного списка аксиом и схемы индукции.[2]

Как только у нас есть определение понятия, немедленно возникает его объем. По сути объем понятия — это все, что подпадает под его определение в рамках выбранной семантики. В случае понятия простого числа — это множество всех простых чисел. В случае понятия нейтронной звезды — множество всех нейтронных звезд во всей вселенной, и т.д. Обычно предполагается, что объем понятия не пуст в любой семантике, т.е. понятие не противоречиво. Хотя для полноты картины следует ввести в обращение и противоречивое понятие, объемом которого является пустое множество.

В противоположность противоречивому понятию с пустым объемом существует понятие универсума («нулевое» понятие), которое включает в себя все объекты рассматриваемой в данный момент семантики (все живые существа, все звезды, все натуральные числа, все геометрические фигуры и т.д.). Важно понимать, что само по себе по-

[2] Речь идет об арифметике первого порядка, т.к. она будет изучаться здесь в дальнейшем.

нятие универсума — универсальное, хотя его наполнение прямо зависит от выбранной семантики.

Заметим, что любое определение должно быть каким-то способом записано на каком-то языке. Поскольку мы уже прошли некоторый путь формализации и определили (хотя и в самых общих чертах) язык, которым мы пользуемся, у нас появляется возможность дать более узкое и точное определение понятию под наши конкретные нужды.

Поэтому в рамках данной книги мы определим лишь математическое понятие. Определение, которое последует ниже, имеет характер косвенного определения и напоминает аксиомы или постулаты, поскольку вводит в обращение сразу несколько терминов путем описания их взаимоотношений.

**Математическое понятие** состоит из трех обязательных компонентов: объем понятия, определение понятия, термин понятия, и одной опциональной компоненты: обозначение понятия.

**Объем понятия** зависит от выбранной семантики языка и состоит из сущностей, принадлежащих к данной семантике, которые объединены общей идеей и выделяются среди прочих сущностей заданным списком свойств, выраженных формулами.[3]

**Определение понятия** — формальная синтаксическая конструкция, записанная с помощью формул выбранного фрагмента языка $\mathfrak{Math}$, не зависящая(!) от выбранной семантики и выражающая все те свойства, одновременное обладание которыми выделяет сущности, принадлежащие объему данного понятия, и только ему. Таким образом определение математического понятия всегда предикативно.

**Термин понятия** — это слово или набор слов разговорного языка в сочетании с лексемами языка $\mathfrak{Math}$, закрепленный за данным понятием.

**Обозначение понятия** — это лексема языка $\mathfrak{Math}$, служащая для обозначения конкретных представителей объема понятия или же для обозначения самого объема понятия.

Следует отметить, что данное определение, несмотря на свою современную форму, имеет глубокие исторические корни. Деление понятия на *объем* и *содержание* (здесь — *определение*) является центральным еще для аристотелевской логики. Однако именно в XX веке, в работах сторонников *формализма*, таких как Давид Гильберт, и особенно в трудах группы математиков под псевдонимом Николя Бурбаки, идея отделения формальной *структуры* от ее конкретных реализаций была положена в основу всей архитектуры современной математики. Наш подход, где *определение понятия* есть чисто синтаксическая конструкция, не зависящая от семантики, а *объем понятия* — совокупность ее моделей в той или иной семантике, является прямым следствием этой структуралистской точки зрения.

Покажем работу данного определения на примерах. Начнем с простого числа. Определение математического понятия требует от нас дать, во-первых, идею простого числа, а во-вторых, дать его формальное определение и термин. Стоит сразу оговориться, что мы сейчас находимся в мире натуральных чисел, т.е. арифметики, и строим идею определения на вполне конкретной семантике.

Мы знаем, что некоторые натуральные числа можно раскладывать на множители, тем самым представляя более сложное число через произведение более простых (меньших). Идея состоит в том, чтобы всякое число уметь раскладывать через какие-то эле-

[3] Имеется в виду, что каждая сущность из объема понятия обладает обязательно всеми заданными свойствами, а всякая сущность вне объема понятия не обладает как минимум одним из заданных свойств.

ментарные числа, которые уже нельзя разложить на меньшие множители. Таким образом, общей идеей для простых чисел является невозможность их разложить на меньшие множители так, чтобы все полученные множители были меньше исходного числа.[4]

Заметим, что идея несколько избыточна, поскольку к любому разложению можно добавить множителем единицу, и ничего не изменится. Поэтому мы должны сразу договориться, что единицу мы не относим к простым числам, т.к. ее использование в разложении на множители бессмысленно. То же самое можно сообщить и про ноль, т.к. если он есть в разложении, то и само раскладываемое число тоже есть ноль, а в разложении других чисел он участвовать не может.

Следовательно, простым числом может быть только такое, которое не раскладывается *существенным* образом на меньшие множители и отлично от нуля и единицы.

Формальное же определение простого числа в языке арифметики таково: простое число имеет ровно два делителя.

Почему формальное определение отличается от данной выше идеи простого числа? Дело в том, что формальное определение задается в формализме, который ничего не знает ни об идее разложимости, ни о том, что значит «меньше». Однако в этом формализме (который мы будем подробно изучать позже) достаточно легко определить понятие делимости, поскольку операция умножения определяется вместе с понятием натурального числа, т.е. она имманентно встроена в этот формализм.

Далее остается лишь понять, как через понятие делимости выразить нашу идею простого числа. Мы хотим, чтобы оно не раскладывалось на меньшие множители, следовательно, оно не должно иметь меньших, чем оно само, делителей, т.е. просто-напросто, оно не должно иметь делителей, отличных от него самого. Однако такой делитель всегда есть — это единица. Но дело в том, что если мы рассматриваем единицу в качестве делителя, то в паре с ней всегда идет делитель, равный самому этому числу, а значит, с использованием единицы мы не добиваемся того, чтобы разложение было на строго меньшие делители. Поэтому корректируем определение, допуская лишь тривиальные делители: единицу и само число.

Попутно заметим, что мы тем самым уже исключили ноль из списка простых чисел, поскольку у него больше двух делителей.

Однако и это не все. Под такое определение подпадает сама единица, а мы хотим ее исключить из списка простых чисел. Но единица обладает уникальным свойством — список ее делителей состоит ровно из одного числа — единицы. В то время как у всех прочих чисел (даже у нуля) делителей не меньше двух.

Тогда мы делаем последний шаг и добавляем в определение слово «ровно», и получается, что простое число — это число, у которого есть ровно два делителя.

Согласно определению мы еще должны дать новому понятию собственный термин, но мы его ввели сразу же, когда формализовали определение, назвав данное понятие простым числом.

Интересно отметить, что при одной и той же идее у нас могут получаться разные формальные определения, а значит, и разные математические понятия. Так, идея элементарного неразложимого кирпичика в целых числах даст определение простого числа как такого, у которого есть ровно 4 делителя, поскольку следует учитывать наличие знака целого числа. Та же идея в гауссовых целых числах уже дает формальное

[4] В высшей алгебре этой идее соответствует понятие *неприводимого элемента* кольца, а *простыми* называются такие элементы, которые, будучи делителями произведения, обязательно делят один из множителей. Однако в области главных идеалов (в частности, в $\mathbb{Z}$) эти понятия совпадают, так что мы пренебрегаем этим различием на начальном уровне.

определение простого числа, как обладающего ровно 8-ю делителями, а в случае чисел Эйзенштейна — ровно 12-ю делителями.

Можно пойти дальше и вспомнить про теорию групп, где та же самая идея неразложимости приводит нас к понятию простой группы, т.е. такой группы, которая не имеет нетривиальных нормальных подгрупп.

При этом нужно отметить, что все эти определения понятий остаются формальными, а это значит, что они будут работать независимо от той семантики, которая может быть описана данным формализмом. Иначе говоря, если мы под группами сначала понимаем какие-то симметрии в кристаллографии, а затем — какие-то преобразования в атомной физике, то простая группа в обоих случаях будет обладать свойством быть неразложимой в смысле факторизации групп.

Таким образом, мы видим, что, с одной стороны, данная конкретная семантика может породить как идею понятия, так и его формальное определение, а с другой стороны, и само формальное определение понятия может выходить за рамки исходной семантики, и тем более идея этого понятия может широко распространяться на другие случаи.

Еще один пример понятия — натуральное число, а точнее, система натуральных чисел.

В основе этого понятия лежит идея неких абстрактных величин, которыми можно, с одной стороны, что-то пересчитывать и упорядочивать, с другой стороны, производить над ними обычные арифметические действия, чтобы подсчитывать количество.

В принципе, этим уже все сказано, но можно придумать более точную идею, если обратиться к общей алгебре. А именно, от натуральных чисел мы хотим, чтобы эта система была минимальным упорядоченным дискретным коммутативным полукольцом с единицей, в котором можно использовать индукцию. Такая идея уже практически превращается в формальное определение, поскольку если расписать все использованные термины аксиоматически через их определения, мы в общем-то и получим арифметику Пеано. Подробно этими вопросами мы займемся в главе B2.1.

Выше мы говорили о том, что можно определить понятие универсум, как такое, которое включает всю предметную область целиком без исключений. В математике понятие универсум имеет более конкретное значение. Под математическим универсумом следует понимать все изучаемые объекты в данной предметной области, т.е. те сущности, над которыми производятся какие-то формализованные в данной формальной системе операции.

Формальное определение математического универсума можно дать только в связи с определением переменных. Идея **математического универсума** состоит в том, что он представляет собой область действия всех переменных рассматриваемого нами в данный момент формального фрагмента языка $\mathfrak{Math}$. А идея переменной состоит в том, что все переменные в совокупности являются обезличенными обозначениями элементов универсума.

Определением математического универсума является пустая синтаксическая конструкция, принадлежащая языку $\mathfrak{Math}$ (пустая строка). Таким образом, определение математического универсума подпадает под требования A2.1 к определению понятия.

Попутно мы ввели косвенное определение переменных, однако у переменных есть общая идея (обозначение элементов универсума) и формальное определение, поскольку обозначения переменных в языке $\mathfrak{Math}$ всегда строго регламентированы. Как правило это буквы или буквы с акцентами и/или индексами. Поэтому понятие переменной тоже можно считать математическим в силу определения A2.1.

Переменные принято разделять на связанные и свободные с одной и той же областью действия. Такое разделение является чисто синтаксическим, однако у него также есть все признаки определения A2.1, поскольку идеей связанных переменных является их предназначение — они могут использоваться только в лексемах-свертках, а идея свободных переменных состоит в обозначении свободных параметров лексемы. Формально же связанные переменные определяются своим положением в лексеме после специального символа свертки (например, квантора), в то время как свободные переменные в таком месте лексемы находиться не могут.

Если мы используем переменные типов (например, переменные для множеств и классов), то за каждым типом переменных закрепляется какая-то часть универсума (иногда она может совпадать с универсумом) и какая-то часть списка переменных. Вводя переменные какого-либо типа, мы неявным образом определяем, во-первых, объем этого типа, во-вторых закрепляем за его элементами общее обозначение в виде собственно переменных данного типа, в-третьих, даем строгое формальное описание переменных данного типа (предъявляем список).

В этой книге мы практически не коснемся типизированных переменных (кроме разделения на логический и предметный типы), поэтому без потери общности можно считать, что все переменные в рассматриваемых формальных системах делятся только на два класса: связанные и свободные.

Как и всякое верхнеуровневое определение, наше определение математического понятия оперирует словами, которые ранее не определены и предполагаются понятными из контекста или некоторых общих представлений. К сожалению, создать полностью детерминированную и отвлеченную от всего сущего логику невозможно, поскольку, пытаясь произнести хоть слово, мы неминуемо оказываемся в определенном семантическом контексте разговорного языка и вынужденно апеллируем к нему как той базе понятий и терминов, которая нам предопределена, однако наша задача состоит в том, чтобы эта предопределенная база понятий была как можно меньше и как можно проще.

Стоит отметить, что коль скоро мы ввели определение математического понятия, то хотелось бы понять, является ли «математическое понятие» математическим понятием. То есть, обладает ли определение A2.1 теми признаками, которые в нем указаны. Или, иначе говоря, принадлежит ли понятие «математическое понятие» своему собственному объему.

Оказывается, нет, поскольку само определение математического понятия задано в разговорной синтаксической и семантической конструкции, а не в рамках того аппарата лексем языка $\mathfrak{Math}$, который должен использоваться при определении любого математического понятия. Если бы не это ограничение, то всем остальным признакам математическое понятие удовлетворяет — у него есть некоторая общая идея (выраженная определением), определение и термин.

Здесь немедленно вспоминаются такие знаменитые логические парадоксы, как парадокс Рассела и парадокс брадобрея.[5]

Но на самом деле определение математического понятия просто-напросто принадлежит к метаязыку, а его конкретные реализации, т.е. собственно математические по-

[5] Парадокс брадобрея: в некоторой деревне есть только один брадобрей, который бреет всех, кто не бреется сам. Вопрос: бреется ли брадобрей? Очевидно, что если он бреется сам, то его не бреет брадобрей, т.е. он сам. Если же он сам не бреется, то его бреет брадобрей, т.е. он сам. Получается, что брадобрей — не из этой деревни, т.е. он выпадает из того семантического универсума, к которому его отнесли формулировкой задачи.

нятия, принадлежат к той части языка $\mathfrak{Math}$, который описывает конкретную область математического знания.

## A2.2. «Истина» и «ложь»

Как уже отмечалось выше, при формализации описания предметной области в языке $\mathfrak{Math}$ мы пользуемся ограниченным понятием истинности, понимая под ним взаимное соответствие свойств объектов некоторому предикату, написанному в данном языке.[6]

При этом нужно понимать, что сама проверка соответствия свойств предикату представляет собой некоторый процесс, сводящий результат проверки к некоторым стартовым истинам, заданным списком аксиом. Тем самым истина для нас является понятием относительным.

Пусть имеется некоторое понятие $\mathfrak{C}$, объем которого мы обозначим за $V$, а его формальное определение — за $\mathscr{D}(a)$, где $a$ — свободная переменная. Принадлежность некоторого объекта $v$ (это либо предметная переменная, либо более сложный терм) к объему данного понятия можно записать в универсальном языке $\mathfrak{Math}$ двумя способами:

$$v \in V \quad \text{или} \quad \mathscr{D}[a/v].$$

Формула $v \in V$ фактически означает, что объект $v$ принадлежит объему $V$, а формула $\mathscr{D}[a/v]$ или, короче, $\mathscr{D}(v)$ означает, что объект $v$ удовлетворяет формальному определению понятия $\mathfrak{C}$.[7]

Таким образом, истинность соответствия объекта $v$ понятию $\mathfrak{C}$ выражается истинностью любой из формул: $v \in V$ и $\mathscr{D}[a/v]$. Если же объект $v$ на самом деле не соответствует понятию $\mathfrak{C}$, то обе эти формулы одновременно являются ложными.

Заметим, что истинность тех или иных формул, как уже отмечалось, мы хотим устанавливать некоторым регулярным способом по правилам вывода, сводя ее к истинности аксиом. При этом мы требуем, чтобы полученные по правилам вывода истины были корректны с точки зрения семантики в том случае, если аксиомы соответствуют данной семантике. Это означает зависимость истинности формул не только от аксиом, но и от выбранной семантики.

Так, например, свойство числа быть отрицательным в универсуме целых чисел может быть истинным, в то время как в универсуме натуральных чисел оно всегда ложно, а в универсуме комплексных чисел это свойство можно выразить по-разному, придав разный объем этому понятию. Это неудивительно, поскольку у перечисленных семантик различные наборы аксиом, и в одном случае свойство быть отрицательным может быть выведено из аксиом, а в других — нет.

Тем не менее, некоторые формальные выражения таковы, что их истинность не зависит от семантики. Например, универсум определяется пустым формальным определением. Если объем универсума обозначить за $U$, то формула $v \in U$ будет всегда истинной независимо от того, что мы понимаем под универсумом, если только этот универсум не пуст. Соответствующая универсуму формула, которая должна быть пустой

[6] Этим определением истинностной категории мы в упрощенном виде выражаем классическую *корреспондентскую концепцию* (т.е. с проверкой на соответствие каким-то критериям) истины, восходящую к Аристотелю и Гегелю.

[7] Напомним, что $[a/v]$ обозначает тотальную замену переменной $a$ в формуле $\mathscr{D}$ на терм $v$.

строкой по нашему определению, также должна быть **тождественной истиной**, поэтому такую формулу обозначают значком $\top$ (от слова True), чтобы отличать от пустых строк, использующихся в другом контексте (например, как нейтральный элемент операции конкатенации строк).

Формула $\top$ не имеет ни свободных, ни замкнутых переменных, поскольку она ни от чего не зависит.

Противоположная ситуация — это противоречивое понятие, объемом которого по определению является пустое множество $\varnothing$, и формула $\nu \in \varnothing$ всегда ложна. Соответствующая ему формула определения обозначается символом $\bot$ и называется **тождественной ложью**.

Формула $\bot$ не имеет ни свободных, ни замкнутых переменных, поскольку она ни от чего не зависит.

Как видим, существует тесная связь между выражениями о множествах и формальными истинностными выражениями, и это не случайно. Дело в том, что язык теории множеств является семантическим воплощением языка логики. Покажем это в ходе определения символов логических связок и теоретико-множественных операций и отношений.

## A2.3. Логика и множества

В контексте изучения логики в классической истинностной категории договоримся использовать каллиграфические буквы $\mathscr{A}, \mathscr{B}, \mathscr{C}$ и т.д. для обозначения переменных, пробегающих высказывания и предикаты, т.е. закрепим за ними *логический тип*. Такие переменные называются *пропозициональными*.[8] Под *пропозициональной формулой* мы будем понимать любую лексему, которая описывает преобразование объектов логического типа в объект логического типа, т.е. действует внутри истинностной категории.

Более точно, среди всех лексем языка $\mathfrak{Math}$ мы хотим выделить определенный класс лексем, построенных по принципу матрешки и отвечающих нашим представлениям о структуре логического выражения. Для этого мы определим базовый ограниченный набор символов с одним или двумя подстановочными местами, после чего объявим, что лексемами логического типа являются те и только те лексемы, которые получаются комбинированием этих базовых символов и пропозициональных переменных по принципу матрешки.

Базовыми логическими символами являются:

$\to$ **Импликация**: двухместный логический оператор $\mathscr{A} \to \mathscr{B}$, означающий, что «из $\mathscr{A}$ следует $\mathscr{B}$» или «если $\mathscr{A}$, то $\mathscr{B}$».[9]

$\neg$ **Отрицание**: одноместный логический оператор $\neg\mathscr{A}$, означающий «не $\mathscr{A}$» или «отрицание $\mathscr{A}$».

$\wedge$ **Конъюнкция**: двухместный логический оператор $\mathscr{A} \wedge \mathscr{B}$, означающий «$\mathscr{A}$ и $\mathscr{B}$».

$\vee$ **Дизъюнкция**: двухместный логический оператор $\mathscr{A} \vee \mathscr{B}$, означающий «$\mathscr{A}$ или $\mathscr{B}$».

[8] От лат. *propositio* — суждение, высказывание.

[9] В некоторых книгах встречается эквивалентное обозначение $\mathscr{A} \supset \mathscr{B}$, но мы не будем его использовать, чтобы избежать путаницы с теоретико-множественным вложением.

↔ **Эквиваленция**: двухместный логический оператор, означающий «$\mathscr{A}$ равносильно $\mathscr{B}$», «$\mathscr{A}$ тогда и только тогда, когда $\mathscr{B}$».

Значки $\to, \neg, \wedge, \vee, \leftrightarrow$ называются **логическими связками**. Таким образом, пропозициональная формула — это лексема, построенная из логических связок и пропозициональных переменных (скобки подразумеваются как вспомогательные символы-разделители)

Понятие пропозициональной формулы в приведенном виде уже можно считать математическим понятием в смысле определения A2.1. Действительно, мы знаем объем этого понятия — все лексемы, построенные из логических связок и пропозициональных переменных по принципу матрешки. Мы дали четкое алгоритмизированное определение этим лексемам, так что по любой строке языка $\mathfrak{Math}$ мы можем распознать, является ли она пропозициональной формулой или нет. Наконец, у нас есть термин — «пропозициональная формула».

Как и в случае произвольных лексем, построенных по правилу матрешки, можно заметить, что пропозициональные формулы можно строить не только по определению, но и, например, заменяя пропозициональные переменные пропозициональными формулами или другими пропозициональными переменными.

Пример пропозициональной формулы:

$$(\mathscr{A} \to (\mathscr{B} \to \mathscr{C})) \to ((\mathscr{A} \wedge \mathscr{B}) \to \mathscr{C}),$$

В случае, когда выражение настолько сложное, что не хватает букв латинского алфавита для обозначения его переменных, применяются различные «добавки» к обозначениям переменных, например, цифровые индексы ($\mathscr{A}_1$, $\mathscr{A}_{11}$ и т.д.).

Хотя выше мы отметили, что понятие пропозициональной формулы уже является математическим, надо понимать, что пока это чисто синтаксическое понятие, не наполненное никакой семантикой, несмотря на то, что при определении логических связок мы давали им словесное объяснение. Чтобы сделать это понятие по-настоящему ценным, нужно определить «правила игры» с этими формулами. Обычно это делается следующим образом: часть пропозициональных формул объявляется заведомо истинными, а для проверки остальных на истинность используются определенные правила, называемые правилами вывода. Таким образом, явно или неявно, но мы должны уметь давать истинностную оценку всем пропозициональным формулам.

Формально базовые истинные пропозициональные формулы (аксиомы) и правила вывода определяются в логике нулевого порядка (логике высказываний), где они изучаются в собственном смысле, т.е. как обособленная алгебраическая конструкция. В таком случае математическое понятие «пропозициональная формула» обретает более глубокое определение, позволяющее придать синтаксису определенный истинностный смысл и увязать формулы с понятиями Истина и Ложь, о которых мы говорили выше. Математическая теория, занимающаяся изучением пропозициональной логики (т.е. логики пропозициональных формул и логических связок), называется **исчислением** (или **логикой**) **высказываний**. Подробнее мы рассмотрим его в главе B1.

Тем не менее, истинностное наполнение пропозициональных формул — это только верхушка айсберга. Ведь умение оперировать чистой логикой, рафинированными представлениями о мыслях и суждениях, дает нам лишь самые общие правила для установления истинностных отношений между знаниями из произвольной предметной области. С одной стороны, логика высказываний универсальна, с другой стороны, она слишком абстрактна.

Поэтому для того, чтобы наполнить логику более конкретным смыслом, мы должны понимать, как формируются те самые высказывания и предикаты, которые являются предметной областью для логики и которые обозначаются пропозициональными переменными. Иначе говоря, мы должны научиться записывать на языке Math предикаты, чтобы, подставляя их вместо пропозициональных переменных, получать более сложные логические суждения (формулы) о конкретной предметной области.

Характерным примером предиката у нас была лексема $\mathscr{A}(k, \text{«красный»})$, которая говорила нам о том, что объект $k$ имеет какое-то отношение к слову «красный» (например, у него красный цвет). Как видим, получая на вход объекты предметной области, на выходе предикат выдает истинностное значение, а значит, может быть подставлен вместо пропозициональной переменной в пропозициональную формулу.

Кроме того, с появлением предметных переменных у нас добавляется еще один вид логических операций, а именно — кванторы, которые образуют лексемы-свертки логического типа и нужны для того, чтобы выражать обобщающие суждения (квантор всеобщности), а также контрпримеры к ним (квантор существования). Например, $\forall k\ \mathscr{A}(k, \text{«красный»})$ выражает, что предикат $\mathscr{A}(k, \text{«красный»})$ всегда верен, т.е. любой предмет $k$ соответствует признаку «красный».

Такая сцепка семантики с чистой логикой приводит нас к необходимости рассматривать более сложный синтаксический аппарат: помимо пропозициональных формул мы должны уметь определять предикаты, выражающие те или иные свойства предметов. Лексема, получаемая в результате подстановки предикатов в пропозициональною формулу вместо пропозициональных переменных (снова принцип матрешки) или под кванторы называется **формулой** (логики предикатов).

Для упрощения терминологического аппарата предикаты тоже относят к формулам, так что предикат является частным случаем формулы и называется **атомарной формулой**.

Некоторые предикаты могут быть *выражены* более сложными формулами через другие предикаты, логические связки и кванторы (например, равенство множеств можно выразить через отношение принадлежности).

Если посмотреть на дерево разбора формулы, то оно представляет собой дерево разбора пропозициональной формулы, продолженное деревьями разбора, соответствующими кванторам и предикатам. Иначе говоря, дерево разбора формулы, связанной с какой-то нелогической предметной областью как бы прорастает своими ветвями в эту предметную область.

Однако при описании предметной области дело не ограничивается только предикатами и формулами. Как уже отмечалось, есть еще такое понятие, как **терм**. Это — лексема предметного типа, представляющая собой алгоритм конструирования одних элементов предметной области из других путем комбинирования (в соответствии с принципом матрешки) операторных символов и переменных. Операторные символы — это примерно то же самое, что и логические связки, только они преобразуют предметный тип в предметный. Эти символы гораздо более разнообразны, чем логические, поскольку они напрямую связаны с предметной областью.

Математическая теория, занимающаяся изучением в общем виде (без конкретизации предметной области) свойств формул с предикатами, термами и кванторами, называется **исчислением** (или **логикой**) **предикатов**. Подробнее мы рассмотрим его в главе B1.

Для того, чтобы сразу не утонуть в разнообразии математических формализмов, здесь мы ограничимся рассмотрением одной предметной области, а именно, множеств.

Тем более что множества, по сути, являются универсальной предметной областью, пригодной для описания любых математических и логических конструкций. В этой конкретной предметной области имеется вполне конкретный список операторных символов, которые мы перечислим ниже.

Как и в случае формул, среди термов также есть атомарные термы. Это такие термы, которые не содержат в своей записи операторных символов. На данный момент в качестве атомарных термов мы будем использовать предметные переменные $A, B, C, \ldots, Z, a, b, c, \ldots, z$ (возможно, с индексами), а также специальные символы-константы, закрепленные за конкретными объектами. Как обычно, термы (предметные лексемы) собираются по принципу матрешки, так что вместо переменных можно подставлять только множества и предметные лексемы того же типа (рис. A2.1).

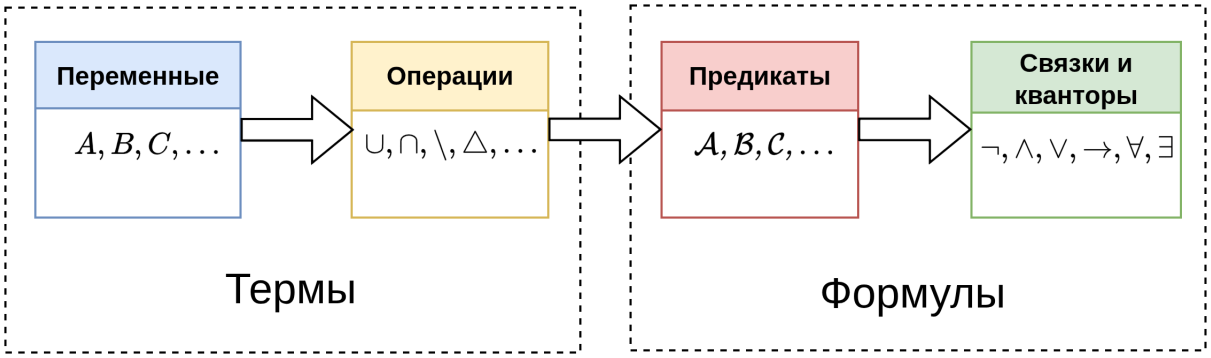



Рис. A2.1. Уровни дерева разбора формулы

Суммируя, заметим, что всякая формула имеет четыре уровня в дереве разбора: уровень пропозициональных формул и кванторов, уровень предикатов, уровень термов и уровень атомарных термов, т.е. предметных переменных.

Наиболее часто применяемые теоретико-множественные операции и предикаты приведены в таблице A2.2.

По поводу последнего предиката отметим, что в теории множеств «все является множеством», поэтому элементы множеств — тоже множества. С точки зрения обычных представлений это кажется абсурдным, но для упрощения нашего рассказа мы предположим, что элементы произвольной природы закодированы некоторым способом с помощью множеств, чтобы не плодить сущности.

Наконец, не забудем про символы-константы:

$\mathfrak{U}$ — весь универсум множеств[10], определяемый свойством-формулой: $A \in \mathfrak{U}$;

$\varnothing$ — пустое множество, которое определяется свойством-формулой: $\neg(A \in \varnothing)$.

Здесь в обоих случаях $A$ — произвольное множество, кроме самого универсума.

Вспоминая наш пример (A1.2) с нейтронными звездами и крокодилами, отметим, что мы уже использовали обозначение $K \cap M$, которое обозначало крокодилов в Москве-реке или нейтронные звезды в зависимости от выбранной семантики.

[10] Забегая вперед, отметим, что универсум всех множеств не может быть множеством в силу известных парадоксов, но на него тоже можно распространить действие указанных операций и предикатов, поэтому пока будем считать его тоже неким множеством специального вида

Таблица А2.2. Операции и предикаты над множествами

| Символ | Описание |
|---|---|
| $\cup$ | *Объединение множеств* $A$ и $B$ есть двухместная операция, которая обозначается $A \cup B$ и представляет собой множество, содержащее как все элементы множества $A$, так и все элементы множества $B$, и никаких других. |
| $\cap$ | *Пересечение множеств* $A$ и $B$ есть двухместная операция, которая обозначается $A \cap B$ и представляет собой множество, содержащее все элементы множества $A$, одновременно являющиеся элементами множества $B$, и только их. |
| $\setminus$ | *Разность множеств* $A$ и $B$ есть двухместная операция, которая обозначается $A \setminus B$ и представляет собой множество, содержащее все элементы множества $A$, одновременно НЕ являющиеся элементами множества $B$, и только их. |
| $\Delta$ | *Симметрическая разность множеств* $A$ и $B$ есть двухместная операция, которая обозначается $A \Delta B$ и представляет собой множество, содержащее все элементы множеств $A$ и $B$, за исключением тех, которые одновременно являются элементами обоих множеств, и только их. |
| $\subseteq$ | *Вложение множеств* $A$ и $B$ есть двухместный предикат, который обозначается $A \subseteq B$ и означает, что все элементы множества $A$ одновременно являются элементами множества $B$. |
| $=$ | *Равенство множеств* $A$ и $B$ есть двухместный предикат, который обозначается $A = B$ и означает, что множества $A$ и $B$ состоят из одних и тех же элементов, т.е. $A \subseteq B$ и $B \subseteq A$ одновременно. |
| $\in$ | *Принадлежность* объекта $A$ к множеству $B$ есть двухместный предикат, который обозначается $A \in B$ и означает, что $A$ является элементом множества $B$. |

## А2.4. Связь логики и семантики через объем понятия

Введя все необходимые обозначения и понятия, посмотрим теперь, как логические связки связаны с теоретико-множественными операциями и предикатами.

Пусть у нас снова есть некоторое понятие $\mathfrak{C}_1$, которое задано определением на языке $\mathfrak{Math}$ с помощью формулы $\mathscr{D}_1(a)$. Пусть далее $V_1$ есть объем данного понятия. Аналогично, пусть есть понятие $\mathfrak{C}_2$ с определением $\mathscr{D}_2(a)$ и объемом $V_2$. Здесь $V_1$ и $V_2$ — множества.

Рассмотрим формулу $\mathscr{A}_1(a) \overset{\text{def}}{\rightleftharpoons} \mathscr{D}_1(a) \wedge \mathscr{D}_2(a)$, которая говорит нам, что объект $a$ должен обладать одновременно свойством $\mathscr{D}_1$ и свойством $\mathscr{D}_2$. Пусть $\mathscr{A}_1$ есть определение нового понятия $\mathfrak{C}$. Чему же равен тогда объем этого понятия? Легко заметить, что в объеме $V$ понятия $\mathfrak{C}$ лежат те и только те объекты, которые одновременно есть как

в объеме $V_1$ (ибо удовлетворяют свойству $\mathscr{D}_1$), так и в объеме $V_2$ (ибо удовлетворяют свойству $\mathscr{D}_2$). Но тогда по определению пересечения множеств и равенства множеств получаем, что $V = V_1 \cap V_2$.

Таким образом мы видим четкое соответствие между логический связкой $\wedge$ и значком $\cap$, т.к. первая порождает определение нового понятия $\mathfrak{C}$, а вторая — его объем. Иначе говоря, логические и теоретико-множественные обозначения — это две стороны одной медали.

Точно такая же связь прослеживается между логической связкой $\vee$ и значком $\cup$, а также между $\neg$ и $\setminus$. В последнем случае, правда, приходится задействовать обозначение универсума, поскольку если $\mathscr{A}_2(a) \overset{\text{def}}{\leftrightarrow} \neg\mathscr{D}_1(a)$, то для соответствующего объема $V$ будет верно равенство $V = \mathfrak{U} \setminus V_1$. Впрочем, часто, если универсум не меняется в ходе исследования, то его обозначение можно опускать и записывать *дополнение* к $V_1$ просто как $\setminus V_1$ или, еще проще, $\overline{V_1}$.

Немного сложнее дело обстоит с импликацией.

Рассмотрим определение $\mathscr{A}_3(a) \overset{\text{def}}{\rightleftharpoons} \mathscr{D}_1(a) \to \mathscr{D}_2(a)$. Оно выражает такое свойство объекта $a$: если объект $a$ принадлежит понятию $\mathfrak{C}_1$, то он принадлежит и понятию $\mathfrak{C}_2$. Таким образом новое понятие $\mathfrak{C}$ с необходимостью должно включать все те объекты, которые, будучи элементами $V_1$, являются также элементами $V_2$, т.е. объем нового понятия $\mathfrak{C}$ содержит в себе как минимум пересечение $V_1 \cap V_2$.

Однако формула $\mathscr{A}_3(a)$ ничего не сообщает нам про те объекты, которые НЕ удовлетворяют $\mathscr{D}_1(a)$, т.е. принадлежат объему $\mathfrak{U} \setminus V_1$. И здесь мы натыкаемся на ключевой момент, определяющий математическую (материальную) импликацию: если объект $a$ НЕ удовлетворяет посылке импликации (т.е. для него не выполняется «если»), то вся импликация в целом считается для него истинной. Об этом свойстве импликации мы поговорим чуть позже, а пока сделаем вывод, что в таком случае объем $V$ нового понятия $\mathfrak{C}$ с определяющей формулой $\mathscr{A}_3(a)$ должен также включать в себя и дополнение к $V_1$, т.е. $\mathfrak{U} \setminus V_1$.

И поскольку мы разобрали все случаи (когда $a$ удовлетворяет $\mathscr{D}_1$ и когда не удовлетворяет $\mathscr{D}_1$), мы полностью вычислили объем понятия $\mathfrak{C}$, который состоит из таких $a$, которые принадлежат либо объему $V_1 \cap V_2$, либо объему $\mathfrak{U} \setminus V_1$, т.е. в этом случае

$$V = (\mathfrak{U} \setminus V_1) \cup (V_1 \cap V_2).$$

Иначе говоря, определение $\mathscr{A}_3(a)$ можно переписать, пользуясь ранее полученными соответствиями логических связок и теоретико-множественных операторов, следующим образом:

$$\neg\mathscr{D}_1(a) \vee (\mathscr{D}_1(a) \wedge \mathscr{D}_2(a)).$$

В дальнейшем мы увидим, что эту формулу можно упростить до $\neg\mathscr{D}_1(a) \vee \mathscr{D}_2(a)$, поскольку $V_2 = (V_1 \cap V_2) \cup (V_2 \setminus V_1)$, но вторая часть этого объединения уже содержится в $\mathfrak{U} \setminus V_1$, так что $(\mathfrak{U} \setminus V_1) \cup V_2 = (\mathfrak{U} \setminus V_1) \cup (V_1 \cap V_2) = V$.

Таким образом логическая связка $\to$ соответствует более сложному теоретико-множественному оператору, составленному из объединения $V_2$ и дополнения $V_1$.

Однако, в том случае, если определение $\mathscr{A}_3(a)$ оказалось тождественно истинным, т.е. оно соответствует пустому понятию с объемом, равным, всему универсуму, то формула $\mathscr{A}_3(a)$ просто-напросто сообщает нам, что всякий представитель первого понятия является представителем второго понятия, т.е. $V_1 \subseteq V_2$. В таком частном случае мы получаем соответствие между импликацией $\to$ и вложением $\subseteq$.

# A2.5. Логические рассуждения

Здесь мы постепенно переходим к той части процесса формализации (см. стр. 45), которая выражает собственно логику, т.е. правила получения новых истин из уже известных. Ниже мы обсудим, как в математике строятся суждения и почему они отличаются от общепринятых в разговорном языке.

## A2.5.1 Понимание логических связок

Выше мы привели несколько определений логических связок и теоретико-множественных операций, в которых использовали разговорные части речи, такие как союзы И, ИЛИ, а также частица НЕ. Нужно понимать, что в математике мы фиксируем за ними конкретный смысл и свойства, хотя в разговорном языке И и НЕ могут менять свое поведение в зависимости от контекста.

Например, союз И ($\wedge$) в математике обозначает коммутативную логическую операцию, т.е. сказать $\mathscr{A} \wedge \mathscr{B}$ означает то же самое, что сказать $\mathscr{B} \wedge \mathscr{A}$, и такая замена правомерна независимо от контекста. В разговорном же языке союз И не всегда коммутативен, так как часто И может подразумевать наличие логической зависимости между его компонентами. Например, фраза «выглянуло солнце, И стало тепло» несмотря на формальный вид конъюнкции имеет неявную импликативную коннотацию (выглянуло солнце, в следствие чего стало тепло). Согласитесь, что если поменять местами члены данной конъюнкции, то фраза станет восприниматься иначе: «стало тепло, и выглянуло солнце». Здесь проявляются те свойства обычного языка, которых нет в математике, — отражение растянутых во времени процессов, так что мы невольно подразумеваем, что сначала выглянуло солнце, а затем стало тепло, хотя явно нам не указывается на то, что второе есть следствие первого (впоследствии не значит вследствие), но мы неявно верим в такую импликацию.

В программировании конъюнкция тоже не вполне коммутативна. Дело в том, что программа исполняется компьютером во времени, и потому исполнение кода в порядке $\mathscr{A} \wedge \mathscr{B}$ не равносильно исполнению в обратном порядке $\mathscr{B} \wedge \mathscr{A}$. Этой особенностью часто пользуются, чтобы сэкономить на вычислениях и избежать некоторых ошибок. Например, проверка конъюнктивного условия `len(a)>0 and a[0]==1` в случае пустого списка `a` остановится на первом условии и выдаст ответ `False` без проверки второго условия. Однако же если поменять члены конъюнкции местами (`a[0]==1 and len(a)>0`), то в случае `a[0]==1` второе условие все равно будет проверено (а это будет лишняя трата времени), а в случае, когда список `a` пуст, мы вообще получим ошибку, т.к. обращение к элементу `a[0]` станет невозможным. Таким образом, поведение логического оператора `and` в коде программы может отличаться при перестановке операндов из-за наличия направления чтения и исполнения текста программы.

Такая детерминированная некоммутативная логика особенно важна в робототехнике. Система управления роботом-манипулятором или беспилотным автомобилем — это, по сути, сложнейшая логическая формула, исполняемая в реальном времени. Условие «проверить наличие препятствия И сделать шаг вперед» является безопасным, в то время как обратное — «сделать шаг вперед И проверить наличие препятствия» — катастрофично. В этом мире, где цена ошибки — физическое разрушение, язык Math в его не вполне математическом, *алгоритмическом, диалекте* выступает единственным средством, гарантирующим предсказуемость и надежность.

Частица НЕ в разговорном языке тоже ведет себя не совсем так, как мы предполагаем в математике и формальной логике. Очень часто отрицательная частица может указывать на явно негативный смысл. Например, «некрасивый» есть противоположность «красивому», но это не означает, что все предметы можно разделить на красивые и некрасивые. В данном случае частица НЕ играет роль арифметического отрицания, а не логического исключения.

В разговорном языке обычно не работает закон двойного отрицания, предполагающий, что $\neg\neg\mathscr{A}$ суть то же самое, что $\mathscr{A}$. Так, «не некрасивый» вовсе не означает «красивый», и здесь уже поведение первого НЕ больше похоже на логическое исключение, чем на арифметическое отрицание. Иначе говоря, оператор НЕ в разговорном языке не *инволютивен*.

Для того, чтобы однозначно зафиксировать, какой смысл мы вкладываем в логические операторы, нужно использовать таблицы истинности, предписывающие вычисление значений выражений $\mathscr{A} \wedge \mathscr{B}$, $\mathscr{A} \vee \mathscr{B}$, $\mathscr{A} \to \mathscr{B}$, $\neg\mathscr{A}$ при условии, что уже вычислены значения обоих выражений $\mathscr{A}$ и $\mathscr{B}$. Обычно эти таблицы напоминают таблицы умножения из школьной тетрадки, только всего лишь с двумя числами: 0 и 1, которые являются алгебраическими обозначениями понятий Ложь и Истина, соответственно (см. таб. А2.3).

Таблица А2.3. Таблица истинности

| $\mathscr{A}$ | $\mathscr{B}$ | $\neg\mathscr{A}$ | $\mathscr{A} \wedge \mathscr{B}$ | $\mathscr{A} \vee \mathscr{B}$ | $\mathscr{A} \to \mathscr{B}$ | $\mathscr{A} \leftrightarrow \mathscr{B}$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1 | 1 | 1 | 1 |

Если какие-то два логических выражения от одних и тех же переменных ведут себя одинаково согласно таблице истинности, то мы их отождествляем, что записывается символом $\equiv$. Например, $\mathscr{A} \wedge \mathscr{B} \equiv \mathscr{B} \wedge \mathscr{A}$ (свойство коммутативности конъюнкции).

Составляя новые пропозициональные формулы по правилу матрешки, мы можем получать все и новые и новые логические выражения, некоторых из которых будут тождественны. Например,

$$\neg\neg\mathscr{A} \equiv \mathscr{A}, \quad \mathscr{A} \to \mathscr{B} \equiv \neg\mathscr{A} \vee \mathscr{B}, \quad \neg(\mathscr{A} \wedge \mathscr{B}) \equiv \neg\mathscr{A} \vee \neg\mathscr{B}, \quad \neg(\mathscr{A} \vee \mathscr{B}) \equiv \neg\mathscr{A} \wedge \neg\mathscr{B}.$$

Таким образом у нас появляется чисто алгебраический аппарат манипулирования логическими выражениями, и в этом месте зарождается *алгебра логики*.

Действительно, у нас есть переменные, которые могут принимать только логические значения (которые мы обозначаем 0 и 1), а значит, под этими переменными мы можем понимать произвольные истинностные высказывания вроде «снег черный» или «Сократ — человек». Кроме того, у нас есть логические связки ($\wedge$, $\vee$, $\neg$, $\to$, $\leftrightarrow$), с помощью которых мы можем строить достаточно сложные логические выражения и манипулировать ими примерно так же, как мы это делаем в школьной арифметике. Разница лишь в том, что за переменными скрываются высказывания вместо чисел, а операциями являются логические операции вместо сложения и умножения.

При этом нужно понимать, что все переменные у нас независимые. В выражении $\mathscr{A} \wedge \mathscr{B}$ переменные $\mathscr{A}$ и $\mathscr{B}$ никак не связаны друг с другом до тех пор, пока вместо

них мы не подставим что-нибудь более сложное. Это означает, что все логические тождества, которые мы можем получить с помощью таблицы истинности, не зависят от природы высказываний, которые мы могли бы подставить вместо этих переменных. Например, закон двойного отрицания $\neg\neg\mathscr{A} \equiv \mathscr{A}$ будет верным не зависимо от того, что мы подразумеваем под $\mathscr{A}$ (свойство быть «красивым» или глагол «пошел»).

В этом месте кроется, пожалуй, самое существенное отличие математических суждений от любых других (как в разговорном языке, так и в языках естественных наук вроде физики или биологии): *форма суждения превалирует над его содержанием*, потому что суждения математического языка строятся по строгим (алгебраическим) правилам манипуляций с логическими формами (или, точнее, *формулами*).

Конечно, выбор направления этих манипуляций уже не есть категория чистой формы, и в большей степени определяется содержанием. Например, если мы хотим доказать теорему Кантора, то мы так подбираем последовательность чисто формальных манипуляций, чтобы получить теорему Кантора, а не что-нибудь совершенно другое. Иначе говоря, технология математических суждений (доказательств) носит чисто формальный характер, в то время как их конечный результат понимается математиками менее формально и подчас содержит очень глубокий смысл.

В физике, например, это не совсем так, поскольку при всех манипуляциях с формулами в физике субъект этих манипуляций (физик-теоретик) всегда руководствуется физическим смыслом при выборе каждого следующего шага формальных манипуляций. Так, например, если математик, решая квадратное уравнение, получает комплексные корни, он рассмотрит их в ходе дальнейших манипуляций как возможные решения, поскольку логика требует рассмотрения всех формально допустимых вариантов ветвления процедуры рассуждений. Физик же в такой ситуации сразу отбросит те корни уравнения, которые не имеют физического смысла, и ограничится в дальнейшем рассуждении только допустимыми с его точки зрения корнями.

Таким образом получается, что физик, несмотря на постоянное использование математического языка в своих поисках истины привлекает некоторые дополнительные ограничители, отбрасывая некорректные с его точки зрения кейсы. Математик же упорно проверят все возможные варианты, даже самые, казалось бы, нелепые, просто потому, что они формально допустимы.


*Джордж Буль*

Отметим, что хотя считается, что еще Аристотель заложил основы логики, систематическое изучение связок между высказываниями (логика высказываний) началось позже, значительный вклад внесли стоики (например, Хрисипп в III веке до н.э.). Однако современная символическая форма и алгебраический подход к логике были разработаны в XIX веке Джорджем Булем («Исследование законов мысли», 1854) и Огастесом де Морганом, чьи работы заложили фундамент математической логики.

## A2.5.2 Принцип сведе́ния

Следующий прием математических рассуждений заключается в том, что наиболее часто используемые процедуры и результаты мы предпочитаем как-то обозначить, и далее ссылаться на них для экономии места и времени, ничуть не опасаясь, что они могут «испортиться» от частого применения или перестать быть актуальными.

Такой подход хорошо описывается известным анекдотом про чайник. Физику и математику ставят одинаковую задачу: нужно подогреть воду, причем в первом варианте

задачи условия такие: есть плита, пустой(!) чайник и кран с водой. И этот вариант оба решают одинаково: нальем воду в чайник, поставим на плиту и подогреем воду. Во втором варианте условия отличаются: вода уже налита в чайник! Физик решает задачу так: поставим чайник на плиту и подогреем его. Математик решает иначе: выльем воду из чайника, и придем к уже решенной задаче.

Более формально этот подход выражается у математиков (и программистов) следующим образом: если нужно регулярно производить с данными какую-то процедуру, то проще всего написать отдельную функцию (или хотя бы ввести специальное обозначение для оператора) и дальше вставлять в текущий текст не преобразованные данные, а функцию от исходных данных. Получается коротко и ясно. Если это попытаться повторить в обычном языке, то получится примерно следующее: введем функцию Perf(x), которая будет получать на вход глагол в начальной форме и возвращать данный глагол в форме перфекта. Тогда вместо фразы «Вася приехал вчера» мы сможем записать фразу «Вася Perfприезжать() вчера». Для математика и программиста такая подача текста является естественной, в то время как для обывателя она выглядит ненормальной.

И хотя иногда такие вещи могут показаться людям со стороны нелепыми, они предсказуемо работают (или не работают) с одинаковой силой и универсальностью.

### A2.5.3 Кванторы

Если мы хотим строить логические выражения не только в виде чисто логических формул с пропозициональными переменными или предикатами, подставленными вместо пропозициональных переменных, то нам потребуются кванторы.

Чуть выше мы уже использовали предикаты, связанные с множествами, например, $x \in A$ или $A = B$. Эти два предиката можно рассматривать как атомарные формулы в формальной теории множеств, а все остальные свойства описывать более сложными формулами. Однако равенство можно выразить через принадлежность более сложной формулой, но уже с использованием кванторов.

В этом месте зарождается **логика предикатов**, или *исчисление предикатов*, или логика первого порядка.

Кванторы — это такие логические операторы, которые обладают свойством свертки, т.е. редуцированием количества свободных переменных в логической лексеме (формуле). Основными кванторами являются: $\forall$ — квантор всеобщности, и $\exists$ — квантор существования.[11] Их семантика такова: $\forall x$ означает «для любого $x$», и далее следует какая-либо формула, зависящая от переменной $x$; $\exists x$ означает «существует такой $x$, что», и далее следует какая-либо формула, зависящая от переменной $x$. Переменная $x$ при этом становится *связанной*, но помимо $x$ в последующей формуле могут быть и другие свободные переменные.

Следующая формула является определением предиката равенства множеств $A = B$:

$$\forall x\ (x \in A) \leftrightarrow (x \in B),$$

где переменная $x$ является связанной, а переменные $A, B$ — свободными. Формула сообщает нам, что два множества равны, если они состоят из одних и тех же элементов.

[11] Хотя символы кванторов появились позже, концептуальный прорыв в формализации утверждений общности и существования принадлежит Готлобу Фреге. В своей работе [21] он впервые ввел ясную систему записи суждений, включающую аналоги кванторов, что позволило анализировать структуру математических утверждений с невиданной ранее точностью.

Используя кванторы и предикат принадлежности, мы можем выразить и другие предикаты теории множеств. Например, вложение множеств $A \subseteq B$ по определению выражается формулой $\forall x\ (x \in A) \to (x \in B)$, которая сообщает, что всякий элемент $A$ есть также элемент $B$ (в полном соответствии с определением отношения $\subseteq$).

Впоследствии из этих двух определений мы сможем вывести еще одно определение равенства множеств $A$ и $B$: $(A \subseteq B) \wedge (B \subseteq A)$.

В матлогике часто используется так называемое *универсальное замыкание*, когда истинная формула с параметрами (например, аксиома) заменятся на таковую же, но с квантором всеобщности по всем переменным, т.е. осуществляется логический переход от формулы $\mathscr{A}(a, b, c)$ к формуле $\forall a \forall b \forall c\ \mathscr{A}(a, b, c)$.

Приведем еще один шуточный, но вполне строгий пример математического рассуждения. Три математика приходят в бар, садятся за столик, и подошедший официант задает им вопрос:

— Все будут пиво?

— Не знаю, — отвечает первый математик, подумав.

— Не знаю, — отвечает второй математик.

— Да! — отвечает третий.

Почему они все отвечали именно так? Первый не знал, чего хотят остальные, но сам хотел пива, поэтому ответил «не знаю». Если бы он не хотел, то сразу бы ответил «нет», т.к. уже было бы понятно, что не все хотят пиво (ведь «не все хотят», значит, «хотя бы один не хочет»). Второй после ответа первого уже понял, что первый будет пиво, но не знал про третьего, а сам тоже хотел. Поэтому тоже ответил «не знаю». Наконец, третий математик из их ответов понял, что они хотят пиво (иначе бы кто-то из них или оба ответили бы «нет»), сам он тоже хотел, так что можно было смело сделать вывод, что пиво будут все, поэтому на вопрос официанта он ответил Да!».

Заметим, что вопрос официанта был понят чисто математически: верно ли, что $\forall x\ Wants\_beer(x)$, где предикат $Wants\_beer$ выражает свойство объекта $x$ «хотеть пиво». Поэтому, когда третий математик вычислил истинность этого выражения, он и ответил Да.

А если бы кто-то из них не хотел пива, верным было бы утверждение, являющееся отрицанием исходного:

$$\neg(\forall x\ Wants\_beer(x)),$$

которое математически записывается с использованием квантора существования так:

$$\exists x\ \neg Wants\_beer(x).$$

Кванторы всеобщности и существования являются двойственными друг другу через оператор логического отрицания: [12]

$$\neg(\forall x\ \mathscr{A}) \equiv \exists x\ \neg\mathscr{A}(x) \text{ и } \neg(\exists x\ \mathscr{A}) \equiv \forall x\ \neg\mathscr{A}(x).$$

Поэтому, чтобы доказать, что утверждение вида «все...» не верно, достаточно лишь привести контрпример, т.е. привести хотя бы один пример обратного. В случае с пивом, если бы кто-то из математиков его не хотел, он и был бы таким контрпримером к

[12] Кванторы $\forall$ и $\exists$ можно понимать, соответственно, как конъюнкцию и дизъюнкцию по неограниченному числу значений переменной. Например, $\forall x\ \varphi(x)$ — это $\varphi(x_1) \wedge \varphi(x_2) \wedge \ldots$, где $x_i$ — перечисление всех возможных значений переменной $x$, если таковых конечный набор.

утверждению про всех, а значит, одного его «нет» было бы достаточно, чтобы официанту вернуть ответ «нет». И если бы, например, первый из них ответил «нет», остальные бы вообще промолчали, т.к. ответ на вопрос официанта уже найден.

В приведенном примере существенно то, что все отвечающие на вопрос про пиво были математиками и, следовательно, рассуждали одинаково математически. Если бы вопрос был адресован не математикам, то наверняка каждый из них бы ответил что-то вроде «Да, пожалуй», и это было бы воспринято официантом как «я буду», т.е. он ответил бы не на прозвучавший вопрос про всех, а на подразумеваемый вопрос, обращенный к каждому по отдельности «будете ли вы пиво?».

### A2.5.4 Про импликацию

Импликация ($\mathscr{A} \to \mathscr{B}$) в математике — это так называемая **материальная импликация**. Ее определение, как и всех прочих формул логики высказываний никак не учитывает взаимосвязь цедентов (т.е. посылки и вывода). И как мы уже видели в таблице истинности, импликация $\mathscr{A} \to \mathscr{B}$ ложна только в одном случае: когда $\mathscr{A}$ истинно и $\mathscr{B}$ ложно. Во всех остальных трех случаях импликация истинна.

Истинными считаются, например, высказывания: «Если на Солнце есть жизнь, то дважды два равно четыре», «Если Волга — озеро, то Токио — большой город», «Если Солнце — куб, то Земля — треугольник», «Если дважды два равно пять, то Токио — маленький город» и т.п. В обычном рассуждении все эти высказывания вряд ли будут рассматриваться как имеющие смысл и еще в меньшей степени как истинные.[13] Очевидно, что материальная импликация плохо согласуется с обычным пониманием условной связи, однако она превосходно работает там, где исчисление форм нужно производить независящим от семантики способом, т.е. — в математике.

На самом деле такого рода высказывания мы часто используем в обычной жизни, чтобы подчеркнуть абсурдность посылки. Например, так: «если он математик, то тогда я папа римский», что буквально означает, что некий он совершенно точно не может быть математиком. Заметим, что в такой конструкции используется именно материальная импликация, ведь посылка и следствие никак между собой не связаны, и только по правилам чистой логики с помощью контрапозиции (рассуждения от противного) мы можем получить ложность посылки (поскольку я не папа римский, то он — не математик), ибо:

$$\mathscr{A} \to \mathscr{B} \equiv \neg\mathscr{B} \to \neg\mathscr{A}.$$

В бытовом языке общения мы используем как минимум две различные импликации: 1) материальную и 2) релевантную. Вторая подразумевает, что межу посылкой (антецедентом) $\mathscr{A}$ и следствием (сукцедентом/консеквентом) $\mathscr{B}$ есть некоторая содержательная связь. *Релевантная импликация* не допускает таких правил вывода, которые являются определяющими для материальной импликации, а именно: из ложной посылки следует любое высказывание; истинное высказывание следует из любой посылки.

Пример релевантной импликации: если запись числа $a$ оканчивается на 0, то оно кратно 5 (речь идет о целых числах). Здесь мы ничего не знаем про число $a$, но если для него выполняется посылка, то выполняется и вывод. А если посылка не выполняется, то истинность самого суждения при этом никак не страдает. При этом как в посылке, так и в выводе есть общая объектная переменная, которая в посылке представлена

[13] Такие суждения называют еще *алогизмами*.

переменной $a$, а в выводе местоимением «оно». Математически более правильно было бы написать это суждение так: если запись числа $a$ оканчивается на 0, то число $a$ кратно 5.

Более того, мы знаем, что на 5 также делятся и другие числа, и это значит, что путать местами посылки и вывод ни в коем случае нельзя! Ведь не всегда верно, что если число делится на 5, то его запись заканчивается на 0. Этот пример четко демонстрирует нам, что нельзя путать импликацию ($\rightarrow$) с эквиваленцией ($\leftrightarrow$)!

В математике мы стараемся четко детерминировать различные импликации разными способами. Например, в логике предикатов помимо чисто логической импликации мы используем дедуктивный вывод. И если логическая импликация выводит абсолютные логические истины, то дедуктивный вывод больше нужен для того, чтобы из нелогических истин (аксиом) получать релевантные выводы (теоремы). Конечно, нельзя не вспомнить здесь про теорему о дедукции, которая утверждает, что $\mathscr{A} \rightarrow \mathscr{B}$ истинно тогда и только тогда, когда из $\mathscr{A}$ выводимо $\mathscr{B}$, т.е. что формально эти две импликации равносильны (в классической логике предикатов). Но по сути это означает, что истинная в чистой логике формула $\mathscr{B}$ считается дедуктивно истинной тоже, и наоборот. Большинство же математических теорем формулируются скорее как релевантные импликации, поскольку их непосредственное доказательство происходит в одном выбранном контексте аксиом заданной теории.

Для сравнения приведем еще два примера теорем из Анализа:

(1) если функция непрерывна на отрезке, то она интегрируема на нем;

(2) если множество натуральных чисел счетно, то всякая непрерывная на отрезке функция интегрируема на нем.

В первом случае мы видим четкую связь посылки и следствия, поскольку в обоих случаях речь идет об одной и той же функции. Во втором случае мы просто связали два истинных утверждения, не имеющих ничего общего между собой. Первый пример представляет нам релевантную импликацию, второй — материальную. И если внимательно разобраться в дедуктивном выводе второго утверждения, то окажется, что посылка про множество натуральных чисел используется в нем фиктивно, т.е. может быть устранена без потерь для вывода.

Так что и саму теорему о дедукции можно рассматривать лишь как дополнительный формальный прием, помогающий сократить дедуктивный вывод по чисто формальным признакам.

Есть в математике и другие способы изучать различные виды импликаций и других логических связок (например, другого отрицания). Здесь мы имеем в виду так называемые неклассические логики, т.е. логики высказываний, в которых изначально логические операции устроены более сложным образом. Например, интуиционистская логика подразумевает запрет закона исключенного третьего, так что в ней отрицание перестает быть инволютивным (не всегда верно, что $\neg\neg\mathscr{A} \equiv \mathscr{A}$, хотя остается верным, что $\mathscr{A} \rightarrow \neg\neg\mathscr{A}$). В релевантной логике от импликации $\mathscr{A} \rightarrow \mathscr{B}$ требуется, чтобы у формул $\mathscr{A}$ и $\mathscr{B}$ была хотя бы одна общая предметная переменная (в нашем примере (1) это функция, о которой мы утверждаем интегрируемость).

Кроме того, в логику можно добавлять новые связки и новые кванторы, в результате чего получаются неклассические логики, которые могут описывать различные алгебраические структуры. К таковым можно отнести, например, модальные, субструктурные, немонотонные и другие логики.

Иначе говоря, математика вполне осознает, что классическая формальная логика имеет некоторые особенности, не всегда понятные и применимые в культурном или

научном контексте, и математика занимается анализом этих особенностей в рамках таких дисциплин как математическая логика и общая алгебра.

## A2.6. Построение выводов

Выше мы обсудили, как правильно строить логические лексемы (формулы) в рамках заданного языка $\mathfrak{Math}$, как их можно связать с математическими понятиями через логический аппарат теории множеств, как их понимать в более строгом, чем бытовой, смысле. Однако для того, чтобы исследовать предметную область и получать нетривиальные результаты, нужно обладать навыками не только правописания и понимания математического текста, но также знать некоторые приемы синтеза новых суждений, которые были бы настолько же достоверными, насколько достоверны базовые (аксиоматические) посылки. Самые общие такие приемы лежат в области логики, и ниже мы рассмотрим некоторые из них.

Здесь мы будем оперировать не только математическими понятиями для упрощения восприятия логических суждений, однако все приведенные примеры при желании можно перенести и в чисто теоретико-множественный язык, определяя подходящим способом объемы понятий.

Типовая конструкция суждения имеет вид:

$$\textbf{Посылки} \vdash \textbf{Вывод} \tag{A2.1}$$

Здесь мы не используем символ импликации ($\rightarrow$), поскольку он является чисто логическим оператором, выражающим часть какого-то высказывания. Символ же вывода ($\vdash$), именуемый на жаргоне «штопором», показывает логическую связь между отдельными высказываниями, скрывая некоторую последовательность рассуждений.[14]

Посылки обычно записываются через запятую, хотя формально их следовало бы соединять символом конъюнкции ($\wedge$), поскольку предполагается, что либо все посылки должны быть выполнены, чтобы можно было перейти к выводу, либо же хотя бы одна из них должна быть ложной (снова работает упоминавшаяся выше материальная импликация!). «Хотя бы одна» в данном случае как раз и означает, что ложность Посылок — это ложность конъюнкции посылок или, что то же самое, истинность дизъюнкции их отрицаний:

$$\neg(\text{Посылка1} \wedge \text{Посылка2} \wedge \text{Посылка3} \dots) \equiv \neg\text{Посылка1} \vee \neg\text{Посылка2} \vee \neg\text{Посылка3} \dots$$

### A2.6.1 Силлогизмы и абдукция

Первый пример нетривиального суждения является самым распространенным в учебниках логики и восходит еще ко временам Сократа и Аристотеля.[15] Здесь мы говорим о двухпосылочном силлогизме, а точнее, о композиции двух импликаций.

[14] Впрочем, как мы знаем из теоремы о дедукции в классическом исчислении предикатов, чисто математический формализм позволяет рассматривать эти два символа как эквивалентные.

[15] Теория силлогизмов была впервые подробно разработана Аристотелем в «Первой аналитике» и на протяжении веков оставалась ядром логического образования. Современная логика предикатов включает силлогистику как частный случай.

*Аристотель*

Пусть нам дано две посылки: 1) Все птицы — животные, 2) Все воробьи — птицы. Эти посылки сами по себе являются импликациями. Действительно, первая говорит нам, что всякая птица есть животное. Более формально это записывается так: обозначим за $\mathfrak{B}$ понятие «птица» и предположим, что его определение задано формулой $\mathscr{B}(x)$, пусть также $\mathfrak{A}$ — понятие «животное» с определяющей формулой $\mathscr{A}(x)$, и, кроме того, $\mathfrak{S}$ — понятие «воробей» с определяющей формулой $\mathscr{S}(x)$. Мы сейчас не акцентируем внимание на том, как выглядят эти определения и могут ли они вообще быть формализованы в языке $\mathfrak{Math}$, т.к. для общей логики это не играет роли.

В таких обозначениях первая посылка записывается импликацией $\mathscr{B}(x) \to \mathscr{A}(x)$, которую можно связать универсальным замыканием, т.е. навесить квантор всеобщности: $\forall x\ \mathscr{B}(x) \to \mathscr{A}(x)$, что как раз и будет читаться так, как нам надо — все птицы являются животными. Аналогично вторая посылка будет иметь вид: $\forall x\ \mathscr{S}(x) \to \mathscr{B}(x)$.

Наконец, если мы обозначим соответствующие объемы понятий за $A, B, S$, то получим два вложения объемов: $B \subseteq A$ (птицы есть животные) и $S \subseteq B$ (воробьи есть птицы). Визуально вложение объемов этих понятий отражено на рис. A2.2 с помощью так называемой **диаграммы Эйлера-Венна**, где объемы понятий (и вообще любые множества) изображаются кругами.

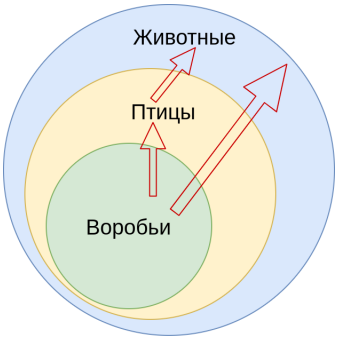



Рис. A2.2. Простейший силлогизм

Очевидным выводом из этих посылок является вложение $S \subseteq A$, которому соответствует формула $\forall x\ \mathscr{S}(x) \to \mathscr{A}(x)$ и словесная формулировка «Все воробьи — животные». Таким образом конструкция данного силлогизма записывается целиком так:

$$\text{Все птицы — животные, все воробьи — птицы} \vdash \text{Все воробьи — животные,}$$

или

$$\forall x\ (\mathscr{B}(x) \to \mathscr{A}(x)),\ \forall x\ (\mathscr{S}(x) \to \mathscr{B}(x)) \vdash \forall x\ (\mathscr{S}(x) \to \mathscr{A}(x)),$$

или

$$B \subseteq A,\ S \subseteq B \vdash S \subseteq A.$$

Последние две записи вывода написаны уже в чистом виде на языке математической логики, а точнее, на языке исчисления предикатов. Отличие этих выводов состоит лишь в выборе конкретного языка, а именно: в первом случае используется язык чистого исчисления предикатов, поскольку он не использует никаких специальных обозначений, кроме логических; а во втором случае используется язык теории множеств.

Общим местом этих записей является то, что у двух посылок есть общий цедент, это формула $\mathscr{B}(x)$, выражающая свойство быть птицей, а также множество $B$ всех птиц.

Этот цедент является интерполянтом,[16] как говорят в логике, для импликации $\mathscr{S}(x) \to \mathscr{A}(x)$. По сути мы здесь видим неявное проявление релевантной импликации.

Вывод, приведенный выше, является правильным независимо от того, правильные ли посылки. Мы можем модифицировать его, например, так:

$$\text{Все птицы — животные, все цветы — птицы} \vdash \text{Все цветы — животные,}$$

Это суждение само по себе по-прежнему остается истинным, хотя одна из его посылок ложна. Суждение показывает истинность *только взаимосвязи* посылок и вывода, но не требует однозначной истинностной оценки для своих компонентов. По этой причине всегда стоит отделять работу «штопора», т.е. процесса вывода, от тех высказываний, которые в нем участвуют. Напомним, что материальная импликация «почти всегда» истинна в том смысле, что есть только один из четырех вариантов значений антецедента и консеквента, когда импликация ложна (см. таб. A2.3). Так, из ложной посылки можно вывести любое высказывание, а истинное высказывание выводится из любой посылки, какой бы абсурдной она ни была. Тем самым реализуется принцип устойчивости истины по отношению к выводимости.

Рассмотрим пример похожего, но неверного суждения: если *некоторые французы — блондины* и *некоторые ученики — французы*, то *некоторые ученики — блондины*. Здесь обе посылки истинные, но вывод ложный, поскольку слово «некоторые» не гарантирует, что таковым признаком обладают все французы. А значит, из свойства «быть французом» не всегда следует «быть блондином», не выполняется соответствующее вложение множеств, являющихся объемами понятий «француз» и «блондин».

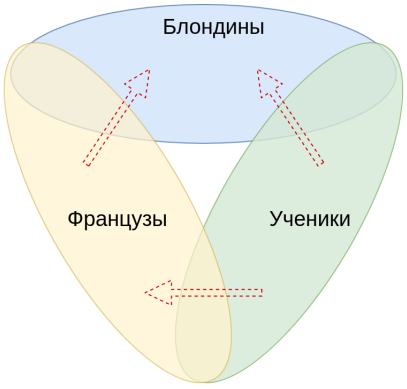



Рис. A2.3. Неверный силлогизм

Хотя, конечно, легко представить ситуацию, когда некоторые ученики действительно будут блондинами. Но это — лишь предположение, а не строгое логическое рассуждение.

На рис. A2.3 представлена схема, на которой мы видим, что все три множества могут пересекаться частично, и поэтому утверждать что-либо о полном вложении одного множества в другое мы не можем. В пересечения же попадают те объекты, которые характеризуются словом «некоторые».

В этом примере нарушается именно связка между посылками и выводом, т.к. две посылки не склеиваются по общему признаку (у них нет интерполянта).

[16] Отсылка к известной интерполяционной теореме Крейга из теории доказательств.

Ранее мы отмечали, что рассуждения в обратную сторону — от вывода к посылкам — неверны. Однако очень часто это верно отчасти. Например, мы знаем такой вывод: если число оканчивается на 0, то оно делится на 5. На основе этого мы не можем доказать точно, но **можем предположить**, что если число делится на 5, то оно, вероятно, может оканчиваться на 0. Как мы знаем, это верно примерно в половине случаев. Если бы такое *разворачивание импликации* было бы всегда абсолютно невозможным, то дедукция представляла бы собой простейший случай вывода, когда ложь влечет любое суждение. Для построения теорий это абсолютно бесполезно.

Метод *рассуждения назад*, к уже известной посылке, называется **абдукцией**. Именно таким методом, как правило, пользовался Шерлок Холмс в своих умозаключениях. Именно поэтому его выводы всегда носят вероятностный характер и сопровождаются словами «вероятно», «скорее всего» и т.п. Искусство Шерлока Холмса заключается в том, чтобы на основе опыта из всех возможных посылок в данной конкретной ситуации выбрать наиболее вероятную.[17]

Например, цитируем из рассказа «Этюд в багровых тонах» (Конан Дойль),

*«Этот человек по типу — врач, но выправка у него военная. Значит, военный врач. Он только что приехал из тропиков — лицо у него смуглое, но это не природный оттенок его кожи, так как запястья у него гораздо белее. Лицо изможденное, — очевидно, немало натерпелся и перенес болезнь. Был ранен в левую руку — держит ее неподвижно и немножко неестественно. Где же под тропиками военный врач-англичанин мог натерпеться лишений и получить рану? Конечно же, в Афганистане». Весь ход мыслей не занял и секунды. И вот я сказал, что вы приехали из Афганистана.*

Рассмотрим только часть умозаключений Холмса и сравним их с арифметическим примером:

| | |
|---|---|
| Ватсон — военный врач с изможденным лицом и загорелый | Число 30 — делится на 5 |
| Воевавшие в Афганистане — военные с изможденным лицом и загорелые | Оканчивающееся на 0 число — делится на 5 |
| Вывод: Ватсон прибыл из Афганистана | Вывод: 30 оканчивается на 0 |

Как видим, нам дано две посылки, в одной из которых дается некая связь между свойствами (воевавшие есть военные и т.д., а также оканчивающиеся на 0 делятся на 5), а в другой дается свойство конкретного объекта (Ватсон и число 30). Это свойство общее в обеих посылках, но по нему нельзя склеить их в силлогизм, т.к. свойство всегда стоит в конце посылки. Но Холмс знает, что практически все военные с изможденным лицом и загорелые — это воевавшие в Афганистане (хотя это и неверно на 100%), и на основании этого он предполагает(!), что и Ватсон такой же, раз он обладает таким же свойством.

На примере числа 30 это тоже сработало, однако стоит нам подставить 25 вместо 30, как вся цепочка рассуждений порушится! Поэтому абдуктивные умозаключения нельзя считать математическими, однако они могут навести на правильное дедуктивное умозаключение, в результате чего либо появляется теорема (*Все военные с изможденным*

[17] Термин 'абдукция' как особый тип логического вывода (выдвижение гипотез или вывод к наилучшему объяснению) был введен и подробно исследован американским философом и логиком Чарльзом Сандерсом Пирсом в конце XIX — начале XX века.

*лицом воевали в Афганистане*), либо обнаруживается контрпример (в нашем случае это число 25, которое опровергает предположение о том, что все делящиеся на 5 числа оканчиваются на 0).

Заметим, что абдуктивные заключения широко применяются в машинном обучении, когда по неполному ряду свойств, обладая массивом данных с аналогичными свойствами, мы классифицируем проверяемый в данный момент объект (Ватсон или число 25) с той или иной долей вероятности. Но справедливости ради нужно отметить, что добавление в схему абдукции вероятностей на самом деле возвращает нас в классическую логику, поскольку суждения теперь относятся не к исходным утверждениям, а к утверждениям о их вероятности. Более того, можно даже рассматривать неклассический вариант логики с вероятностными импликациями. Но это уже совсем другая история.

### A2.6.2 Модусы

Из рассмотренного выше вывода $(\mathscr{S} \to \mathscr{B}),\ (\mathscr{B} \to \mathscr{A}) \vdash (\mathscr{S} \to \mathscr{A})$ можно извлечь более простой метод построения выводов, который называется **Modus Ponens** и представляет собой одно из правил устранения импликации:

$$\mathscr{B},\ (\mathscr{B} \to \mathscr{A}) \vdash \mathscr{A}.$$

Его можно обосновать следующим образом. Подставим в предыдущее правило вместо высказывания $\mathscr{S}$ тождественную истину $\top$, тогда получим $(\top \to \mathscr{B}),\ (\mathscr{B} \to \mathscr{A}) \vdash (\top \to \mathscr{A})$. Но импликация вида $(\top \to \mathscr{A})$ равносильна самому высказыванию $\mathscr{A}$ в силу того свойства импликации, что из истины может следовать только истина. Тем самым получаем, что формулу $\top \to \mathscr{B}$ можно заменить на $\mathscr{B}$, а формулу $\top \to \mathscr{A}$ — на $\mathscr{A}$. В результате получится правило Modus Ponens.

Это правило можно проверить и на основе таблицы истинности A2.3, рассматривая все возможные логические значения переменных $\mathscr{A}$ и $\mathscr{B}$, при которых посылки правила истинны, и убеждаясь, что всякий раз при этом истинным будет и вывод.

И конечно же, это правило легко проверить с помощью множеств, заменяя импликацию вложением. Действительно, предполагая, что $B$ есть объем пустого понятия, т.е. универсум, а также, что $B \subseteq A$, легко понять, что тогда $A$ тоже совпадает с универсумом, т.е. является объемом пустого понятия (определяемого формулой $\top$), т.к. оно содержит в себе универсум, а большем, чем универсум, оно быть не может по определению универсума.

Modus Ponens — ключевое правило вывода при определении свойств штопора ($\vdash$). Удивительным фактом является то, что этого правила достаточно, чтобы вывести все логические истины (тавтологии), включая и более сложные правила вывода.

Выше мы говорили, что штопор ($\vdash$) означает, что мы перешли от посылок к следствиям, возможно, скрыв некоторую цепочку рассуждений. Но такие правила, как Modus Ponens, представляют собой одношаговый вывод, применяемый в логике как элементарный шаг вывода. Чтобы отличать многошаговый вывод от элементарного принято использовать другую нотацию при написании основных правил вывода, а именно, вертикальную:

$$\frac{\mathscr{B},\ \mathscr{B} \to \mathscr{A}}{\mathscr{A}},$$

где вертикальная черта выполняет ту же роль, что и $\vdash$, одновременно указывая на элементарность логического перехода. Поэтому базовые правила вывода мы всегда будем записывать таким способом.

Еще одним известным правилом вывода является Modus Tollens:

$$\frac{\mathscr{A} \to \mathscr{B},\ \neg\mathscr{B}}{\neg\mathscr{A}},$$

которое означает, что если верна импликация $\mathscr{A} \to \mathscr{B}$ и при этом ложно $\mathscr{B}$, то тогда и $\mathscr{A}$ ложно. По сути это правило иллюстрирует метод сведения к противоречию.

Рядом с Modus Tollens стоит правило доказательства «от противного» (*контрапозиция*):

$$\frac{\neg\mathscr{A} \to \bot}{\mathscr{A}},$$

которое говорит, что если в предположении ложности $\mathscr{A}$ мы приходим к противоречию (выводим ложь), то, значит, $\mathscr{A}$ истинно.

В логике существует довольно много правил, позволяющих переходить от истин к истинам. Все они являются свойствами выводимости, т.е. отношения между формулами, обозначаемого как $\vdash$.

Современная математическая логика изучает различные виды выводимости, а также различные типы правил вывода и зависимостей между ними с целью выявить минимальный достаточный набор правил вывода (своего рода базис выводимости) в разных конкретных случаях реализации этого отношения.

Конечно же, все эти сложные вещи относятся к неклассическим логикам, но мы здесь идем строго по классике, так что в нашем случае выводимость будет иметь довольно-таки простой вид: базовым правилом вывода является один лишь Modus Ponens (если не считать безусловного правила подстановки, о котором речь пойдет позже), а все остальные правила являются производными от него.

Выбор именно правила Modus Ponens, а не какого-либо иного, в качестве базиса есть вопрос традиций, т.е. по существу является случайным.

### A2.6.3 Дедукция, индукция

Построение строгих выводов из заданных или полученных ранее истинных высказываний и предикатов называется **дедукцией** и является основным методом рассуждений при получении математических теорем.

Иногда для построения нужного вывода требуется перебрать сотни комбинаций ранее доказанных посылок. Но часто для нащупывания правильной цепочки доказательства хватает вспомогательных иллюстраций или опыта исследователя, погруженного в данную тему.

Дедукция всегда есть переход об общего к частному. Например, аксиомы геометрии описывают в общем виде отношения точек, прямых и плоскостей, а теоремы геометрии есть применение аксиом в конкретных случаях для разных классов фигур (треугольников, трапеций и т.п.).

В противоположность дедукции существует метод **индукции**, предполагающий переход от частного общему. Если точнее, то индуктивное суждение строится так: мы наблюдаем один и тот же результат во многих однородных случаях и ожидаем, что результат будет тем же и в следующем случае того же рода.

Перейдем к конкретике. Рассмотрим арифметический пример высказывания:

($\mathscr{A}$) Если $a$ — четное число, то оно делится на 4.

Такое высказывание ложно, т.к. не все четные числа делятся на 4. Обратно,

($\mathscr{B}$) если число делится на 4, то оно четное.

А это высказывание уже истинное.

Высказывание ($\mathscr{B}$) является *дедуктивным*, поскольку основано на строгом выводе из свойств натуральных чисел. Оно **выводится** из аксиом или ранее доказанных теорем.

Высказывание ($\mathscr{A}$) может быть лишь предположением. Если бы мы взяли числа 4, 16, 32, 64, 128, 256, 512, 1024, то оказалось бы, что все они не только четные, но и делятся на 4. Может возникнуть подозрение, что так бывает всегда, и мы строим гипотезу: если число четное, то оно делится на 4. Такой вывод называется индуктивным.

Но затем мы обнаруживаем, что, например, 6 не делится на 4, хотя является четным (т.е., как говорят математики, мы нашли **контрпример**). Гипотеза оказывается неверной.

Другой пример индуктивного рассуждения: сколько мы ни брали нечетных чисел, а их квадрат всегда имел вид $4k + 1$, тогда мы строим гипотезу, что у любого нечетного числа квадрат имеет вид $4k+1$. Мы можем попробовать отыскать контрпример, если сомневаемся в верности нашего индуктивного заключения. Но у нас ничего не получится, поскольку на этот раз индукция подсказала нам верный ответ.

И чтобы дедуктивно доказать, что на самом деле так оно и есть, нам уже потребуется другой метод, а именно: **математическая индукция**, которая является краеугольным камнем арифметики, если не всей математики.

Математическая индукция — это суждение следующего вида. Пусть у нас имеется некоторое свойство $\mathscr{A}(n)$ натуральных чисел. Предположим, что верно $\mathscr{A}[n/0]$ и всякий раз, когда истинно $\mathscr{A}[n/x]$, истинно также и $\mathscr{A}[n/x + 1]$. Тогда $\mathscr{A}(n)$ тотально истинно (т.е. для всех реализаций переменной $n$ в натуральных числах). Формально аксиома индукции выглядит так:

$$\mathscr{A}[x/0] \wedge (\forall x\ (\mathscr{A}[n/x] \to \mathscr{A}[n/x + 1])) \vdash \forall x\ \mathscr{A}[n/x].$$

Напомним, что слеш в данном случае означает замену исходной переменной $n$ на соответствующий терм, стоящий под этим слешем.

Итак, математическая индукция — это не индукция в общем логическим смысле, а дедуктивный метод, который, в зависимости от выбранной теории, либо является аксиомой, либо выводится как теорема.

С математической индукцией связаны еще несколько принципов, о которых мы будем говорить в контексте арифметики:

- принцип бесконечного спуска;
- принцип фундированности;
- принцип Дирихле.

В целом можно сказать, что математика берет на вооружение все логические методы, однако только дедуктивные рассматривает как надежные способы получения результатов. А такие методы, как индукция (не математическая) и абдукция используются математиками для поиска опровержений или как попытка найти общее правило, которое потом следует доказать дедуктивно.

## A2.7. Про отношения и функции

Ранее мы все время оперировали свойствами предметов вида $\mathscr{A}(x)$, которые можно охарактеризовать как *унарные отношения* на универсуме. Унарным отношениям соответствуют объемы понятий, т.е. подмножества универсума. Однако мы можем рассмотреть и более сложные свойства предметов, а именно — их совместные свойства, или *отношения*. Так, если свойство $\mathscr{R}(x, y)$ утверждает что-либо одновременно про предметы $x$ и $y$, то мы говорим, что пара $\langle x, y\rangle$ находится в отношении $\mathscr{R}$.

Например, если мы в качестве предметной области рассмотрим людей, то под отношением $\mathscr{R}(x, y)$ мы можем понимать, например, отношение дружбы ($x$ и $y$ — друзья) или отношение родства (отец-сын, брат-сестра, предок-потомок и т.п.).

При этом объем такого понятия, как отношение, становится более сложным. Это — не подмножество универсума $\mathfrak{U}$, а подмножество некоторой степени универсума $\mathfrak{U}^n$. Под $n$-ой степенью универсума $\mathfrak{U}$ мы понимаем совокупность всех возможных упорядоченных наборов элементов $\mathfrak{U}$ длины $n$ (последовательных выборок с возвращением). Эти наборы принято записывать как вектор: $\langle x_1, \dots, x_n\rangle$ и часто даже используется сокращение $\vec{x}$, если $n$ известно из контекста.

Таким образом объемом $n$-арного отношения является подмножество $\mathscr{R} \subseteq \mathfrak{U}^n$, но чаще сам этот объем и называется **$n$-арным отношением** (при $n = 2$ — бинарным, при $n = 3$ — тернарным, а при $n = 1$ — унарным) на $\mathfrak{U}$. Число $n$ при этом называется *арностью* (или *валентностью*) отношения $\mathscr{R}$.

Так, множество всех пар людей $\langle x, y\rangle$, в которых $x$ есть брат $y$, является бинарным отношением, отношение $B(x, y, z)$, означающее, что точка $y$ лежит между точками $x$ и $z$, — тернарным отношением, а отношение $Par(a, b, c, d)$, означающее, что прямая, проходящая через точки $a, b$, параллельна прямой, проходящей через точки $c, d$, — кватернарным (четырехместным) отношением.

Если $\mathfrak{U}^n$ рассматривать как новый универсум, $n$-арные отношения будут соответствовать неким объемам понятий, так что всякое математическое отношение можно определять как математическое понятие со своим определением (формулой от $n$ аргументов), объемом (собственно отношение), термином и, опционально, обозначением.

Более того, можно пойти еще дальше и расширить универсум до суммы всех возможных степеней $\mathfrak{U}^n$ для всех натуральных $n \geqslant 1$, т.е. включить в наш универсум все упорядоченные наборы любой конечной длины, состоящие из элементов исходного универсума $\mathfrak{U}$. Такой универсум обозначается $\mathfrak{U}^{<\infty}$. Все возможные унарные, бинарные, тернарные, и т.д. отношения суть подмножества этого универсума.[18]

Этот прием конвертации произвольных отношений в множества широко используется в математике и полностью переводит логику в теорию множеств, поскольку всякая логическая формула от $n$ аргументов определяет некоторое $n$-арное отношение (хотя обратное, вообще говоря, не верно). В некотором смысле теоретико-множественный подход даже расширяет естественно-логический.

Укажем некоторые виды бинарных отношений:

1. $\mathscr{R}(x, y)$ — *рефлексивное*, если $\mathscr{R}(x, x)$ истинно для любого $x \in \mathfrak{U}$;
2. $\mathscr{R}(x, y)$ — *симметричное*, если из $\mathscr{R}(x, y)$ всегда следует $\mathscr{R}(y, x)$ для любых $x, y \in \mathfrak{U}$;
3. $\mathscr{R}(x, y)$ — *транзитивное*, если из $\mathscr{R}(x, y) \wedge \mathscr{R}(y, z)$ всегда следует $\mathscr{R}(x, z)$ для любых $x, y, z \in \mathfrak{U}$;

[18] Оставим за скобками вопрос о том, почему обратное утверждение не верно.

4. $\mathscr{R}(x, y)$ — *отношение эквивалентности*, если оно рефлексивное, симметричное и транзитивное;

5. $\mathscr{R}(x, y)$ — *предпорядок*, если оно рефлексивное и транзитивное.

В качестве иллюстрации рассмотрим отношение «отец-сын», т.е. $\mathscr{R}(x, y)$ истинно тогда и только тогда, когда $x$ есть отец $y$. Очевидно, что такое отношение не является рефлексивным, более того, оно *антирефлексивное*, т.е. формула $\mathscr{R}(x, x)$ ложна для всех $x \in \mathfrak{U}$. Оно также не является симметричным, т.к. если $x$ есть отец $y$, то наоборот уже быть не может (по крайней мере при соблюдении принципа причинности). И тем более оно не транзитивно, поскольку если $x$ есть отец $y$, а $y$ — отец $z$, то $x$ не может быть отцом $z$. Соответственно, отношение $\mathscr{R}$ не является ни отношением предпорядка, ни отношением эквивалентности.

Однако на его основе можно определить два новых отношения: 1) $\mathscr{P}(x, y)$ истинно тогда и только тогда, когда либо $\mathscr{R}(x, y)$, либо существуют люди $x_1, \ldots, x_n$ такие, что $\mathscr{R}(x, x_1) \wedge \mathscr{R}(x_1, x_2) \wedge \ldots \wedge \mathscr{R}(x_{n-1}, x_n) \wedge \mathscr{R}(x_n, y)$, т.е. существует цепочка людей, связанных отношением отец-сын в указанном порядке; 2) $\mathscr{Q}(x, y) \overset{\text{def}}{\leftrightarrow} \exists z\ (\mathscr{R}(z, x) \wedge \mathscr{R}(z, y))$.

Первое отношение $\mathscr{P}(x, y)$ говорит нам, что $x$ есть предок $y$, т.е. это отношение «предок-потомок». Данное отношение по-прежнему антирефлексивно, однако транзитивно, т.к. если $x$ — предок $y$, а $y$ — предок $z$, то $x$ — предок $z$. Антирефлексивное транзитивное отношение называется **строгим (частичным) порядком**.

Конечные частично упорядоченные множества часто визуализируют с помощью **диаграмм Хассе**. На таких диаграммах элементы изображаются вершинами, и если $x < y$, то $x$ рисуется ниже, чем $y$. Ребро соединяет $x$ и $y$ только в том случае, когда $x < y$ и не существует такого $z$, что $x < z < y$ (т.е. ребра, отвечающие подразумеваемой транзитивности, опускаются).

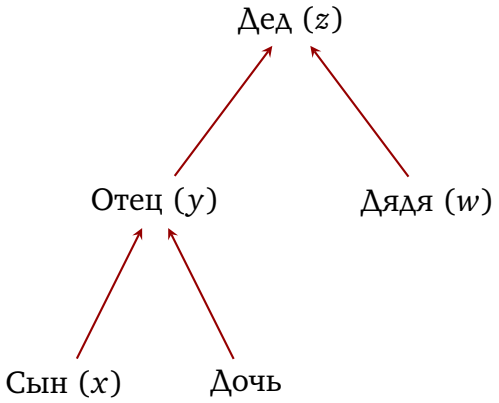



Рис. А2.4. Диаграмма Хассе для отношения «потомок ⩽ предок»

Рассмотрим, например, определенное выше отношение «предок» $\mathscr{P}$. Если условиться, что «ниже» означает потомка, а «выше» — предка, то мы получим классическое семейное дерево (см. рис. А2.4). Здесь Сын ($x$) связан с Дедом ($z$) отношением $\mathscr{P}(z, x)$, т.е. $z$ — предок $x$. Однако прямая линия между ними не проводится: связь подразумевается через Отца ($y$), поскольку $\mathscr{P}(z, y)$ и $\mathscr{P}(y, x)$. Стоит отметить, что *ребра* диаграммы Хассе в точности соответствуют исходному отношению $\mathscr{R}$ («отец»), в то время как *пути* в графе соответствуют транзитивному отношению $\mathscr{P}$ («предок»). Именно это визуальное опускание транзитивных линий делает диаграммы Хассе ясными и читаемыми по сравнению со стандартными графовыми представлениями отношений.

При желании мы можем пополнить отношение $\mathscr{P}$ до рефлексивного отношения, добавив к множеству $\mathscr{R}$ *диагональ* универсума $\mathfrak{U}^2$, а именно, множество всех пар $\langle x, x\rangle$. В итоге получим нестрогое отношение предок-потомок, допускающее, чтобы всякий $x$ был своим же предком. Как бы это странно ни звучали применительно к людям, но такие «замыкания» математических конструкций часто оказываются весьма удобными с точки зрения возможности упростить язык и теоремы.

Здесь можно вспомнить один юридический сюжет. Отношение поставщик-клиент по умолчанию подразумевается антирефлексивным, т.е. никто не может быть своим собственным поставщиком (услуг, товаров). Однако мы вполне можем представить себе случай, когда такое отношение может быть рефлексивным. Например, парикмахер может сам себя стричь (и не только парикмахер), в таком случае он и поставщик (услуги), и клиент одновременно в рамках одного и того же отношения (услуги стрижки). Но в таком случае следует признать, что отношения поставщик-клиент могут быть рефлексивными хотя бы частично. Дальше вступает в действие правовой аспект, предполагающий а) оплату услуг и б) начисление налогов на этот вид деятельности. И поскольку нет никакого ограничения по поводу применения налогового законодательства для рефлексивных финансовых отношений, строго говоря, всякий, кто сам себя стрижет, должен оформлять эту услугу и платить с нее налоги. Конечно, на практике это не работает, но осадок после подобного рода чисто логических рассуждений остается.

Далее, отношение $\mathscr{Q}(x, y)$ сообщает нам, что у $x$ и $y$ есть общий отец. Такое отношение, во-первых, рефлексивно (у $x$ и $x$ действительно есть общий отец),[19] во-вторых, симметрично (если отец есть у $x$ и $y$, то он есть у $y$ и $x$), в-третьих, транзитивно (если $w$ — отец $x$ и $y$, а $w'$ — отец $y$ и $z$, то $w$ и $w'$ — один и тот же человек, являющийся отцом $x$ и $z$). Таким образом $\mathscr{Q}$ есть отношение братства (по-английски оно точнее описывается словом *siblings*, т.к. включает и сестер). $\mathscr{Q}$ — пример отношения эквивалентности.

На самом деле, имея некоторый предпорядок $\mathscr{R}(x, y)$, всегда можно определить отношение эквивалентности формулой $\mathscr{R}(x, y) \wedge \mathscr{R}(y, x)$.[20]

Отношение эквивалентности позволяет разбить весь универсум на непересекающиеся *классы эквивалентности* так, что в каждом классе находятся те и только те объекты, которые попарно связаны между собой этим отношением. В предыдущем примере отношение $\mathscr{Q}$ разбивает всех людей на классы по прямому кровному родству. В каждом таком классе находятся братья и сестры, имеющие общего отца (заметим, что если «отца» заменить на «родителя», то схема сломается — отношение перестанет быть транзитивным).

Для определения следующих видов отношений нам потребуется привлечь одно из фундаментальных отношений — **равенство**. Это бинарное отношение эквивалентности на элементах универсума $\mathfrak{U}$, обладающее тем свойством, что в каждом классе эквивалентности находятся только такие предметы, которые невозможно отличить друг от друга теми средствами языка, которые у нас имеются.

В разделе B1.2.5 мы определим равенство более строгим способом, опирающимся на язык и логику предикатов. Равенство обычно обозначается символом $=$ и вместо $=(x, y)$ пишется как $x = y$.

Дадим еще несколько определений:

6. $\mathscr{R}(x, y)$ — *антисимметричное* отношение, если из $\mathscr{R}(x, y) \wedge \mathscr{R}(y, x)$ следует $x = y$;

[19] С оговоркой, что он есть у каждого человека из рассматриваемого универсума.

[20] Проверьте, что это так.

7. $\mathscr{R}(x, y)$ — (нестрогий) *частичный порядок* (или просто *порядок*), если это антисимметричный предпорядок;

8. $\mathscr{R}(x, y)$ — (нестрогий) *линейный порядок*, если это частичный порядок, обладающий свойством *связности*: для любых $x, y \in \mathfrak{U}$ имеет место $\mathscr{R}(x, y) \vee \mathscr{R}(y, x)$.

Интересно заметить, что если у нас имеется отношение предпорядка, то, как мы уже отмечали, нетрудно построить из него отношение эквивалентности. После чего, рассматривая в качестве новой предметной области классы эквивалентности как индивиды, несложно индуцировать на них исходное отношение предпорядка, которое окажется уже частичным порядком.[21] Таким образом факторизация (переход от исходного универсума к универсуму классов эквивалентности) улучшает свойства исходного отношения путем *огрубления* исходного универсума.

И еще пара определений:

9. отношение $\mathscr{R}(x, y)$ *тотально*, если для всякого $x$ существует ответный $y$, т.е. такой, что выполнено $\mathscr{R}(x, y)$;

10. отношение $\mathscr{R}(x, y)$ *функционально* (или просто *функция*), если оно тотально и из условия $\mathscr{R}(x, y) \wedge \mathscr{R}(x, z)$ всегда следует, что $y = z$, для всех $x, y, z \in \mathfrak{U}$.[22]

Например, рефлексивное отношение тотально. А если его урезать до диагонали (оставить только пары $\langle x, x\rangle$), то оно представляет собой функцию, которая обычно обозначается id.

Выше мы рассматривали только отношения на универсуме, однако чаще всего в математике рассматриваются более узкие случаи отношений — на множестве, когда переменные $x, y$ в лексеме $\mathscr{R}(x, y)$ пробегают лишь какое-то определенное множество $A$, заданное как часть универсума, т.е. $A \subseteq \mathfrak{U}$. В этом случае мы можем говорить не только об отношениях на множестве $A$, но и об отношениях *между* разными множествами $A$ и $B$, предполагая, что переменная $x$ пробегает элементы множества $A$, а переменная $y$ — элементы множества $B$.

Такое же обобщение относится и к произвольным $n$-арным отношениям, когда мы предполагаем, что отношение $\mathscr{R}(x_1, \ldots, x_n)$ связывает переменные, имеющие свои независимые области пробегания: $x_k \in A_k$. Само такое отношение представляет собой подмножество множества всех возможных $n$-ок $\langle x_1, \ldots, x_n\rangle$, которое обозначается $A_1 \times \cdots \times A_n$ и называется прямым произведением этих множеств.

Легко понять, тем не менее, что всякое более узкое $n$-арное отношение, заданное на множествах (между множествами) является, тем не менее, отношением на всем универсуме, хотя оно и не всюду определено.

Такие же соображения применимы и к функциям, как частному случаю отношений. Именно, мы можем говорить о том, что $\mathscr{F}$ есть функциональное отношение на $A \times B$, где $A$ и $B$ — какие-то множества в нашем универсуме. При этом тотальность $\mathscr{F}$ ограничивается лишь множеством $A$, и в этом случае пишут $\mathscr{F} : A \to B$ как обозначение утверждения «$\mathscr{F}$ есть функциональное отношение, тотальное на $A$».

[21] Это несложное упражнение предлагается проделать читателю самостоятельно.

[22] Если явно не оговорено иное, слово **функция** в этой книге обозначает *тотальную* функцию, определенную на каждом элементе своей области определения. Это стандартное соглашение теории множеств. Однако читателям, знакомым с информатикой или теорией вычислимости, следует иметь в виду, что в этих областях нормой являются частичные функции.

Более того, в качестве множества $A$ можно взять более сложное множество: $A_1 \times \cdots \times A_n$, и получить функцию $\mathscr{F} : A_1 \times \cdots \times A_n \to B$. Такая функция называется $n$-арной, ее аргументами являются $n$-ки вида $\langle x_1, \ldots, x_n \rangle$, где $x_k \in A_k$. Отметим, что если на такую функцию смотреть как на отношение, то, строго говоря, это бинарное отношение между множествами $A_1 \times \cdots \times A_n$ и $B$, но также его можно рассматривать и как $(n+1)$-арное отношение на множестве $A_1 \times \cdots \times A_n \times B$.

Подводя итог, заметим, что отношения в самом общем виде — это практически и есть предикаты, о которых мы говорили ранее. Разница лишь в том, что предикат — это лексема логического типа, участвующая в строительстве формул языка, т.е. это свойство предметов, записанное формально, а отношение — это область истинности предиката или, иначе говоря, объем того понятия-свойства, которое задается предикатом. Поэтому в книгах часто можно встретить отождествление между теоретико-множественной сущностью «отношение» и формально-логической «предикат». Про предикаты можно еще сказать, что они, как правило, имеют собственные названия и обозначения, т.е. каждый из них является математическим понятием, в то время как отношения далеко не все могут быть поименованы (хотя бы из соображения мощностей), а значит, не все могут быть математическим понятием, но все они являются элементами объема общего понятия «отношение».

Дальнейшей нашей целью является строгое, но максимально простое изложение логики высказываний на уровне B1 и затем, на ее основе, логики предикатов. Мы будем придерживаться схемы A2.1. При этом само изложение формальной теории мы будем производить уже на достаточно строгом языке, который можно считать частью языка $\mathfrak{Math}$ и который уже содержит данные нами выше определения логических связок и теоретико-множественных обозначений как математических понятий.

## A2.8. Вопросы для самоконтроля

**Q1** Какова основная функция логики применительно к языку $\mathfrak{Math}$? [стр. 43]

**Q2** Почему синтаксической логики (логики лексем) недостаточно для полноценного анализа предметной области? [стр. 43]

**Q3** Перечислите основные этапы формализации предметной области в языке $\mathfrak{Math}$. [стр. 45]

**Q4** Что такое «математическое понятие»? Назовите его обязательные и опциональные компоненты. [стр. 47]

**Q5** Объясните на примере простого числа, как идея понятия может отличаться от его формального определения в разных семантиках. [стр. 51]

**Q6** Какова связь между истинностью формул, аксиомами и выбранной семантикой? Объясните связь между логическими связками $(\wedge, \vee, \neg, \to)$ и теоретико-множественными операциями $(\cap, \cup, \setminus)$ через объем понятия. [стр. 52]

**Q7** Что такое кванторы всеобщности ($\square$) и существования ($\square$)? Как они связаны через оператор логического отрицания? [стр. 61]

**Q8** Объясните разницу между материальной импликацией, используемой в математике, и релевантной импликацией, характерной для бытового языка. [стр. 63]

## A2.9. Упражнения

**Ex1.** Классифицируйте следующие выражения по трем категориям: истинное высказывание, ложное высказывание или предикат (истинность зависит от значения переменных).

- $2 + 2 = 5$
- $x + 1 = 5$
- Все простые числа нечетны.
- $5 > 3$

**Ex2.** Запишите отрицание следующих утверждений (не добавляя просто «Неверно, что...»):

- Все кошки черные.
- Некоторые студенты любят математику.
- Если идет дождь, то земля мокрая.

**Ex3.** Пусть $A = \{1, 2, 3\}$ и $B = \{2, 3, 4\}$. **Определите истинностное значение** следующих формул:

- $\forall x \in A \quad (x < 4)$
- $\exists x \in B \quad (x$ — четное$)$
- $\forall x \in A \cap B \quad (x \geqslant 2)$

**Ex4.** Определите, является ли конструкция «если... то...» *материальной импликацией* или *релевантной импликацией*. Используйте критерий из Раздела A2.5.4: следует ли консеквент логически или семантически из антецедента, обычно имея с ним общую переменную?

- Если число $n$ делится на 6, то $n$ делится на 3.
- Если Эйфелева башня находится в Париже, то снег белый.
- Если человек — бабушка, то она женщина.

**Ex5.** Проверьте, является ли следующий логический вывод обоснованным, используя диаграмму Венна или логические рассуждения:

Все квадраты — прямоугольники.
Все прямоугольники — четырехугольники.
Следовательно, все квадраты — четырехугольники.

**Ex6.** (Предполагается, что все именные множества не пустые) Даны две посылки, выберите **все** заключения, которые логически следуют из них.

**P1:** Все Факси суть Кроло.
**P2:** Ни один Винда не есть Кроло.

a) По крайней мере один Факси не является Винда.

b) По крайней мере один Кроло является Факси.

c) По крайней мере один Кроло не является Винда.

d) По крайней мере один Винда не является Факси.

e) Ни один Факси не является Винда.

**Ex7.** (Предполагается, что все именные множества не пустые) Даны две посылки, выберите **все** заключения, которые логически следуют из них.

**P1:** Все Донас суть Судр.
**P2:** По крайней мере один Донас не является Калси.

a) По крайней мере один Судр не является Калси.

b) По крайней мере один Калси не является Судр.

c) По крайней мере один Судр является Донас.

d) Ни один Судр не является Калси.

**Ex8.** (Предполагается, что все именные множества не пустые) Даны две посылки, выберите **все** заключения, которые логически следуют из них.

**P1:** Ни один Тека не есть Арати.
**P2:** Все Тека суть Фато.

a) Все Арати суть Фато.

b) По крайней мере один Фато не является Арати.

c) По крайней мере один Тека является Фато.

d) По крайней мере один Арати не является Тека.

**Ex9.** (Предполагается, что все именные множества не пустые) Даны две посылки, выберите **все** заключения, которые логически следуют из них.

**P1:** Все Брон суть Ханто.
**P2:** По крайней мере один Турт является Брон.

a) Все Ханто суть Брон.

b) По крайней мере один Турт является Ханто.

c) По крайней мере один Ханто является Брон.

d) Ни один Турт не является Ханто.

**Ex10.** Используя связь между логическими связками и операциями над множествами (например, $A \cap (B \cup C)$ соответствует $P \wedge (Q \vee R)$), упростите следующие теоретико-множественные выражения.

1. $A \cup (A \cap B)$;
2. $(A \cup B) \cap (A \cup \overline{B})$;
3. $A \setminus (A \setminus B)$;

4. $(A \cap B) \cup (A \cap \overline{B}) \cup (\overline{A} \cap B) \cup (\overline{A} \cap \overline{B})$.

**Ex11.** Нарисуйте диаграммы Венна, чтобы проверить, выполняются ли следующие равенства:

1. $A \setminus (B \setminus C) = (A \setminus B) \cup C$;
2. $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.

**Ex12.** Пусть $R$ — бинарное отношение на множестве $M$. Определите, является ли $R$ рефлексивным, симметричным, антисимметричным или транзитивным в следующих случаях:

1. $M$ — множество всех людей, $xRy$ означает «$x$ — брат $y$».
2. $M = \mathbb{R}$, $xRy$ означает «$|x - y| \leqslant 1$».
3. $M$ — множество слов в словаре, $xRy$ означает «слово $x$ стоит после слова $y$».
4. $M = \mathbb{N}$, $xRy$ означает «$x$ делит $y$».

**Ex13.** Пусть $M = \{a, b, c\}$. Постройте (перечислите пары) отношение $R$ на $M$, которое является:

1. Рефлексивным, но не транзитивным;
2. Симметричным, но не рефлексивным;
3. Строгим частичным порядком (антирефлексивным и транзитивным).

**Ex14.** Нарисуйте диаграмму Хассе (граф, где $x$ соединен с $y$, если $x < y$ и не существует такого $z$, что $x < z < y$) для отношения делимости на множестве $D_{12} = \{1, 2, 3, 4, 6, 12\}$.

**Ex15.** Пусть $M = \mathbb{Z}$ (целые числа). Проверьте, являются ли следующие отношения отношениями эквивалентности. Если да, опишите классы эквивалентности.

1. $x \sim y \overset{\text{def}}{\leftrightarrow} x + y$ четно;
2. $x \sim y \overset{\text{def}}{\leftrightarrow} x^2 = y^2$;
3. $x \sim y \overset{\text{def}}{\leftrightarrow} x \leqslant y$.

**Ex16.** Основываясь на определении из Раздела A2.7 (отношение является функцией, если оно тотально и функционально), определите, какие из следующих отношений на $A = \{1, 2, 3\}$ являются функциями $f : A \to A$:

1. $R_1 = \{(1, 2), (2, 3), (3, 1)\}$;
2. $R_2 = \{(1, 2), (2, 3)\}$;
3. $R_3 = \{(1, 2), (1, 3), (2, 1), (3, 1)\}$;
4. $R_4 = \{(1, 1), (2, 1), (3, 1)\}$.

**Ex17.** На острове Рыцари всегда говорят правду, а Лжецы всегда лгут. Вы встречаете двух жителей, A и B.

1. A говорит: «По крайней мере один из нас — Лжец». Кто такие A и B?

2. А говорит: «Если В — Рыцарь, то я — Лжец». Кто такие А и В?

(Подсказка: Формализуйте утверждения, используя переменные пропозициональной логики).

**Ex18.** Определите, являются ли следующие умозаключения обоснованными.

1. Посылка 1: Если идет дождь, то улица мокрая.
   Посылка 2: Улица мокрая.
   Заключение: Следовательно, шел дождь.
2. Посылка 1: Все люди смертны.
   Посылка 2: Сократ — человек.
   Заключение: Следовательно, Сократ смертен.
3. Посылка 1: Если $x$ делится на 4, то $x$ четное.
   Посылка 2: $x$ нечетное.
   Заключение: Следовательно, $x$ не делится на 4.

**Ex19.** Классифицируйте следующие аргументы как *Дедуктивные* (выведенные из аксиом/общих правил) или *Индуктивные* (обобщенные из наблюдений):

1. «Солнце вставало на востоке каждое утро за всю известную историю. Следовательно, завтра солнце встанет на востоке.»
2. «Сумма углов всех треугольников равна 180°. Фигура ABC — треугольник. Следовательно, сумма ее углов равна 180°.»
3. «Каждое число, оканчивающееся на 0, делится на 5. Число 30 оканчивается на 0. Следовательно, 30 делится на 5».

**Ex20.** В математике $\mathscr{A} \wedge \mathscr{B}$ эквивалентно $\mathscr{B} \wedge \mathscr{A}$. Приведите пример предложения на естественном языке или команды в программировании, где перестановка частей конструкции «И» меняет смысл или вызывает ошибку.

**Ex21.** Пусть универсум равен $\mathbb{N} = \{0, 1, 2, \dots\}$. Перечислите элементы (или опишите множество), соответствующие объему (extension) следующих понятий/формул:

1. $\mathscr{A}(x) : x < 5$;
2. $\mathscr{B}(x) : \exists y \in \mathbb{N}(x = 2y)$;
3. $\mathscr{C}(x) : (x < 3) \wedge (x > 5)$;
4. $\mathscr{D}(x) : x \cdot 0 = 0$.

**Ex22.** Используя базовое отношение Отец$(x, y)$ («$x$ является отцом $y$»), запишите формальные определения (формулы) для:

1. Дед$(x, y)$ ($x$ — дед $y$);
2. Прадед$(x, y)$;
3. ОбщийОтец$(x, y)$ ($x$ и $y$ имеют общего отца).

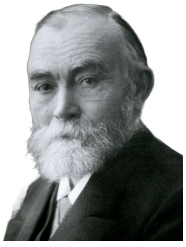
Какие это виды отношений (рефлексивное, транзитивное, симметричное, эквивалентность)?

# Формальная логика

*Боже, дай мне разум и душевный покой, принять то, что я не могу изменить, мужество изменить то, что я могу, и мудрость отличить одно от другого.*

— Молитва об умиротворении Рейнхольда Нибура

## B1.1. Логика высказываний



*Готлоб Фреге*

Формализация самой логики — превращение ее в объект математического изучения — стала ключевой задачей на рубеже XIX–XX веков. Работы Готлоба Фреге, Бертрана Рассела и Альфреда Норта Уайтхеда (особенно их фундаментальный труд «Principia Mathematica», 1910–1913) и Давида Гильберта были направлены на создание строгих аксиоматических систем для логики, что позволило бы затем на этой основе перестроить всю математику.

На уровне B1 мы начинаем обсуждение логики в строго формальном ключе, так, как это делается в учебниках. Цель такого подхода для нас заключается в том, чтобы сравнить наши предыдущие полуформальные изыскания с современным представлением о математической логике.

### B1.1.1 Язык логики высказываний

Логика (или исчисление) высказываний характеризуется тем, что в нем нет разницы между термами и формулами, поскольку предметной областью в данном случае является истинностная категория, т.е. универсум высказываний. Под высказываниями мы при этом понимаем любые выражения (без привязки к языку), каждое из которых либо истинно, либо ложно. В рамках логики высказываний предполагается, что у высказываний нет параметров, т.е. каждое высказывание имеет какое-то одно конкретное логическое значение. Таким образом, мы изучаем некий однотипный универсум, элементы которого обозначаются пропозициональными переменными $\mathscr{A}, \mathscr{B}, \ldots$, возможно, с цифровыми индексами. При этом слово «пропозициональный» обретет смысл только при рассмотрении логики предикатов — той логики, в которой предметная область перестанет быть частью истинностной категории.

Кроме того, мы используем символы логических связок $\neg, \wedge, \vee, \to$ в качестве операторных символов, с помощью которых строятся формулы логики высказываний (пропозициональные формулы, далее — формулы). Наконец, мы используем буквы $\varphi, \psi$ (возможно, с цифровыми индексами) для обозначения произвольных формул. Символы $\varphi, \psi$ называются *нетерминальными*, поскольку не участвуют в построении каждой

конкретной формулы.[1] Они нужны для того, чтобы можно было в виде единой схемы записать правила формулостроения. Если бы мы не использовали нетерминальные символы, то нам пришлось бы написать бесконечное множество правил под каждый конкретный набор формул и переменных. Такой прием часто используется в математической логике, да и в математике в целом.

Правила построения формул таковы:

1. всякая переменная есть формула;
2. если $\varphi$ и $\psi$ — формулы, то таковы же и $\neg(\varphi)$, $(\varphi) \wedge (\psi)$, $(\varphi) \vee (\psi)$, $(\varphi) \to (\psi)$;
3. любая формула построена по правилам 1 и 2.

Третий пункт в учебниках логики иногда заменяется требованием, что множество формул есть *минимальное* множество лексем, замкнутое относительно правил 1 и 2.

Итак, мы определили стартовые графемы (переменные и логические связки), а также правила их комбинирования. В результате у нас получилось бесконечное (счетное) множество правильно построенных лексем, которые мы будем называть формулами, а все множество формул обозначим за $\mathbb{L}$ и будем называть языком логики высказываний.

Попросту говоря, язык логики высказываний состоит из всех формул, которые можно построить путем комбинирования пропозициональных переменных с помощью логических связок.

Отметим, что второе правило генерации формул предписывает все операнды логических связок погружать в круглые скобки, из-за чего получаются такие неудобоваримые «колбаски», как, например:

$$(((\mathscr{A}) \to (\mathscr{B})) \wedge ((\mathscr{A}) \vee (\neg(\mathscr{B})))) \to ((\mathscr{A}) \wedge (((\mathscr{B}) \wedge (\mathscr{C})) \vee (\neg(\mathscr{D})))).$$

Чтобы упростить восприятие формул, принимаются правила редукции скобок путем обозначения приоритетов операций. Так, наивысший приоритет закрепляется за уже имеющимися скобками, далее идет $\neg$, далее $\wedge$, затем $\vee$, и последний приоритет у $\to$. Подряд идущие операции с одним приоритетом группируются в порядке слева направо. Это позволяет упростить предыдущую запись до следующего вида:

$$(\mathscr{A} \to \mathscr{B}) \wedge (\mathscr{A} \vee \neg\mathscr{B}) \to \mathscr{A} \wedge (\mathscr{B} \wedge \mathscr{C} \vee \neg\mathscr{D}).$$

Часто операторы $\wedge$ и $\vee$ считаются равноправными, и в этом случае в отсутствие скобок они выполняются слева направо. Но мы все же будем считать их похожими на арифметические операции, соответственно, $\cdot$ и $+$, чем и будет определяться их приоритет.

[1] Название «нетерминальный» заимствовано из теории формальных грамматик, где так называют символы, служащие подстановочными местами в правилах порождения строк языка. В нашем случае такие символы, как $\varphi$ и $\psi$, принадлежат *метаязыку*, которым мы описываем наш *предметный язык* $\mathbb{L}$: они не встречаются ни в одной итоговой конкретной формуле, а процесс порождения формулы остается «нетерминальным» (т.е. незавершенным), пока такие подстановочные места не заполнены. Стоит также пояснить, что поскольку предметной областью логики высказываний являются объекты истинностной категории, то и формулы, в которых все переменные оценены какими-либо высказываниями, являются высказываниями. Получается, что формулы представляют собой высказывательные термы, т.е. алгоритмы сборки более сложных высказываний из более простых. Поэтому мы здесь не различаем термы и формулы, а значит слово «нетерминальный» означает «не участвующий в записи итоговых термов и формул».

Соглашение о приоритетах позволяет однозначно восстановить все редуцированные скобки, а значит, дает возможность предъявить единственное правильное дерево разбора для всякой формулы. Например, формула

$$\mathscr{A} \vee \mathscr{B} \wedge \mathscr{C} \to \mathscr{D} \to \mathscr{A} \vee \mathscr{B} \vee \neg \mathscr{C} \wedge \mathscr{D}$$

восстанавливается до правильно построенной формулы

$$(((\mathscr{A}) \vee ((\mathscr{B}) \wedge (\mathscr{C}))) \to (\mathscr{D})) \to (((\mathscr{A}) \vee (\mathscr{B})) \vee ((\neg(\mathscr{C})) \wedge (\mathscr{D}))).$$

### B1.1.2 Аксиомы и правила вывода

После того как мы научились генерировать лексемы, соответствующие правильно построенным формулам логики высказываний (язык $\mathbb{L}$), нам следует определиться с тем, как он должен соответствовать той истинностной семантике, которую мы предполагаем в таблице истинности A2.3.

Дело в том, что хотя мы можем задать значение любой формулы по таблице истинности, действуя чисто алгебраически, как бы применяя «таблицу умножения», это наше внешнее знание не известно созданному нами языку $\mathbb{L}$, который не включает в свой алфавит ни элементы этой таблицы, ни само понятие «таблица», ни правила вычисления значений формул с помощью этой таблицы.

Поэтому над этим языком (читай, на множестве $\mathbb{L}$) мы определим своего рода демиурга истины, систему правил, состоящую из двух простых компонент: аксиомы и отношение выводимости между формулами.

Аксиомы возникают естественным для математики путем: в них мы просто фиксируем базовые свойства логических операторов, которые можем извлечь из истинностной таблицы или из тех соображений, которые в разделе A2.3 мы считали определяющими для логических связок.

Например, мы хотим, чтобы истина следовала откуда угодно, это одно из определяющих правил для материальной импликации. Тогда мы можем сказать следующее: если $\mathscr{A}$ истинно, то истинна импликация $(\mathscr{B} \to \mathscr{A})$ независимо от того, ложно или истинно $\mathscr{B}$. Это требование в нашем языке $\mathbb{L}$ мы запишем формулой

$$\mathscr{A} \to (\mathscr{B} \to \mathscr{A}) \tag{B1.1}$$

Эта аксиома формализует принцип, согласно которому истинное утверждение $(\mathscr{A})$ следует из любой посылки $(\mathscr{B})$.

Другая фундаментальная аксиома, часто называемая аксиомой Фреге, позволяет дистрибутировать импликацию:

$$(\mathscr{A} \to (\mathscr{B} \to \mathscr{C})) \to ((\mathscr{A} \to \mathscr{B}) \to (\mathscr{A} \to \mathscr{C})). \tag{B1.2}$$

По таблице истинности легко проверить, что обе формулы (B1.1) и (B1.2) являются **тавтологиями**.[2] Это подтверждает, что наш выбор аксиом корректен относительно классической истинностной семантики.

Симметричная аксиома про импликацию утверждает, что из ложной посылки следует все, что угодно, и оно записывается так:

$$\neg\mathscr{A} \to (\mathscr{A} \to \mathscr{B}). \tag{B1.3}$$

[2] Еще более научно говорят так: формула имеет оценку 1 при любых оценках переменных $\mathscr{A}$ и $\mathscr{B}$. Под оценкой понимается сопоставление переменным значений 0 или 1.

Аналогичным способом мы описываем аксиомы, например, для конъюнкции:

$$(\mathscr{A} \wedge \mathscr{B}) \to \mathscr{A}; \quad (\mathscr{A} \wedge \mathscr{B}) \to \mathscr{B},$$

которые по сути означают, что если истинна конъюнкция, то истинны ее компоненты.

Следующая аксиома позволяет дизъюнктивно соединять альтернативные посылки:

$$(\mathscr{A} \to \mathscr{C}) \to ((\mathscr{B} \to \mathscr{C}) \to (\mathscr{A} \vee \mathscr{B} \to \mathscr{C})), \tag{B1.4}$$

которая утверждает буквально, что если из $\mathscr{A}$ следует $\mathscr{C}$, то тогда если и из $\mathscr{B}$ следует $\mathscr{C}$, то уж наверняка из $\mathscr{A} \vee \mathscr{B}$ тоже следует $\mathscr{C}$.

Правило для отрицания представляет собой **закон исключенного третьего** (Tertium non datur):

$$\mathscr{A} \vee \neg\mathscr{A}, \tag{B1.5}$$

который утверждает, что для всякого высказывания существует лишь две альтернативы: либо оно само истинно, либо его отрицание истинно.

Мы не будем здесь выписывать все аксиомы логики высказываний, отсылая читателя за ними в раздел D2.1 Части II. Для общего понимания достаточно знать, что таковых аксиом существует 11 штук (в классической версии логики), все они являются тавтологиями в указанном смысле, и их набор необходим и достаточен, чтобы вывести все тавтологии языка $\mathbb{L}$.

Осталось понять, как наш демиург истины умеет производить новые истины из уже имеющихся (например, аксиом). Оказывается, у него для этого есть ровно два способа: правило подстановки и Modus Ponens.

Правило подстановки имеет вид:

$$\frac{\varphi}{\varphi[\mathscr{A}/\psi]}, \tag{B1.6}$$

где $\varphi$ — произвольная тавтология, а $\psi$ — произвольная формула языка .

Это правило работает следующим образом. Во-первых, это схема, потому что мы одной лексемой сразу задаем бесконечную серию правил вывода, каждое из которых получается из данной схемы заменой нетерминальных символов $\varphi$ и $\psi$ на конкретные формулы языка $\mathbb{L}$. Во-вторых, предположим, что у нас уже получена некоторая истинная формула $\varphi$, тогда истинной будет и формула, которая получается из $\varphi$, если в ней всюду заменить переменную $\mathscr{A}$ на формулу $\psi$ (неважно, истинную или ложную). Если в формуле $\varphi$ нет переменной $\mathscr{A}$, то таковая замена фиктивна — результатом подстановки останется формула $\varphi$. Стоит подчеркнуть, что выбор переменной $\mathscr{A}$ здесь не играет роли, вместо нее можно написать любую другую пропозициональную переменную, так что можно считать, что у нас столько схем правил подстановки, сколько переменных.

Приведем пример. Пусть $\varphi \overset{\text{def}}{=\!=} \mathscr{A} \vee \neg\mathscr{A}$ и $\psi \overset{\text{def}}{=\!=} \mathscr{A} \to \mathscr{B}$, тогда по правилу подстановки мы получим, что формула $(\mathscr{A} \to \mathscr{B}) \vee \neg(\mathscr{A} \to \mathscr{B})$ истинна, поскольку $\varphi$ такова же.

Правило подстановки легко верифицируется таблицей истинности, ведь с алгебраической точки зрения оно всего лишь говорит, что если в аргументы функции, тождественно равной 1, подставлять какие угодно функции, значение от этого не перестанет быть равным 1. Это кажется очевидным, но даже такие вещи следует программировать в прошивке нашего демиурга истины, чтобы он абсолютно точно знал, как ее *вычислять*.

Из таблицы истинности мы также легко можем понять пределы применимости правила подстановки. Если формула $\varphi$ не тождественно истинна, то подстановка в нее произвольной формулы может привести к тому, что при одних и тех же значениях переменных будет получаться разный результат вычисления у формул $\varphi$ и $\varphi[\mathscr{A}/\psi]$. Например, имея формулу $\mathscr{A} \vee \mathscr{B}$, которая истинна при $\mathscr{A} = 1$ и $\mathscr{B} = 0$, и подставляя вместо переменной $\mathscr{A}$ формулу $\mathscr{A} \wedge \neg\mathscr{A}$, мы получим формулу $(\mathscr{A} \wedge \neg\mathscr{A}) \vee \mathscr{B}$, которая при тех же значениях переменных даст ложь. Получается, что правило вывода от истинной формулы привело нас к ложной, а такие правила не имеют никакой ценности. Поэтому *применение правила подстановки всегда ограничивается только тавтологиями*.

В связи с этим часто логику высказываний формулируют вовсе без правила подстановки, но при этом аксиомы рассматривают не как отдельные формулы, а как схемы аксиом, чтобы можно было при необходимости аксиому превратить в какую-то более удобную для доказательства формулу, но заведомо истинную.

Наконец, уже известное нам правило вывода — Modus Ponens (или MP):

$$\frac{\varphi, \quad \varphi \to \psi}{\psi}, \tag{B1.7}$$

которое тоже является схемой, где вместо нетерминальных символов $\varphi$ и $\psi$ можно подставлять любые формулы языка $\mathbb{L}$.

Это правило также легко верифицируется таблицей истинности: предполагая, что значения формул $\varphi$ и $\varphi \to \psi$ истинны, легко увидеть, что в этом случае значение $\psi$ также будет истиной, каковы бы при этом ни были значения переменных, фигурирующих в этих формулах. И здесь мы видим универсальность этого правила (в отличие от подстановки) — неважно, истинные ли сами по себе входные формулы правила при тех или иных значениях переменных, выходящая формула с необходимостью будет истинной всегда, когда истинны посылки.

Комбинируя эти два правила многократно, наш демиург истины может безостановочно генерировать тавтологии, отправляясь от аксиом логики высказываний.

Более того, мы можем, наконец, полностью определить отношение выводимости $\vdash$ («штопор») на множестве формул $\mathbb{L}$.

Скажем, что из множества формул $\Gamma$ **выводится** формула $\varphi$, что будем записывать как $\Gamma \vdash \varphi$, если, отправляясь от формул из множества $\Gamma$ и аксиом, за конечное число шагов, применяя лишь правило Modus Ponens к предыдущим формулам и правило подстановки к аксиомам, можно получить формулу $\varphi$. Формулы из $\Gamma$ в таком случае называются *гипотезами* или *посылками вывода*.

Заметим, что в этом определении мы прибегли к теоретико-множественному понятию, указав, что $\Gamma$ есть подмножество языка $\mathbb{L}$, т.е. некоторое множество правильно построенных формул. Но в силу конечности вывода в каждом конкретном случае вместо $\Gamma \vdash \varphi$ можно записать выражение $\psi_1, \dots, \psi_n \vdash \varphi$, не требующее теоретико-множественной коннотации.

Если множество гипотез $\Gamma$ пусто, то вывод $\Gamma \vdash \varphi$ представляет собой вывод из чистой аксиоматики логики высказываний. Формула, выведенная только из аксиом, называется **теоремой**. Если $\Gamma$ пусто, то вместо $\Gamma \vdash \varphi$ пишут короче: $\vdash \varphi$.

Покажем для примера вывод такой теоремы: $\mathscr{A} \to \mathscr{A}$. Напишем следующую последовательность формул, каждая из которых есть либо аксиома, либо получается из предыдущих формул по одному из двух правил вывода:

1. $(\mathscr{A} \to ((\mathscr{A} \to \mathscr{A}) \to \mathscr{A})) \to ((\mathscr{A} \to (\mathscr{A} \to \mathscr{A})) \to (\mathscr{A} \to \mathscr{A}))$ [подстановка в аксиому (B1.2): $\mathscr{B}/(\mathscr{A} \to \mathscr{A}), \mathscr{C}/\mathscr{A}$];

2. $\mathscr{A} \to ((\mathscr{A} \to \mathscr{A}) \to \mathscr{A})$ [аксиома (B1.1) с подстановкой $\mathscr{B}/(\mathscr{A} \to \mathscr{A})$];

3. $(\mathscr{A} \to (\mathscr{A} \to \mathscr{A})) \to (\mathscr{A} \to \mathscr{A})$ [из 1. и 2. по правилу Modus Ponens];

4. $\mathscr{A} \to (\mathscr{A} \to \mathscr{A})$ [аксиома (B1.1) с подстановкой $\mathscr{B}/\mathscr{A}$];

5. из 3. и 4. по правилу Modus Ponens получаем $\mathscr{A} \to \mathscr{A}$. Готово!

Существование такого вывода коротко записывается так: $\vdash \mathscr{A} \to \mathscr{A}$.

Любой вывод $\Gamma \vdash \varphi$ можно изобразить в виде дерева, в котором корнем является полученная формула $\varphi$, листьями — аксиомы и/или гипотезы из $\Gamma$, промежуточными узлами — выведенные по пути формулы, а ребра отвечают правилам вывода (в случае правила подстановки используется одно ребро, в случае Modus Ponens — два.)

Дерево вывода теоремы $\mathscr{A} \to \mathscr{A}$ представлено на рис. B1.1.

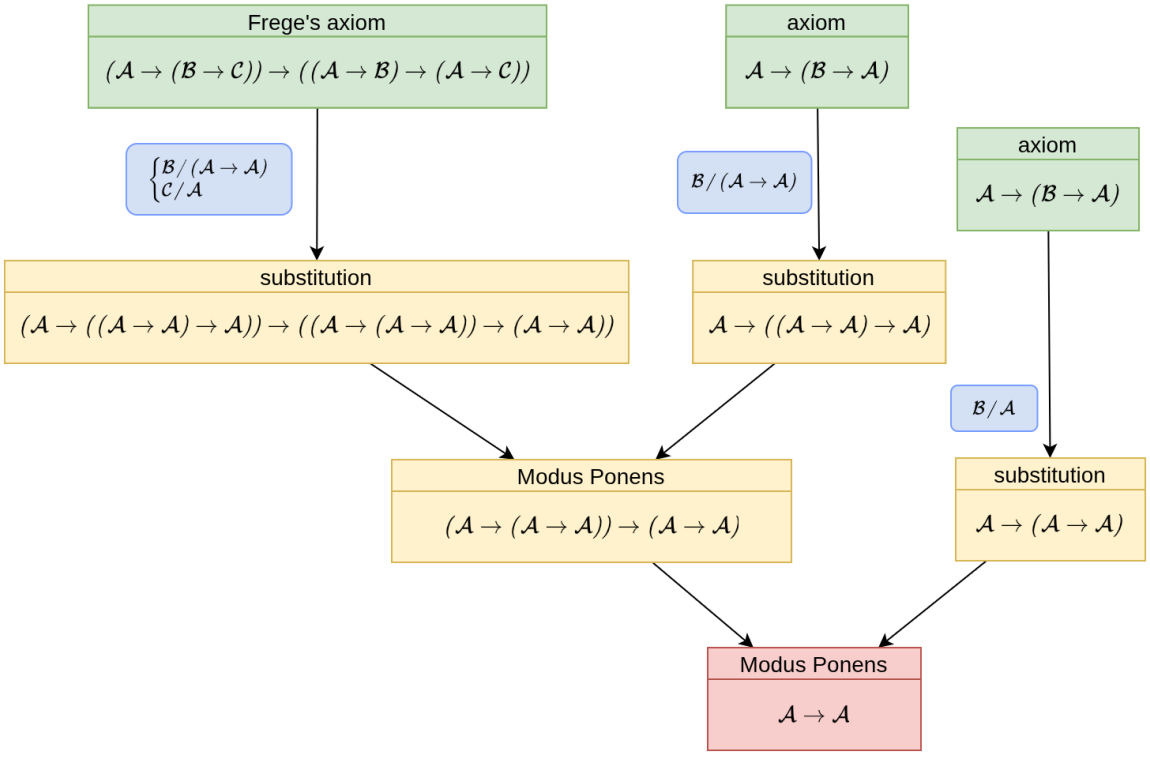



Рис. B1.1. Пример дерева вывода

## B1.1.3 Основные факты о логике высказываний

### Корректность и полнота вывода

Первое, что стоит отметить, любая теорема логики высказываний, является тавтологией, т.е. при замене переменных в ней на значения 0 или 1, следуя таблице истинности A2.3, всегда получается 1. Это свойство логики называется **корректностью** (оно означает, что «штопор нам не врет»).

Верно и обратное: если какая-то формула логики высказываний является тавтологией (тождественно истинна как функция от 0 и 1), то она является теоремой логики высказываний. Это свойство логики называется **полнотой**, но следует уточнить, что это

свойство отношения выводимости $\vdash$, чтобы не путать этот термин с другими вариантами полноты (см. ниже).

## Про мета-теорию

Второй важный факт, который мы можем наблюдать: все определения понятий, а также процессов генерации формул и построения выводов, даются нами не внутри логики $\mathbb{L}$, а во вне ее, т.е. в некоторой мета-теории, при помощи которой все эти понятия формализуются как математические понятия. Эта мета-теория должна быть достаточно богатой, чтобы оперировать такими вещами, как множества (конечные и некоторые счетные), функции (на конечных множествах) и рекурсивные определения. В качестве такой мета-теории можно рассматривать различные формальные теории, позволяющие все это запрограммировать внутри себя. К таковым относятся некоторые ослабленные варианты теории множеств и арифметики Пеано.

Иначе говоря, когда мы создаем какой-то формализм, пусть даже самый примитивный, мы создаем его не на пустом месте, а в рамках некоторой «обычной» математики, которая также допускает формализацию, причем в относительно слабых формах (слабых с точки зрения умения что-либо доказывать).

Соответственно, свойства логики высказываний, такие как корректность, полнота и многие другие (см. ниже), доказываются в рамках *этой* мета-теории, они не являются теоремами самой логики высказываний. Такие теоремы часто принято называть мета-теоремами (относительно данного формализма).

Поэтому, изучая формальные теории, математик работает одновременно на трех уровнях абстракции: формальном (внутри изучаемого формализма), мета-уровне (внутри мета-теории, но вне формализма) и общем (на котором он поясняет свое творчество, привлекая разговорный язык и разного рода аллюзии и аллегории).

## Теорема о дедукции

**Теорема B1.1** (о дедукции). *Пусть $\varphi_1, \dots, \varphi_n, \psi$ — формулы из $\mathbb{L}$. Тогда*

$$\varphi_1, \dots, \varphi_n \vdash \psi \quad \Leftrightarrow \quad \vdash (\varphi_1 \wedge \dots \wedge \varphi_n) \to \psi.$$

Иными словами, существует вывод формулы $\psi$ тогда и только тогда, когда соответствующая импликация является тавтологией. Естественно, в рамках аксиоматики логики высказываний. Заметим, что здесь мы использовали знак $\Leftrightarrow$ вместо $\leftrightarrow$, т.к. приведенное утверждение является мета-теоремой, а не формулой языка $\mathbb{L}$.

## Функциональная полнота

Таблица истинности, к которой мы часто апеллируем, позволяет вычислить значение любой формулы логики высказываний при заданных значениях переменных. В частности, для любой формулы можно проверить, является ли она тавтологией (тожественной истиной) или нет. Проблема в том, что проверка формулы на тавтологичность является проблемой класса NP в общем случае, т.е. не решается за полиномиальное время относительно количества переменных. Для огромных формул это очень длительный вычислительный процесс. В то же время получение тавтологий путем применения правил вывода — процесс достаточно простой и быстрый. Но есть нюанс: если вам *дана*

произвольная формула, то задача проверки ее на тавтологичность как функциональным способом (по таблице истинности), так и поиском вывода может быть одинаково трудоемкой.

Поэтому, рассматривая логику как исчисление, т.е. систему правил вывода и аксиом, мы не сбрасываем со счетов и ее функциональную интерпретацию. Более того, между этими двумя подходами существует очень тесная связь, которая называется **функциональной полнотой**. Теорему о функциональной полноте логики высказываний мы даем во второй части книги (см. раздел D2.1). В упрощенном виде ее можно озвучить так: всякой формуле соответствует таблица истинности и наоборот, всякой таблице истинности соответствует некоторая формула.

Функциональная полнота позволяет ввести на множестве $\mathbb{L}$ отношение равносильности. Скажем, что формулы $\varphi$ и $\psi$ **равносильны**, обозначая это как $\varphi \equiv \psi$, если они имеют одинаковые таблицы истинности. Например,

$$\mathscr{A} \to \mathscr{B} \equiv \neg\mathscr{B} \to \neg\mathscr{A}; \quad \text{но(!)} \quad \mathscr{A} \to \mathscr{B} \not\equiv \neg\mathscr{A} \to \neg\mathscr{B}.$$

Во второй части книги мы приводим целый ряд полезных равносильностей формул, здесь же дадим только законы де Моргана:

$$\neg(\mathscr{A} \vee \mathscr{B}) \equiv \neg\mathscr{A} \wedge \neg\mathscr{B}; \quad \neg(\mathscr{A} \wedge \mathscr{B}) \equiv \neg\mathscr{A} \vee \neg\mathscr{B},$$

закон двойного отрицания:

$$\neg\neg\mathscr{A} \equiv \mathscr{A},$$

а также выражение эквиваленции через импликацию:

$$\mathscr{A} \leftrightarrow \mathscr{B} \equiv (\mathscr{A} \to \mathscr{B}) \wedge (\mathscr{B} \to \mathscr{A}).$$

Не лишним будет упомянуть и законы дистрибутивности для $\wedge$ и $\vee$:

$$\mathscr{A} \wedge (\mathscr{B} \vee \mathscr{C}) \equiv (\mathscr{A} \wedge \mathscr{B}) \vee (\mathscr{A} \wedge \mathscr{C}), \quad \mathscr{A} \vee (\mathscr{B} \wedge \mathscr{C}) \equiv (\mathscr{A} \vee \mathscr{B}) \wedge (\mathscr{A} \vee \mathscr{C}).$$

Пользуясь теоремой о дедукции и таблицей истинности для эквиваленции, можно получить следующую мета-теорему.

**Теорема B1.2.**

$$\varphi \equiv \psi \quad \Leftrightarrow \quad \vdash \varphi \leftrightarrow \psi \quad \Leftrightarrow \quad \varphi \dashv\vdash \psi,$$

*где последнее означает взаимную выводимость формул друг из друга.*

## Пример из жизни

Предположим, что мы хотим спроектировать систему включения/выключения освещения из двух мест. Мы можем начать с построения соответствующей логической формулы.

Пусть $\mathscr{S}_1$ и $\mathscr{S}_2$ — переменные, выражающие состояние первого и второго выключателя, соответственно. У выключателей есть два состояния: 0 и 1. Пусть $\varphi$ задает состояние лампочки (1 — горит, 0 — не горит). Определим таблицу истинности для $\varphi$ так, что свет горит, если оба выключателя в одинаковых положениях, и не горит, если в разных (см. слева). Таким образом, изменение состояния любого из выключателей приводит к изменению состояния лампочки.

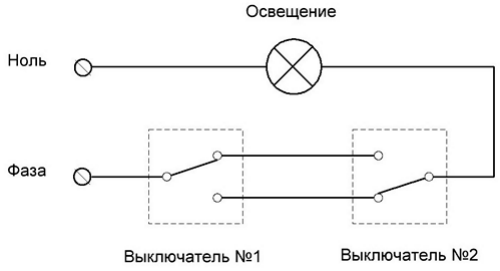
| $\mathscr{S}_1$ | $\mathscr{S}_2$ | $\varphi$ |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

Чтобы найти формулу $\varphi$, вспомним таблицу истинности A2.3 для $\leftrightarrow$, из которой легко видеть, что $\varphi \equiv (\mathscr{S}_1 \leftrightarrow \mathscr{S}_2)$. Отсюда, раскладывая эту эквиваленцию в дизъюнктивную нормальную форму (выбирая строки, где $\varphi = 1$), находим, что:

$$\varphi \equiv (\neg\mathscr{S}_1 \wedge \neg\mathscr{S}_2) \vee (\mathscr{S}_1 \wedge \mathscr{S}_2).$$

Здесь $\wedge$ соответствует последовательному соединению, а $\vee$ — параллельному. Из этих соображений получается такая схема (см. справа).

В качестве упражнения предлагается подумать над схемой включения из трех мест.




### Логические константы

В предыдущей главе мы использовали символы-константы $\top$ (истина) и $\bot$ (ложь). Здесь же, следуя классическому изложению логики, мы их пропустили для упрощения языка. Настало время вернуть их в оборот. Положим по определению

$$\top \rightleftharpoons^{\text{def}} \mathscr{A} \vee \neg\mathscr{A}; \quad \bot \rightleftharpoons^{\text{def}} \mathscr{A} \wedge \neg\mathscr{A}.$$

Легко проверить, что первая формула есть тавтология, а вторая формула есть тождественная ложь. При этом, на самом деле, неважно, какая пропозициональная переменная тут использована, значение формул останется тем же.

Для констант можно вывести, например, такие равносильности:

$$\top \wedge \mathscr{A} \equiv \mathscr{A}; \quad \top \vee \mathscr{A} \equiv \top; \quad \bot \wedge \mathscr{A} \equiv \bot; \quad \bot \vee \mathscr{A} \equiv \mathscr{A}.$$

Кроме того, можно заметить, что формула является тавтологией тогда и только тогда, когда она равносильна $\top$.

## B1.2. Логика предикатов

В разделе A2.3 мы уже имели дело с предикатами и термами, но наше повествование носило весьма неформальный характер. Теперь же настало время подвести прочную базу под все те идеи, которые были изложены ранее.

В разделе A2.7 мы подчеркивали, что существует тонкая, но важная разница между синтаксическим объектом (предикатным символом или формулой) и его семантической интерпретацией (отношением). В строгой логике эти понятия разделяют. Однако в математической практике, когда семантика зафиксирована и понятна из контекста, символ часто отождествляют с его значением.

Далее в этой книге мы будем придерживаться следующего подхода: при обсуждении общих свойств формальных языков мы будем различать *предикатный символ* (синтаксис) и *отношение* (семантика). Однако в контексте конкретных теорий (арифметики, теории множеств), где интерпретация символов очевидна, мы, следуя общепринятой математической традиции, для удобства будем использовать слово «предикат» для обозначения и самой формулы, и того свойства или отношения, которое она выражает. Это позволит сделать изложение более естественным и менее громоздким.

Таким образом, мы можем рассматривать каждый конкретный **предикат** как полноценное *математическое понятие*. Его обозначением является предикатный символ (графема) логического типа, определением служит либо прямое определение формулой, либо список формул, содержащих данный предикатный символ (косвенное определение через аксиомы). Объемом этого понятия в каждой конкретной семантике выступает соответствующее ему отношение. У каждого предиката обычно есть собственное название.

Предикатный символ, в подстановочные места которого подставлены допустимые термы рассматриваемого языка, называется *атомарной формулой*.

Наличие собственного обозначения у предикатов позволяет отделять атомарные формулы от произвольных формул (которые тоже задают отношения).

### B1.2.1 Термы

Пусть у нас имеется некоторая однородная предметная область, общим обозначением объектов которой являются переменные $a, b, c, \dots, x, y, z$. В силу однородности все эти переменные имеют один тип, так что их можно свободно заменять друг на друга без согласования типов. Если в предметной области предполагается, как сейчас, только один тип (или род) объектов, то такую предметную область называют *бестиповой*.

Переменные принято разделять на два класса: *свободные* и *связанные*. К свободным переменным обычно относят буквы из начала алфавита, к связанным — из конца алфавита. Мы также будем использовать цифровые индексы у переменных, чтобы сделать текст более комфортным для восприятия.[3]

Помимо переменных мы можем использовать символы-константы, которые закреплены за какими-то конкретными объектами (например, 0 и 1 в случае арифметики или числа $\pi$ и $e$ в случае Анализа). Множество всех символов-констант обозначим за $\mathfrak{C}$.

Далее, нам нужны **функциональные символы**, которые обозначают некоторые базовые операции на универсуме объектов. В разделе A2.3 мы вводили обозначения для теоретико-множественных операций: $\cap, \cup, \setminus$ и т.п. В арифметике это будут операции сложения и умножения. Функциональные символы играют такую же роль в строении термов, какую роль играют логические связки в строении формул. За функциональными символами мы закрепим следующие обозначения $F, F_1, F_2 \dots$ . Следует отметить, что для каждого функционального символа необходимо также указывать его арность, т.е. количество подстановочных мест. Обычно это делается приписыванием следом за функциональным символом свободных переменных в круглых скобках в необходимом количестве, например, $F(a, b, c)$. Аналогичным способом программист задает функцию с аргументами.[4] Множество всех функциональных символов обозначим за $\mathfrak{F}$.

Обычно считается, что $\mathfrak{C} \subseteq \mathfrak{F}$, поскольку константы можно считать 0-арными функциями.

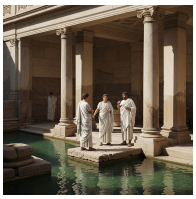
Нетерминальные символы $T_1, T_2, \dots$ будем использовать как общие обозначения термов (аналог обозначений $\varphi$ и $\psi$ для произвольных формул)

Правила построения **термов** таковы:

[3] Более строгий подход предписывает указать рекурсивное правило формирования новых имен переменных, например, добавлением штриха.

[4] Если бы предметная область содержала два и более различных типов объектов, то прописывание свободных переменных следом за функциональным символом заодно указывало бы и на тип данного подстановочного места, поскольку все переменные мы тоже разделили бы по типам.

1. всякая свободная переменная есть терм;
2. всякая константа есть терм;
3. если $F$ — функциональный символ арности $n$, а $T_1, \ldots, T_n$ — произвольные термы, то выражение $F(T_1, \ldots, T_n)$ есть терм;
4. любой терм построен по правилам 1–3.



*Термы*

Итак, в области термостроения мы наблюдаем все тот же рекурсивный процесс: начальными (наименьшими термами) являются свободные переменные и константы, а все остальные термы получаются путем комбинирования уже готовых термов с функциональными символами.

Например, $(a+b)\cdot c$ есть арифметический *терм* (а не формула!). Правда, в данном примере нужно отметить, что вместо символов $F_1(a,b)$ и $F_2(a,b)$ мы используем более привычные $a+b$ и $a\cdot b$. Такие вольные обозначения не используются в общем случае, когда мы изучаем произвольный формализм, но в каждом конкретном формализме они встречаются постоянно, что мы в дальнейшем и увидим. Сейчас просто отметим, что операция $F(a,b)$ может в каждом конкретном случае иметь достаточно произвольную запись ($a+b$, $a \in b$, $a^b$, $a/b$ и т.п.).

Терм называется *замкнутым*, если он не содержит свободных переменных. Например, константы, а также композиция функциональных символов и констант не содержит свободных переменных и фактически является алгоритмом построения какого-либо конкретного объекта в предметной области (например, $((1+1)\cdot 0)+1$).

Незамкнутый терм содержит свободные переменные и фактически описывает алгоритм построения функции, преобразующей один или несколько объектов в один объект предметной области (например, $(a+b)\cdot c$).

## B1.2.2 Формулы

Символы $P, Q, P_1, Q_1, P_2, Q_2 \ldots$ назовем предикатными символами. Их семантическое отличие от функциональных символов состоит в том, что они преобразуют объекты в истинностную категорию, т.е. участвуют не в термо-, а в формулостроении. Для предикатных символов также требуется указывать арность путем перечисления свободных переменных в нужном количестве, например, $P(a,b,c)$. Множество всех предикатных символов обозначим за $\mathfrak{P}$.

Набор множеств $\mathfrak{P}, \mathfrak{F}, \mathfrak{C}$ называется **сигнатурой** формального языка логики предикатов и обычно обозначается буквой $\Sigma$.

Нетерминальные символы $\varphi$ и $\psi$ (возможно, с цифровыми индексами и указанием в скобках свободных переменных) мы будем использовать в качестве обозначений произвольных формул.

Правила построения **формул** в логике предикатов таковы:

1. если $P$ — предикатный символ арности $n$, а $T_1, \ldots, T_n$ — произвольные термы, то выражение $P(T_1, \ldots, T_n)$ есть формула (называемая атомарной);
2. если $\varphi$ и $\psi$ — формулы, то таковы же $\neg(\varphi)$, $(\varphi)\wedge(\psi)$, $(\varphi)\vee(\psi)$, $(\varphi)\to(\psi)$, а также, если текст формулы $\varphi$ не содержит переменной $x$, то

$$\forall x\ (\varphi[a/x]), \quad \exists x\ (\varphi[a/x])$$

суть формулы, где $[a/x]$ означает замену всех вхождений свободной ременной $a$ в формуле $\varphi$ на связанную переменную $x$.[5]

3. любая формула построена по правилам 1–2.

Здесь мы практически повторили определение формул логики высказываний, только вместо пропозициональных переменных использовали предикатные символы, а к логическим операциям добавили кванторы. Из-за кванторов нам понадобилось деление переменных на свободные и связанные. Но такой шаг является очень скромной платой за то, чтобы не объяснять, что такое коллизии переменных под кванторами (хотя мы это уже успели немного обсудить на стр. 38 в разговоре о лексемах-свертках).

Строение термов и формул полностью укладывается в принципы строения лексем (в частности, принцип матрешки), о которых мы говорили в разделе A1.2. Так что все термы и формулы — это правильно построенные лексемы языка Math, имеющие деревья разбора. Кроме того, всякая формула имеет четыре абстрактных уровня строения: объектные переменные и константы, функциональные символы, предикатные символы, логические связки и кванторы (рис. B1.2).

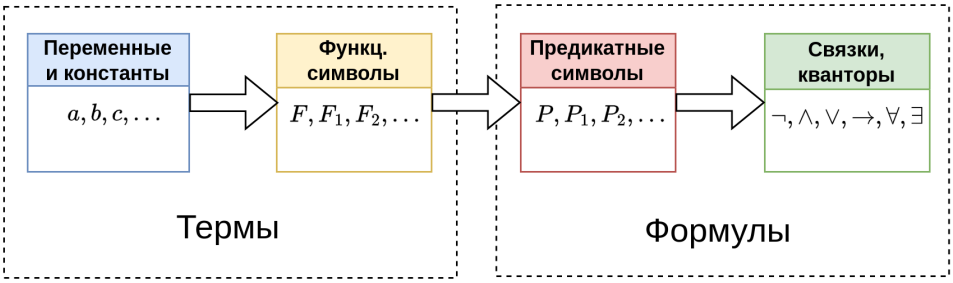



Рис. B1.2. Уровни дерева разбора формулы

Примеры формул логики предикатов:

$$P(a,b,0), \quad P(a+b, b\cdot c, 1) \wedge Q(a,0,1), \quad \exists x \forall y\ P(x,y,a) \rightarrow \forall y \exists x\ P(x,y,a),$$

где $P$ и $Q$ — некоторые тернарные предикатные символы.

Здесь, как и в логике высказываний мы используем приоритеты логических операторов для редуцирования скобок, но в случае формулы, стоящей под квантором, рекомендуем делать это с осторожностью, только в самых очевидных случаях. Формула, стоящая в скобках под квантором, является *областью действия* этого квантора, а при снятии скобок иногда бывает затруднительно определить, где эта область заканчивается.

Отметим, что если из определения формул убрать использование кванторов, то все формулы можно описать еще проще. Это все, что получается из формул логики высказываний, если пропозициональные переменные заменить атомарными формулами. Такие формулы называются *бескванторными*, их текст не содержит связанных переменных.

[5] Строго говоря, нужно было бы использовать нетерминальные символы $A$ и $X$ для обозначения *произвольных* свободной и связанной переменной, чтобы не создалось впечатление, будто только конкретную букву $a$ можно заменять на конкретную букву $x$.

Более того, если предположить, что в нашем языке есть лишь один предикатный символ — пустой, и нет функциональных символов, т.е. всякая атомарная формула имеет вид $(a)$, где $a$ — свободная переменная, то бесквантерные формулы — это в точности формулы логики высказываний.

Формула называется **замкнутой**, если ее текст не содержит свободных переменных. *Универсальным замыканием* формулы называется замкнутая формула, в которой все свободные переменные закрыты кванторами всеобщности ($\forall$). Например, формула $\forall x \forall y\ P(x,y)$ есть универсальное замыкание формулы $P(a,b)$, где $P$ — бинарный предикатный символ.

Далее нам потребуются обозначения: $\mathbb{F}$ — множество всех формул, $\mathbb{T}$ — множество всех термов. Ясно, что наполнение этих множеств варьируется в зависимости от того, какие конкретно функциональные символы, константы и предикатные символы мы используем.

Множество всех формул $\mathbb{F}$ называется **формальным языком первого порядка**.[6]

### B1.2.3 Аксиомы и правила вывода логики предикатов

Следуя общей логике построения логик, займемся теперь определением истинностного базиса, т.е. аксиом логики предикатов, а также отношения выводимости на множестве формул $\mathbb{F}$.

Аксиомами логики предикатов (*логическими аксиомами*) являются следующие формулы:

PC1 универсальные замыкания всех подстановок всех формул из $\mathbb{F}$ во все тавтологии логики высказываний;

PC2 аксиомы для кванторов:

$$(\forall x\ \varphi[a/x]) \to \varphi[a/T]; \quad \varphi[a/T] \to \exists x\ \varphi[a/x],$$

где $\varphi$ — любая формула из $\mathbb{F}$, не содержащая связанную переменную $x$, $T$ — любой терм из $\mathbb{T}$. Здесь, как и ранее, мы предполагаем, что вместо $a$ можно иметь в виду любую свободную переменную, а вместо $x$ — любую связанную переменную, отсутствующую в формуле $\varphi$.

В первом пункте мы фактически указали бесконечный перечень аксиом, который определяется множествами $\mathbb{L}$ (точнее его подмножеством, состоящим из тавтологий) и $\mathbb{F}$. Его можно было бы выразить более формально, если бы мы использовали нетерминальные символы-переменные, пробегающие по всем формулам логики высказываний, всем пропозициональным переменным и всем формулам из $\mathbb{F}$. Требование универсального замыкания сообщает нам о том, что в качестве аксиом мы хотим видеть только замкнутые формулы, т.к. они соответствуют понятию высказывания. Однако часто аксиомы пишутся как формулы со свободными переменными, но при этом подразумевается, что их нужно замкнуть кванторами всеобщности.

[6] Существуют т.н. языки (логики) высших порядков, которые мы здесь не рассматриваем. Например, в логике второго порядка наши нетерминальные символы $\varphi, \psi$ инкапсулированы в качестве переменных по всем первопорядковым свойствам (т.е. становятся терминальными), что допускает использовать формулы второго порядка, содержащие кванторы по свойствам и функциям первого порядка. И т.д.

Кванторные аксиомы говорят примерно следующее: если формула $\varphi$ истинна при любом значении $a$, то вместо $a$ можно подставить любой терм; если какой-то терм является свидетелем формулы $\varphi$, то существует такое значение $a$, при котором формула $\varphi$ истинна. Здесь мы уже не требуем замкнутости формул, чтобы оставить поле для маневра: позволить навесить квантор существования или снять квантор всеобщности.

Правила вывода:

$$(MP)\quad \frac{\varphi,\quad \varphi \to \psi}{\psi};\qquad (R1)\quad \frac{\varphi \to \psi}{\varphi \to \forall x\ \psi[a/x]};\qquad (R2)\quad \frac{\psi \to \varphi}{(\exists x\ \psi[a/x]) \to \varphi},$$

где для правил $(R1)$ и $(R2)$ переменная $a$ не входит в формулу $\varphi$. $(R1)$ и $(R2)$ называются **правилами Бернайса**. Как обычно замечаем, что под $a$ здесь подразумевается любая свободная переменная, а под $x$ — любая связанная переменная.

В правилах вывода мы также не требуем, чтобы формулы были замкнутыми, поскольку навешивать кванторы можно только на формулу со свободной переменной.

Говорим, что множество гипотез $\Gamma \subseteq \mathbb{F}$ **выводит** формулу $\varphi$, обозначая это $\Gamma \vdash \varphi$, если отправляясь от формул из $\Gamma$ и аксиом, за конечное число шагов по правилам вывода можно получить формулу $\varphi$. В случае пустого множества $\Gamma$, т.е. когда формула $\varphi$ выводится только из аксиом логики предикатов, пишем просто $\vdash \varphi$.

**Теорема B1.3** (свойства выводимости)**.**

1° *(монотонность) если* $\Delta \subseteq \Gamma$ *и* $\Delta \vdash \varphi$*, тогда* $\Gamma \vdash \varphi$*;*

2° *(компактность) если* $\Gamma \vdash \varphi$*, то существует конечное подмножество* $\Delta \subseteq \Gamma$ *такое, что* $\Delta \vdash \varphi$*;*

3° *(транзитивность) если* $\Gamma \vdash \varphi$ *для всех* $\varphi \in \Delta$ *и* $\Delta \vdash \psi$*, то* $\Gamma \vdash \psi$*.*

**Теорема B1.4** (о дедукции)**.**

$$\Gamma \cup \{\varphi\} \vdash \psi \quad \Leftrightarrow \quad \Gamma \vdash (\varphi \to \psi).$$

*Техническое ограничение: в направлении слева направо при выводе формулы* $\psi$ *из* $\Gamma \cup \{\varphi\}$ *свободные переменные формулы* $\varphi$ *не участвуют в правилах обобщения (не замыкаются кванторами).*

*Замечание*: вместо $\Gamma \cup \{\varphi\}$ чаще всего пишут $\Gamma, \varphi$ или $\Gamma + \varphi$. Доказательство этой теоремы можно найти, например, в [42].

Теорема о дедукции, связывающая выводимость и импликацию, является важным металогическим результатом. Она была независимо доказана Жаком Эрбраном (1930) и Альфредом Тарским (в работах 1920-30-х годов). Эта теорема — удобный способ заменять вывод на импликацию, и наоборот. Часто она позволяет сильно сократить формальное доказательство теоремы.

Настало время дать точные определения таким математическим понятиям, как теория, аксиома и теорема.

**Теорией** называется множество замкнутых формул, замкнутое относительно отношения выводимости. Формулы теории называются **теоремами**. Для теории можно выделить порождающее (в смысле выводимости) подмножество формул, которое принято называть **аксиоматикой** этой теории, а его элементы — **аксиомами**. При этом желательно, чтобы аксиомы были *независимыми*, т.е. чтобы никакую из них нельзя было

вывести из прочих. На практике (чаще всего в силу традиции) оказывается, что аксиомы теории могут быть частично зависимыми. Тем не менее, аксиоматику стараются выбирать как можно более компактной.[7]

Если в качестве аксиоматики теории взять лишь аксиомы логики предикатов, то соответствующая теория (множество всех выведенных замкнутых формул) состоит из *теорем логики предикатов* и называется *чистой теорией предикатов*. Ясно, что такая теория зависит от языка $\mathbb{F}$, т.е. от набора функциональных и предикатных символов. Поэтому в отличие от логики высказываний существует огромное разнообразие конкретных чистых теорий предикатов.

Заметим, что поскольку аксиомы логики предикатов всегда участвуют в любом выводе по умолчанию, то когда речь идет об *аксиоматике теории*, обычно имеют в виду только *нелогические аксиомы*, т.е. формулы, не являющиеся теоремами чистой теории предикатов.

Дальнейшее изучение теорий требует введения понятия модели, которое мы рассмотрим чуть позже, а пока рассмотрим пару простых примеров языка и теории.

## B1.2.4 Примеры теорий

### Теория строгих частичных порядков

Рассмотрим язык $\mathbb{F}$, в котором есть только один бинарный предикатный символ $<$ и нет функциональных символов и констант. Вместо $<(a,b)$ будем писать $a < b$. Атомарные формулы в таком языке имеют вид $(a < b)$. Теорию строгих частичных порядков зададим с помощью двух нелогических аксиом:

$$\neg(a < a); \quad (a < b) \wedge (b < c) \to (a < c),$$

первая из которых называется аксиомой антирефлексивности, а вторая — аксиомой транзитивности. По традиции мы не используем универсальное замыкание на аксиомах, однако подразумеваем его. В этой теории можно доказать, например, такую теорему:

$$(a < b) \to \neg(b < a).$$

Действительно, предположим обратное, т.е. что верно отрицание данной импликации $\neg((a < b) \to \neg(b < a))$, после чего воспользуемся логикой высказываний, в которой имеет место равносильность $\neg(\mathscr{A} \to \neg\mathscr{B}) \equiv \mathscr{A} \wedge \mathscr{B}$. Тогда из нашей гипотезы следует формула $(a < b) \wedge (b < a)$, откуда из аксиомы транзитивности получаем, что $a < a$, а это вместе с аксиомой $\neg(a < a)$ выводит $\bot$. Следовательно, одна из гипотез не верна.

Но нашими гипотезами были только две аксиомы и предположение $\neg((a < b) \to \neg(b < a))$, т.е. мы имеем вывод:

$$\varphi_1, \varphi_2, \neg\psi \vdash \bot,$$

где $\varphi_i$ — аксиомы, $\psi \overset{\text{def}}{\rightleftharpoons} (a < b) \to \neg(b < a)$. По теореме о дедукции получаем, что $\varphi_1, \varphi_2 \vdash \neg\psi \to \bot$, откуда с помощью логики высказываний получаем, что $\varphi_1, \varphi_2 \vdash \psi$, поскольку $\neg\mathscr{A} \to \bot \equiv \mathscr{A}$.

[7] Аксиомы являются теоремами в силу данных определений. Это удобно, т.к. всякая аксиома умеет доказывать саму себя в силу тавтологии $\varphi \to \varphi$.

По сути мы провели здесь формальное доказательство от противного в рамках заданной аксиоматики.

## Чистая теория равенства

Рассмотрим язык $\mathbb{F}$, в котором есть только один бинарный предикатный символ $=$ и нет функциональных символов и констант. Вместо $=(a,b)$ будем писать $a=b$. Атомарные формулы в таком языке имеют вид $(a=b)$. Теорию чистого равенства зададим с помощью трех нелогических аксиом:

$$a=a;\quad (a=b)\to(b=a);\quad (a=b)\wedge(b=c)\to(a=c), \tag{B1.8}$$

которые мы пишем без универсального замыкания и которые выражают свойства рефлексивности, симметричности и транзитивности равенства.

При использовании предиката равенства вместе с ним обычно используется и предикат неравенства $a\neq b$, который определяется как $\neg(a=b)$.

Теория равенства занимает одно из центральных мест в логике предикатов, поскольку равенство входит в подавляющее число формальных теорий, и всякий раз, когда мы включаем в язык предикат равенства, мы автоматически подразумеваем наличие в теории аксиом равенства так же, как мы автоматически подразумеваем наличие логических аксиом.

Более того, помимо аксиом чистого равенства мы также добавляем аксиомы конгруэнтности, которые сообщают нам о том, что замена равного на равный терм не меняет значения ни терма, ни предиката. Об этом см. чуть ниже.

## Теория полугрупп

Рассмотрим язык $\mathbb{F}$, в котором есть один бинарный предикатный символ $=$ и один функциональный символ $\circ$. Вместо $=(a,b)$ и $\circ(a,b)$ будем писать $a=b$ и $a\circ b$. Теория полугрупп определяется следующим списком нелогических аксиом: аксиомы равенства (B1.8), а также:

$$(a\circ b)\circ c=a\circ(b\circ c);\quad (T_1=T_2)\wedge(T_3=T_4)\to(T_1\circ T_3)=(T_2\circ T_4),$$

где $T_i\in\mathbb{T}$, т.е. являются произвольными термами языка теории полугрупп (т.е. это всевозможные комбинации переменных и операции $\circ$).

Первая аксиома является собственно аксиомой полугруппы и говорит нам об ассоциативности операции $\circ$, а вторая является примером *аксиомы конгруэнтности*, она говорит, что под знаком операции $\circ$ можно свободно заменять равные термы друг на друга, значение операции при этом не изменится (относительно равенства). Без аксиомы конгруэнтности многие привычные нам выкладки тождественных преобразований оказались бы просто невозможными.

Из аксиомы ассоциативности для трех переменных и аксиомы конгруэнтности можно вывести общий закон ассоциативности для произвольных $n$ переменных, который словами выражается так: порядок расстановки скобок в записи $x_1\circ\ldots\circ x_n$ не важен (и, значит, скобки можно вообще не писать). Формально же это придется записывать как множество тождеств со всеми правильными расстановками скобок для каждого конкретного $n$ (поскольку в этой теории нет натуральных чисел).

Чистая теория полугрупп является для нас хорошим примером формализма, включающего все необходимые компоненты: и логику предикатов, и функциональный символ, и теорию равенства с аксиомой конгруэнтности.

Формальную теорию полугрупп не следует путать с алгебраической теорией полугрупп, которая по сути занимается изучением класса моделей полугрупп и всевозможных морфизмов между ними.

### B1.2.5 Конгруэнтность равенства

**Конгруэнтность равенства** означает свойство логики не различать равные объекты. То есть если мы однажды выяснили, что два объекта равны в смысле предиката равенства, то они могут быть взаимозаменяемыми в любых термах и формулах. Иначе говоря, перефразируя известную фразу, если что-то является уткой, то оно выглядит как утка, плавает как утка и крякает как утка. Таким образом за предикатом равенства закрепляется свойство различать только такие объекты, которые способен различить данный формализм. По сути, равенство — это самый низкий уровень различия предметов, который способен предоставить формальный язык.[8]

Формально **аксиомы конгруэнтности** в общем виде формулируются следующим образом. Пусть $T, T_1, T_2 \in \mathbb{T}$ — произвольные термы и $\varphi \in \mathbb{F}$ — произвольная формула, тогда

$$T_1 = T_2 \to T[a/T_1] = T[a/T_2]; \quad T_1 = T_2 \to (\varphi[a/T_1] \leftrightarrow \varphi[a/T_2]), \tag{B1.9}$$

где вместо $a$ можно рассматривать любую свободную переменную языка. Ясно, что приведенные аксиомы — это на самом деле бесконечная серия формул, каждая из которых получается заменой нетерминальных символов $T, T_1, T_2, \varphi$ на конкретные формулы и термы, а также переменная $a$ заменяется любыми другими свободными переменными.

Отсюда, в частности, следует аксиома конгруэнтности теории полугрупп, в которой в роли терма $T$ выступал функциональный символ с переменными: $a \circ b$.

Чаще всего аксиомы (B1.9) задаются в базовом виде, где в качестве терма $T$ рассматриваются все функциональные символы сигнатуры языка, а в качестве формулы $\varphi$ — предикатные символы сигнатуры языка. Имея такое допущение, формулы общего вида можно вывести, действуя индукцией по сложности формул. Однако такой подход заставляет нас привлекать т.н. внешнюю индукцию из мета-теории, что является уже довольно сильным требованием к мета-теории. Так что мы будем придерживаться схемы (B1.9) в тех случаях, когда рассуждаем на самом абстрактном уровне, а в конкретных случаях вроде теории полугрупп, арифметики или теории множеств будем формулировать эти аксиомы в упрощенном виде, опираясь только на атомарные формулы и термы.

Аксиомы конгруэнтности в некоторых источниках называются также аксиомами Гильберта.

**Важное замечание**: при определении формальной теории, в которой используется предикат равенства (=), аксиомы конгруэнтности (B1.9) (в полном или сокращенном

[8] В разговорных языках мы можем заметить такое явление: некоторые народы севера имеют несколько десятков наименований для оттенков цвета, который более южными народами обозначается одним словом «белый». То есть уже сам язык предполагает достаточное количество различных констант, которые в другом языке отождествляются. В физике же язык позволяет еще сильнее детализировать картину, предоставляя континуальный спектр.

виде), а также аксиомы равенства (B1.8) всегда подразумеваются наряду с аксиомами логики предикатов. Поэтому их не всегда можно встретить в перечне аксиом теории.

### B1.2.6 Модель языка и теории

Здесь мы переходим к синергии формальной логики и теории множеств. Точнее, мы предполагаем в качестве мета-теории теорию множеств, по модулю которой становятся доступны многие результаты про формальные теории, такие как, например, теоремы Лёвенгейма-Скулема или критерий Лося–Воота.

При этом мы не озвучиваем требования к мета-теории, хотя чаще всего предполагается, что это ZFC. Мы лишь должны четко понимать, что мета-теория может быть формализована точно так же, как все остальные теории, причем сама по себе формализация не требует каких-то сильных допущений вроде аксиомы выбора или даже индукции, она может быть произведена, например, силами достаточно слабой теории множеств или арифметики.

Иначе говоря, принимая в качестве основы некоторую достаточно слабую теорию, мы получаем возможность строить формальные языки и формальные теории любой сложности. Это не означает, что мы можем интерпретировать любую теорию в этой базовой слабой теории, она лишь является техническим средством, с помощью которого мы можем описать более сложные теории, а затем, выбирая более сложные теории в качестве мета-теорий, мы сможем получать различные результаты про различные формальные теории.

Таким образом получается что-то вроде карабкания по стенкам колодца, когда, начиная с первой легкой ступеньки, мы шаг за шагом усложняем структуру формализма, логики и теорий, постепенно усиливая их, а между тем твердая почва под ногами становится все дальше и дальше.

Следующее понятие, которое мы здесь рассмотрим, — это модель теории. Итак, пусть у нас имеется язык $\mathbb{F}$, построенный по правилам логики предикатов, где $F_1, F_2, \ldots$ — функциональные символы, $C_1, C_2, \ldots$ — символы констант, $P_1, P_2, \ldots$ — предикатные символы. Вместе все эти символы образуют множество $\Sigma$, именуемое *сигнатурой* языка $\mathbb{F}$.

Предположим теперь, что у нас имеется непустое множество $\mathfrak{m}$ (мы пользуемся готическими буквами для обозначения мета-теоретических объектов). Мы можем рассматривать это множество $\mathfrak{m}$ как базовый универсум, в рамках которого с помощью языка $\mathbb{F}$ мы можем вводить различные понятия: формулы языка $\mathbb{F}$ будут их определениями, а подмножества $\mathfrak{m}$ — объемами.

Далее мы можем рассмотреть множество $\mathfrak{m}^n$ всех $n$-ок элементов множества $\mathfrak{m}$, которое называется декартовой степенью множества $\mathfrak{m}$. Это позволит нам задавать отношения и функции на $\mathfrak{m}$. Воспользуемся понятиями отношения и функции, которые были введены в разделе A2.7.

Сопоставим символам нашей сигнатуры $\Sigma$ конкретные «значения» в множестве $\mathfrak{m}$: каждому константному символу $C_k$ сопоставим определенный элемент $\mathfrak{c}_k$ из $\mathfrak{m}$; каждому функциональному символу $F_k$ — конкретную функцию $\mathfrak{f}_k$; каждому предикатному символу $P_k$ — конкретное отношение $\mathfrak{p}_k$. Будем обозначать сопоставление символом $\dashrightarrow$, т.е. $C_k \dashrightarrow \mathfrak{c}_k$, $F_k \dashrightarrow \mathfrak{f}_k$, $P_k \dashrightarrow \mathfrak{p}_k$. Такое сопоставление задает **интерпретацию** сигнатуры в множестве $\mathfrak{m}$ (подробнее см. раздел D2.2)..

Кроме того, для определения истинности формул со свободными переменными нам понадобится **оценка** (или *означивание*) — это функция, которая каждой свободной переменной сопоставляет некоторый элемент из $\mathfrak{m}$.

Имея интерпретацию символов и оценку переменных, мы можем рекурсивно определить значение любого терма и истинностное значение любой формулы языка $\mathbb{F}$.

Структура $\mathscr{M} \overset{\text{def}}{\rightleftharpoons} \langle \mathfrak{m}, \mathfrak{C}, \mathfrak{F}, \mathfrak{P} \rangle$, где $\mathfrak{C}$ — множество констант $\mathfrak{c}_k$, $\mathfrak{F}$ — множество функций $\mathfrak{f}_k$, $\mathfrak{P}$ — множество отношений $\mathfrak{p}_k$, называется **моделью** языка $\mathbb{F}$.

Поскольку аксиомы и теоремы всегда рассматриваются как **замкнутые формулы** (без свободных переменных), их истинность в модели не зависит от выбора конкретной оценки свободных переменных. Формула считается *истинной в модели*, если она истинна при *любой* оценке переменных.

Если в языке $\mathbb{F}$ задана некоторая теория $\mathfrak{T}$, все аксиомы (и теоремы) которой оказываются истинными в данной модели при данной интерпретации символов сигнатуры и любой оценке свободных переменных, то структура $\mathscr{M}$ называется *моделью теории* $\mathfrak{T}$. Этот факт записывается так: $\mathscr{M} \models \mathfrak{T}$.

## B1.2.7 Примеры интерпретации

### Теория строгих линейных порядков

Чтобы не повторяться, рассмотрим новый пример теории, расширяющий сразу два ранее рассмотренных примера: теорию частичных порядков и теорию чистого равенства. Пусть в нашем языке $\mathbb{F}$ имеются два предикатных символа: $=$ и $<$. Соответственно, атомарными формулами будут $(a = b)$ и $(a < b)$. Моделью такого языка будет любое непустое множество предметов с двумя бинарными отношениями. Например, элементами множества могут быть карандаши в школьном пенале, а бинарными отношениями такие: 1) два предмета находятся в отношении $\mathfrak{p}_1$, если они имеют одинаковый цвет, 2) два предмета находятся в отношении $\mathfrak{p}_2$, если они имеют одинаковую длину. Тогда мы можем сделать сопоставления:

$$=\dashrightarrow \mathfrak{p}_1; \quad <\dashrightarrow \mathfrak{p}_2.$$

Заметим, что пока у нас нет никаких требований к предикатам, т.к. у нас нет аксиом, задающих свойства символов $=$ и $<$, поэтому единственное, что нас ограничивает при интерпретации — это арность отношений.

Добавим теперь аксиомы, т.е. рассмотрим в языке $\mathbb{F}$ теорию строгих линейных порядков (как обычно, без универсального замыкания кванторами всеобщности):

$$\begin{aligned}
&a_1 : a = a && a_6 : \neg(a < a)\\
&a_2 : (a = b) \to (b = a) && a_7 : (a < b) \wedge (b < c) \to (a < c)\\
&a_3 : (a = b) \wedge (b = c) \to (a = c) && a_8 : (a < b) \vee (a = b) \vee (b < a)\\
&a_4 : (a = b) \to (c < a \leftrightarrow c < b)\\
&a_5 : (a = b) \to (a < c \leftrightarrow b < c)
\end{aligned}$$

В первых трех строках находятся аксиомы равенства (рефлексивность, симметричность, транзитивность) и аксиомы линейного порядка (антирефлексивность, транзитивность, связность). Аксиомы $a_4$ и $a_5$ есть воплощение аксиом конгруэнтности (B1.9), поскольку в нашей теории любой терм — это переменная (из-за отсутствия функциональных символов).

Обычно, как уже отмечалось, аксиомы равенства и конгруэнтности подразумеваются автоматически, поэтому собственными нелогическими аксиомами теории линейного порядка являются аксиомы $a_6, a_7, a_8$.

Теперь мы можем проверить, работает ли наше сопоставление $=\dashrightarrow \mathfrak{p}_1$ и $<\dashrightarrow \mathfrak{p}_2$. Оказывается, что нет в обоих случаях. Отношение $\mathfrak{p}_1$, основанное на тождестве цветов карандашей, на первый взгляд, может моделировать равенство, поскольку удовлетворяет аксиомам равенства $a_1, a_2, a_3$. Но вместе с интерпретацией $<\dashrightarrow \mathfrak{p}_2$ возникает проблема: аксиома конгруэнтности $a_4$ требует, что если два карандаша ($a$ и $b$) имеют одинаковый цвет ($\mathfrak{p}_1(a, b)$), то каков бы ни был третий карандаш $c$, если он имеет такую же длину, как первый ($\mathfrak{p}_2(c, a)$), то он должен иметь такую же длину, как и второй ($\mathfrak{p}_2(c, b)$). Что, разумеется, не верно в общем случае, поскольку цвет карандаша никак не накладывает ограничение на его длину.

Неверной является и интерпретация предиката ($a < b$) отношением $\mathfrak{p}_2(a, b)$, поскольку это отношение рефлексивное в противоречии с аксиомой $a_6$. Поэтому рассмотрим на множестве карандашей еще одно отношение $\mathfrak{p}_3(a, b)$, которое будет означать, что карандаш $a$ короче карандаша $b$. В этом случае сопоставление $<\dashrightarrow \mathfrak{p}_3$ уже окажется корректным, т.к. сравнение по длине удовлетворяет аксиомам $a_6, a_7, a_8$.

Однако аксиома $a_5$ по-прежнему не верна, т.к. цвет карандаша никак не связан с его длиной.

Дальше возникает вопрос, как же корректно смоделировать отношение равенства в коробке с карандашами. Чтобы не вступать в конфликт с аксиомами порядка и конгруэнтности, мы можем символ $=$ поставить в соответствие отношению $\mathfrak{p}_2$, которое ранее пытались ассоциировать с символом $<$. Иначе говоря, мы будем отождествлять карандаши, имеющие равную длину. Тогда все аксиомы будут выполняться, несмотря на то, что равные по длине карандаши могут отличаться другими своими признаками, например, цветом.

Итак, моделью теории, описанной аксиомами $a_1 - a_8$ в языке с предикатами $=, <$ является множество $\mathfrak{m}$ карандашей с предикатами $\mathfrak{p}_2$ и $\mathfrak{p}_3$ при соответствии $=\dashrightarrow \mathfrak{p}_2$, $<\dashrightarrow \mathfrak{p}_3$.

Возникает вопрос — можно ли символ $=$ моделировать как истинное тождество предметов в модели? В нашем случае это сделать не удастся, т.к. если мы найдем два разных карандаша $a$ и $b$ одинаковой длины, то, с одной стороны, $a \neq b$, а с другой стороны, для них не выполняется ни $a < b$, ни $b < a$. Это напрямую противоречит аксиоме связности $a_8$, которая требует, чтобы для любой пары различных элементов один был меньше другого.

Поэтому модели, в которых удается $=$ интерпретировать как тождество в самой модели, выделяют в отдельный класс и называют **нормальными моделями**.

Итак, мы видим, что **а)** процесс адаптации модели языка к аксиомам теории не всегда тривиален, **б)** равенство не всегда может и должно интерпретироваться как равенство, главное, чтобы оно разбивало носитель модели (множество $\mathfrak{m}$) на классы эквивалентности так, чтобы внутри этих классов все свойства предметов были одинаковыми с точки зрения интерпретируемого языка.

## Теория групп

В теории групп мы используем язык с одной константой 1, одним бинарным функциональным символом $\circ$, одним унарным функциональным символом $()^{-1}$ и одним бинар-

ным предикатом $=$. Выпишем только нелогические аксиомы теории групп (исключая также аксиомы равенства и конгруэнтности):

$g_1$ : $a \circ (b \circ c) = (a \circ b) \circ c$ [полугруппа];

$g_2$ : $a \circ 1 = a$; $1 \circ a = a$ [моноид];

$g_3$ : $a \circ a^{-1} = 1$; $a^{-1} \circ a = 1$ [группа].

Нетрудно понять, что моделью данного языка и теории будет, например, множество целых чисел $\mathbb{Z}$ с операциями $+$, $-$ (не разность, а противоположный элемент) и константой 0 (которая интерпретирует символ 1 языка $\mathbb{F}$), где равенство интерпретируется как равенство (т.е. модель является нормальной).

Если нам хочется использовать умножение целых чисел в качестве модели операции $\circ$, то нам следует рассмотреть умножение положительных целых чисел (универсум $\mathfrak{m}$) по простому модулю $\mathfrak{p}$ ($a \circ b$ есть остаток от деления $ab$ на $\mathfrak{p}$). В этом случае символ 1 будет интерпретироваться обычной единицей, а обратный по умножению элемент $a^{-1}$ будет вычисляться как остаток от деления $a^{\mathfrak{p}-2}$ по модулю $\mathfrak{p}$ (*малая теорема Ферма*). Но при этом равенство будет интерпретироваться как эквивалентность по модулю $\mathfrak{p}$, чтобы не «сломались» аксиомы равенства.[9]

Существуют и «более физические» модели теории групп, например, сложение отрезков времени на часах выполняется по модулю 12 и представляет собой группу по сложению остатков. Вращения правильных многогранников (кристаллов) — пример группы, где операция $\circ$ интерпретируется как композиция (последовательное применение) вращений. Теория групп имеет огромное количество принципиально различных интерпретаций в различных областях науки и техники.

## Делимые абелевы группы без кручения

Рассмотрим теорию групп с дополнительными аксиомами (помимо приведенных выше $g_1 - g_3$), но в слегка модифицированном языке. А именно, групповая бинарная операция теперь будет обозначаться как $+$, операция взятия обратного элемента — как $-$, нейтральный элемент — как 0. Такова традиция обозначений для абелевых (коммутативных) групп.

$g_1$ : $a + (b + c) = (a + b) + c$ [полугруппа];

$g_2$ : $a + 0 = a$, $0 + a = a$ [моноид];

$g_3$ : $a + (-a) = 0$; $(-a) + a = 0$ [группа];

$g_4$ : $a + b = b + a$ [абелевость/коммутативность];

$g_5$ : $\forall n > 0\ \forall x\ \exists y\ x = \underbrace{y + \cdots + y}_{n}$ [делимость].

$g_6$ : $\forall n > 0\ \forall x \neq 0 : \underbrace{x + \cdots + x}_{n} \neq 0$ [без кручения];

[9] Простые выкладки показывают, что, например, $6 = 6 \circ 1 = 6 \cdot 1 \pmod 5 = 1$, а в нормальной модели должно быть $6 \neq 1$.

Обычно теорию делимых абелевых групп, определяемую аксиомами $g_1 - g_5$, обозначают DAG (Divisible Abelian Groups), а DAG без кручения обозначается DTFA (Divisible Torsion-Free Abelian groups).

Отметим, что аксиомы $g_5$ и $g_6$ являются схемами аксиом с параметром $n$, поэтому квантор по $n$ у нас выделен красным цветом, он принадлежит мета-теории.

Аксиома $g_5$ говорит нам, что любой элемент $x$ можно представить как $n$-кратную сумму элемента $y$, и в таком случае пишут, что $y = x/n$. Кроме того, сумму одного элемента в количестве $m$ также принято записывать в виде $mx$ (при $m = 0$ полагаем $mx = 0$), а для отрицательного $m$ под $mx$ понимают $-((-m)x)$. Так что вместе с аксиомой делимости мы получаем возможность умножать любой элемент группы на произвольное рациональное число $m/n$. Это значит, что DAG описывает то, что в алгебре называется $\mathbb{Q}$-модулем, или векторным пространством над полем $\mathbb{Q}$.

Аксиома $g_6$ говорит, что никакой ненулевой элемент группы, будучи сложенным с самими собой положительное число раз, не равен 0. Это исключает, например, циклические группы, в частности, группы сложения целых чисел по некоторому модулю, и делает такие группы заведомо бесконечными, т.к. при данном условии все $nx$ попарно различны (при $x \neq 0$).

Стандартной интерпретацией DTFA является множество рациональных чисел $\mathbb{Q}$, а также множество вещественных и комплексных чисел (с операцией сложения). К менее стандартным примерам можно отнести конечные расширения поля $\mathbb{Q}$ (например, множество чисел вида $x + y\sqrt{2}$, где $x, y \in \mathbb{Q}$, и т.п.).

Если мы снимем требование отсутствия кручения, т.е. рассмотрим теорию DAG, то у такой теории стандартной моделью, пожалуй, будет группа вращений окружности $U(1)$ (она же $SO(2)$). Здесь в качестве операции + выступает сложение углов поворота. Очевидно, что это группа с делением, т.к. любой поворот можно разделить на $n$ равных поворотов, и в то же время в этой группе есть кручения, а именно, поворот на угол $360^o/n$, сложенный с самим собой $n$ раз, даст нулевой поворот.

В физике (оптика, акустика, квантовая механика) фаза волны является ключевой характеристикой. Фазы складываются по модулю $2\pi$, то есть их естественная модель — $U(1)$. Делимость важна, например, при анализе интерференции от $n$ источников.

Делимые абелевы группы возникли как естественный и важный объект на пересечении изучения бесконечных абелевых групп, поиска структурных теорем и развития гомологической алгебры, причем их полная и простая классификация как $\mathbb{Q}$-векторных пространств сделала их особенно полезными и исторически значимыми.

Отметим один очень важный аспект сравнения формальных теорий и общематематических теорий: формальная теория состоит ровно из тех теорем, которые можно вывести из аксиом по правилам вывода, в то же время общематематическая теория изучает не только следствия внутри самого формализма, но и все модели этого формализма силами теории множеств. И большинство известных и важных теорем математической теории групп — это теоремы о моделях формальной теории групп. К таковым теоремам относятся, например, теорема Кэли, Лагранжа, Силова, теоремы об изоморфизмах групп, классификационные теоремы и т.д. Все они так или иначе используют мета-теоретические конструкции и определения: функции между группами, мощность группы (количество элементов), факторизация группы и т.д.

Поэтому если мы открываем учебник по теории групп, то мы сразу видим определение группы как объекта теории множеств (структуры), т.е. множества с операцией, подчиненной аксиомам формальной теории групп. Объектами общематематической

теории групп являются сами группы и их элементы, а объектами формальной теории групп — только элементы группы.

### B1.2.8 Некоторые понятия теории моделей

Теория моделей позволяет наполнять смыслом формализмы и анализировать их внешним образом. Дадим несколько определений, основанных на возможности строить модели формальных теорий.

Теория $\mathfrak{T} \subset \mathbb{F}$ называется **совместной** (выполнимой), если у нее существует модель. Например, рассмотренные выше теория строгого линейного порядка и теория групп совместны.

Формула $\varphi \in \mathbb{F}$ называется **общезначимой** (обозначение: $\models \varphi$), если она истинна в любой модели. Приведем примеры общезначимых формул:[10]

$$\neg(\forall x \varphi(x)) \leftrightarrow \exists x \neg\varphi(x), \quad \neg(\exists x \varphi(x)) \leftrightarrow \forall x \neg\varphi(x),$$

$$\exists x \forall y \varphi(x, y) \rightarrow \forall y \exists x \varphi(x, y),$$

где $\varphi$ — произвольная формула языка $\mathbb{F}$. К общезначимым формулам относятся также все подстановки формул в тавтологии логики высказываний.

Формула $\varphi$ **логически (семантически) следует** из множества формул $\Gamma \subset \mathbb{F}$ (обозначение: $\Gamma \models \varphi$), если для любой модели, в которой все формулы $\Gamma$ тождественно истинны, формула $\varphi$ также тождественно истинна. Обычно в качестве элементов $\Gamma$ рассматриваются только нелогические формулы, а все логические считаются по умолчанию включенными в него, поэтому если мы говорим, что множество посылок $\Gamma$ пусто, то это означает, что оно состоит из чистой теории предикатов в данном языке. Так что запись $\models \varphi$ означает, что формула $\varphi$ логически следует из чистой теории предикатов, что, как мы увидим в дальнейшем, равносильно ее общезначимости: $\models \varphi \Leftrightarrow \models \varphi$.

Формулы *равносильны*, если они одновременно истинны или ложны в одних и тех же моделях (т.е. логически следуют друг из друга). Для обозначения равносильности формул мы используем такое же обозначение, как в логике высказываний: $\varphi \equiv \psi$. Кстати, из равносильности пропозициональных формул автоматически вытекает равносильность всех подстановок в них формул исчисления предикатов. Например, нам известно, что

$$\mathscr{A} \rightarrow \mathscr{B} \equiv \neg\mathscr{B} \rightarrow \neg\mathscr{A},$$

тогда, производя подстановки $[\mathscr{A}/\varphi]$ и $[\mathscr{B}/\psi]$, независимо от языка и моделей, мы получим равносильность

$$\varphi \rightarrow \psi \equiv \neg\psi \rightarrow \neg\varphi.$$

### B1.2.9 Основные факты о логике предикатов

#### Корректность и полнота вывода

Вспомним теперь о том, что у логики высказываний мы упоминали такие свойства как корректность и полнота, и эти свойства были напрямую связаны с представлением формул логики высказываний в виде двоичных функций. Множество таких функций являет-

[10] Третья формула будет выведена в Части II, теорема D2.7

ся не чем иным, как моделью логики высказываний. У классической логики высказываний существуют и другие модели (например, булеан какого-либо непустого множества), однако все они в некотором (а именно, алгебраическом) смысле эквивалентны.

Корректность и полнота логики высказываний означали для нас два факта: «штопор не врет» (все выводимое из тавтологий есть тавтология) и «аксиоматика полна» (все тавтологии выводимы из аксиом).

Примерно то же самое можно сказать и про логику предикатов с оговоркой про разнообразие моделей.

**Теорема B1.5** (о корректности)**.**
*Если в некоторой модели истинны все формулы множества* $\Gamma \subset \mathbb{F}$ *и имеет место формальный вывод* $\Gamma \vdash \varphi$*, то* $\varphi$ *также истинна в данной модели.*

Иначе говоря, если в модели истинны аксиомы теории, то истинны и все теоремы («штопор не врет»). Эта теорема проверятся индукцией по длине вывода $\mathfrak{T} \vdash \varphi$ (т.е. мета-теория должна включать в себя аксиому индукции). Действительно, истинность посылок нам уже дана (множество Γ), а все переходы к последующим формулам в дедуктивном выводе осуществляются строго по правилам вывода. Значит, индукционный шаг — это проверка того, что если в посылках правила вывода стоят истинные в модели формулы, то и в выводе стоит истинная в модели формула. В этом достаточно легко убедиться, проверив каждое из правил вывода (MP и правила Бернайса).

Теория $\mathfrak{T} \subset \mathbb{F}$ называется **непротиворечивой**, если среди ее теорем нет одновременно некоторой формулы вместе с ее отрицанием (т.е. нельзя вывести $\varphi \wedge \neg\varphi$ или, короче, $\bot$).[11] В противном случае теория *противоречива*. У противоречивой теории множество теорем состоит из всех замкнутых формул языка $\mathbb{F}$, т.к. однажды получив при выводе противоречие, мы можем дальше вывести любую формулу.

**Теорема B1.6.** *Если теория совместна (имеет модель), то она непротиворечива.*

Эта теорема предполагает непротиворечивость той теории, в которой строится модель, т.е. теории множеств. Действительно, если бы теория была противоречивой, то в ней можно было бы вывести $\varphi$ и $\neg\varphi$, но тогда интерпретации обеих этих формул были бы истинными в данной модели (по теореме о корректности), т.е. в модели была бы истинной ложь. А значит, мы сумели вывести противоречие в мета-теории.

**Теорема B1.7** (Гёделя о полноте логики предикатов)**.**

**(1)** *Если теория непротиворечива, то она имеет модель (совместна).*

**(2)** *Эквивалентная формулировка:*[12] *если* $\Gamma \Vdash \varphi$*,* $\Gamma \vdash \varphi$*.*

Первая часть теоремы, что характерно для математической логики, доказывается по сути построением модели из… самих формул. Действительно, если у нас ничего нет, кроме языка $\mathbb{F}$, то почему бы не построить универсум из тех букв, что у нас есть? Во-первых, мы включаем в универсум все символы-константы, т.к. они должны иметь сопоставление в модели, во-вторых, из всех истинных замкнутых формул с квантором существования (*экзистенциальных формул*) мы извлекаем их свидетелей, т.е. пользуемся таким

[11] Напомним, что мы определили символ $\bot$ как пропозициональную формулу $\mathscr{A} \wedge \neg\mathscr{A}$, но все подстановки формул логики предикатов в пропозициональные формулы тоже являются формулами логики предикатов, так что определение символов $\bot$ и $\top$ можно без труда расширить и на логику предикатов.

[12] Почему эти формулировки эквивалентны с точки зрения мета-теории, мы будем разбираться в Части II, см. раздел D2.2

специальным фактом, что у любой такой формулы есть свидетель, выразимый термом в нашем языке.[13] В итоге множество-носитель модели состоит из констант и таких вот термов, делающих экзистенциальные формулы истинными. Для всех остальных аксиом и теорем теории истинность проверяется уже логическим путем.

Вторая часть, равносильная первой, утверждает, что если $\varphi$ «на самом деле» следует из $\Gamma$, то она и выводима формальным способом. Таким образом, выводимость ($\vdash$) и логическое (семантическое) следование ($\models$) равносильны в классической логике предикатов, а непротиворечивость теории равносильна ее совместности (наличию модели).

Доказательство теоремы о полноте для логики предикатов Куртом Гёделем в 1929 году стало одним из величайших достижений логики XX века. Оно показало, что синтаксические правила вывода в логике первого порядка достаточны для вывода всех семантически истинных утверждений.

Следующие теории непротиворечивы (относительно мета-теории множеств):

- логика предикатов с пустым множеством нелогических аксиом (чистое исчисление предикатов);
- теория частичного порядка; теория линейного порядка;
- теория чистого равенства;
- теория полугрупп; теория групп;
- элементарная геометрия Тарского;
- арифметика Пеано первого порядка.

Про саму теорию множеств утверждать непротиворечивость уже затруднительно, ведь для этого нужно предъявить модель теории множеств в рамках самой же теории множеств. Такие модели можно построить, только усилив теорию множеств Цермело-Френкеля специальными аксиомами больших множеств (например, аксиомой строго недостижимого кардинального числа). Иначе говоря, непротиворечивость теории множеств можно обосновать только в еще более сильной теории.

Тем не менее, простота формулировок аксиом ZF, особенно в части наследственно конечных множеств (т.е. без аксиомы бесконечности), и возможность их интерпретации в рекурсивной (читай: компьютерной) арифметике вселяют в нас уверенность в непротиворечивости теории множеств и уверенность в том, что она может быть надежной мета-теорией.

## Полнота теории

Говорят, что замкнутая формула $\varphi$ **не зависит** от множества формул $\Gamma \subset \mathbb{F}$, если как $\varphi$, так и $\neg\varphi$ не выводимы в логике предикатов из $\Gamma$ ($\Gamma \nvdash \varphi$ и $\Gamma \nvdash \neg\varphi$).

**Теорема B1.8.**
*Если теории $\mathfrak{T} \cup \{\varphi\}$ и $\mathfrak{T} \cup \{\neg\varphi\}$ имеют модели, то формула $\varphi$ не зависит от $\mathfrak{T}$.*

[13] Указанное свойство теории называется *условием Хенкина*, а возможность расширить всякую теорию до такой, которая удовлетворяет условию Хенкина, доказывается отдельно, причем в случае несчетных языков — не без помощи подходящей версии аксиомы выбора.

Данная теорема является основным инструментом доказательства независимости математических утверждений от некоторого аксиоматического базиса.

Приведем наиболее известные примеры независимых формул:

- Аксиома Эвклида (формализация V постулата) относительно абсолютной геометрии (постулаты I–IV).
- Теорема Гудстейна относительно формальной арифметики Пеано первого порядка.
- Аксиома выбора относительно теории множеств ZF.
- Континуум-гипотеза Кантора относительно ZFC.

Если на аксиоматику теории смотреть как на базис векторного пространства, то можно провести следующие аналогии:

- аксиоматику можно рассматривать как систему векторов (не обязательно независимую);
- множество всех теорем с данной аксиоматикой подобно линейной оболочке системы векторов;
- независимая формула подобна независимому вектору.

У аналогии, как водится, есть изъяны. Например, отрицание формулы нельзя понимать как противоположный вектор, т.к. противоположный вектор ничего не добавляет к линейной оболочке векторов, в то время как добавление отрицания формулы к исходной дает противоречивую систему, из которой выводится весь язык $\mathbb{F}$.

Кроме того, возможна такая ситуация: формулы $\varphi_1$ и $\varphi_2$ не зависят от множества формул $\Gamma$, более того, они друг другу противоречат, и при этом существует такая формула $\psi$, что $\Gamma \nvdash \psi$, но $\Gamma, \varphi_1 \vdash \psi$ и $\Gamma, \varphi_2 \vdash \psi$. В случае векторов обязательно оказалось бы тогда, что $\Gamma, \varphi_1$ и $\Gamma, \varphi_2$ имеют одинаковую линейную оболочку (эквивалентны). В случае выводимости теории, порожденные этими системами аксиом, будут разными, но в каждой из них будет теорема $\psi$, и в то же время ее не будет в теории, порожденной аксиоматикой $\Gamma$.

В качестве примера достаточно взять $\Gamma = \mathrm{ZF}$, $\varphi_1$ — аксиома выбора AC, $\varphi_2$ — аксиома детерминированности AD, $\psi$ — счетная аксиома выбора для множеств вещественных чисел $\mathrm{AC}_\omega(\mathbb{R})$. Здесь $\mathrm{AC}_\omega(\mathbb{R})$ утверждает, что всякая счетная последовательность непустых множеств вещественных чисел имеет функцию выбора.

Если *непротиворечивая* теория $\mathfrak{T} \subset \mathbb{F}$ такова, что никакая замкнутая формула $\varphi \in \mathbb{F}$ не является независимой, то теория $\mathfrak{T}$ называется **полной** (*в смысле выводимости*).

Несомненно, центральным и даже эпохальным результатом о формальных теориях первого порядка является

**Теорема B1.9** (Гёделя о неполноте (первая))**.** *Если теория*

(G1) *непротиворечива;*

(G2) *перечислима (т.е. существует алгоритм, умеющий перечислять все ее теоремы);*

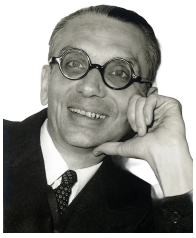
(G3) *может интерпретировать достаточно сильную арифметику (например,* PA*),*[14]

[14] Точнее, в стандартных формулировках достаточно интерпретировать арифметику Робинсона Q (или эквивалентную слабую арифметику, достаточную для арифметизации синтаксиса).

*то она не полна, т.е. существует такое предложение в языке этой теории, которое нельзя ни доказать, ни опровергнуть в системе ее аксиом.*

К перечислимым теориям относятся, например, все теории в конечном или счетном алфавите (включая сигнатуру), поскольку грамматика и правила вывода позволяют алгоритмизировать процесс «вычисления» теорем, так что не очень сильное ограничение геделевых теорий. Более сильным ограничением является возможность интерпретации арифметики, т.е. перевод арифметики на язык формул этой теории так, что переведенные аксиомы арифметики становятся теоремами этой теории. В случае теории множеств это означает возможность построить модель натуральных чисел (например, числа фон Неймана, как будет показано далее). Встраивание арифметики в теорию означает возможность внутренним способом (формулами этой теории) закодировать весь ее язык, в том числе теоремы и доказательства теорем. После чего становится возможным записать некоторое высказывание про натуральные числа, которое будет независимым в этой теории.

Существует и вторая теорема Гёделя о неполноте, которая гласит, что всякая теория геделевского типа, т.е. удовлетворяющая условиям (G1)–(G3), не может доказать свою собственную непротиворечивость (или, точнее, закодированное арифметикой утверждение об этом).



*Курт Гёдель*

После теорем Гёделя о неполноте стало ясно, что любая достаточно сильная формальная теория будет содержать истинные, но недоказуемые утверждения. Поиск и классификация таких утверждений (как теорема Париса-Харрингтона или теорема Гудстейна) стал важным направлением в математической логике.

Тем не менее, при ослаблении условий (G1)–(G3) появляются примеры полных теорий. Прежде всего, интерес представляют, конечно, теории в счетном языке, а значит, нарушающие условие (G3), т.е. не умеющие интерпретировать в себе арифметику первого порядка.

Можно привести следующие примеры полных теорий.

- Теория плотного линейного порядка без первого и последнего элементов ($\mathrm{DLO}_\infty$). Аксиомы этой теории включают аксиомы строгого линейного порядка, а также:

$$(a < b) \to \exists x\ (a < x) \wedge (x < b), \quad \forall x \exists y\ (y < x), \quad \forall x \exists y\ (x < y),$$

  где первая утверждает, что между любыми двумя элементами всегда найдется третий, вторая — что нет наименьшего элемента, третья — что нет наибольшего элемента.

- Теория равенства на бесконечном множестве. Здесь к аксиомам равенства нужно добавить бесконечную серию аксиом, запрещающих конечные носители (см. далее).

- Теория вещественно замкнутых полей (RCF, см. далее).

- Элементарная геометрия Тарского.

- Арифметика Пресбургера (арифметика без операции умножения).

## B1.2.10 Еще раз о теории равенства

Мы уже определили теорию чистого равенства, как теорию с единственным предикатом $=$ и тремя аксиомами: рефлексивности, симметричности и транзитивности. В

этой теории нет необходимости добавлять аксиомы конгруэнтности, поскольку никаких функциональных и предикатных символов больше нет. Однако легко понять, что чистая теория равенства не полна, поскольку достаточно легко предъявить примеры независимых формул.

Пусть $n$ — положительное натуральное число. Рассмотрим формулу

$$\varphi_n \overset{\text{def}}{\leftrightarrow} \exists y_1 \exists y_2 \ldots \exists y_n \forall x \ (x = y_1) \vee (x = y_2) \vee \ldots \vee (x = y_n).$$

Как нетрудно догадаться, формула сообщает нам, что существует $n$ объектов таких, что любой объект совпадает с одним из них, т.е. что в универсуме этой теории не может быть больше, чем $n$ объектов. В математике часто используют специальные сокращения для записи однородных итераций с параметром, иначе именуемых свертками, достаточно вспомнить формулы со значками суммы $\sum$ или произведения $\prod$. Аналогично, можно использовать знак большой дизъюнкции и конъюнкции. Так, формулу $\varphi_n$ можно переписать короче:

$$\varphi_n \overset{\text{def}}{\leftrightarrow} \exists y_1 \exists y_2 \ldots \exists y_n \forall x \ \bigvee_{i=1}^{n} (x = y_i).$$

Более того, когда мы пишем подряд однородные кванторы по пронумерованным переменным, мы тоже можем упростить себе жизнь, пользуясь обозначением $\exists \vec{y}$ вместо $\exists y_1 \exists y_2 \ldots \exists y_n$, причем количество переменных в таком случае восстанавливается из последующей части формулы. Тем не менее, это тоже удобно:

$$\varphi_n \overset{\text{def}}{\leftrightarrow} \exists \vec{y} \ \forall x \bigvee_{i=1}^{n} (x = y_i).$$

Записи подобного рода мы не относим к языку $\mathbb{F}$, а считаем их «синтаксическим сахаром» на уровне мета-теории. Однако же они легко укладываются в описанный нами в разделе A1.2 общий подход генерации лексем языка $\mathfrak{Math}$.

Для таких сверточных лексем также используются соглашения, чему считать их равными в том случае, если множество индексов окажется пустым (например, при $n = 0$ в нашем случае). При этом используются алгебраические соображения (ассоциативность). Так, пустая конъюнкция заменятся на $\top$, а пустая дизъюнкция — на $\bot$. Для квантора $\exists \vec{y}$ при отсутствии индексов следует принять соглашение, что его нужно заменить на пустую строку, т.е. вовсе удалить из текста формулы, поскольку переменных $y_i$ при $n = 0$ не существует.

Если теперь мы хотим добавить условие, что все $y_i$ попарно различны, то мы получим формулу, которая говорит, что в универсуме должно быть ровно $n$ объектов:

$$\psi_n \overset{\text{def}}{\leftrightarrow} \exists \vec{y} \bigwedge_{i<j} (y_i \neq y_j) \wedge \forall x \bigvee_{i=1}^{n} (x = y_i),$$

где символ $\bigwedge_{i<j}$ означает одну длинную конъюнкцию с количеством сравниваемых пар $y_i, y_j$ $(i < j)$, равным числу сочетаний из $n$ по 2.

Таким образом чистая теория равенства с аксиомой $\psi_n$ в качестве моделей может иметь только конечные множества с $n$ элементами. Отсюда также ясно, что любые две аксиомы $\psi_n$ и $\psi_m$ противоречат друг другу при $n \neq m$, но поскольку каждая в отдельности имеет свою модель, то аксиомы $\psi_n$ являют собой бесконечную серию примеров утверждений, независящих от аксиом чистой теории равенства.

Тем не менее, если мы рассмотрим теорию $\mathfrak{T}_n$, порожденную аксиоматикой, состоящей из аксиом равенства и аксиомы $\psi_n$, то такая теория окажется полной. Это довольно легко объяснить, потому что любая замкнутая формула в таком бедном языке (где нет ничего, кроме предиката равенства) либо истинна во всех моделях с $n$ элементами, либо ложна во всех таких моделях, а значит, логически либо следует из аксиом, либо опровергается. Но тогда в силу полноты логики предикатов для любой такой формулы или для ее отрицания существует доказательство, т.е. либо сама формула, либо ее отрицание есть теорема в $\mathfrak{T}_n$. Значит, теория $\mathfrak{T}_n$ полна.

Наконец, рассмотрим такую теорию равенства, где вместо одной аксиомы $\psi_n$ добавлены отрицания $\psi_n$ для всех натуральных $n$. У такой теории может быть только бесконечная модель. И такая теория тоже окажется полной, но уже в силу более сложной теоремы, а именно, признака полноты Лося-Воота, о котором речь пойдет во второй части книги (см. теорему D2.17).

## B1.3. Подытог и вопросы для самоконтроля

На уровне B1 мы уже существенно продвинулись в области термо- и формулостроения, ввели многочисленные понятия, связанные с формализмами, а также с их семантикой — моделями. Овладение уровнем B1 в этой книге, как и в случае изучения разговорного языка, — это умение читать и понимать основные концепции и структуры математического языка, типично возникающие в различных источниках, умение выразить формулами большинство простых фактов, понимание концепции доказательства и умение его воспроизвести в простейших случаях.

Ключевыми навыками на данном уровне являются представления о следующих понятиях и их свойствах:

- язык пропозициональных формул, включая правила редуцирования скобок;
- язык логики предикатов первого порядка с произвольной бестиповой сигнатурой;
- тавтологии и общезначимые формулы;
- выводимость в обоих типах логик (высказываний и предикатов);
- корректность и полнота вывода в обеих логиках;
- теорема о дедукции;
- аксиомы равенства и конгруэнтности;
- интерпретация языка и теории в модели;
- логическое (семантическое) следование;
- совместность и непротиворечивость теории;
- полнота теории и независимые формулы.

Теперь мы имеем возможность более точно указать рецепт изготовления формальной теории, описывающей некоторую предметную область, следуя той же схеме, которая была представлена в таблице A2.1. С целью упрощения мы рассматриваем здесь только бестиповую (однородную) предметную область (табл. B1.1). Мы не включили

Таблица B1.1. Рецепт создания формальной теории

**(1)** Определяем алфавит, из которого будут собираться все лексемы языка.

**(2)** Задаем сигнатуру языка (константные, функциональные и предикатные символы с указанием их арности).

**(3)** Перечисляем нелогические аксиомы теории в соответствии с концепцией того понятия, которое мы определяем этими аксиомами.

сюда шаги, описывающие построение термов и формул, а также конвенции редуцировании скобок, поскольку они являются универсальными для всех формальных теорий. Мы также не включили шаг, на котором определяются логические аксиомы и правила вывода, поскольку мы предполагаем использование классической логики предикатов, если не оговорено иное. Короче говоря, мы сосредоточились в этом рецепте на том, что действительно определяет облик формальной теории.

Следуя этому рецепту, мы уже определили выше несколько конкретных примеров формальных теорий:

- теория строгих линейных порядков с полными модификациями;
- чистая теория равенства с полными модификациями;
- теория полугрупп и теория групп;

Все изученное показывает нам тесную связь между формализмом и семантикой, а также наглядно демонстрирует тот факт, что строгость математики зиждется на некоторых простых, но обязательных предпосылках, а именно, на умении определять рекурсивные по своей природе объекты (термы, формулы, доказательства), умении «овеществлять» логику в теоретико-множественной семантике, и понимание того, что одно неотделимо от другого.

В завершение раздела B1 предлагаем читателю ответить на следующие вопросы для самоконтроля.

**Q1** Из каких основных компонентов (символов) состоит язык логики высказываний ($\mathbb{L}$) и каковы правила построения его формул? [стр. 81]

**Q2** Какова роль аксиом и правил вывода (в частности, Modus Ponens и правила подстановки (B1.6)) в системе логики высказываний? [стр. 84]

**Q3** Объясните понятия корректности и полноты вывода для логики высказываний. [стр. 81]

**Q4** Что такое функциональная полнота в логике высказываний и как она связана с таблицами истинности и равносильностью формул? [стр. 87]

**Q5** Чем отличаются термы от формул в логике предикатов? Опишите правила построения термов, включая переменные, константы и функциональные символы. [стр. 90]

**Q6** Каковы правила построения формул в логике предикатов, включая использование предикатных символов, логических связок и кванторов? [стр. 91]

**Q7** Перечислите основные группы логических аксиом логики предикатов и основные правила вывода. [стр. 94]

**Q8** Что такое интерпретация языка и модель теории в логике предикатов? Когда формула считается истинной в модели? [стр. 98]

**Q9** В чем заключается теорема Гёделя о полноте логики предикатов? Какая связь между непротиворечивостью теории и существованием модели? [стр. 103]

**Q10** Что такое формальная теория, нелогические аксиомы и теоремы в контексте логики предикатов? Приведите пример простой формальной теории, описанной в тексте. [стр. 95]

**Q11** В чем состоит отличие формальной теории от общематематической? Поясните на примере теории групп. [стр. 102]

## B1.4. Упражнения

**Ex1.** Определите, какие из следующих формул являются тавтологиями (всегда истинны):

1. $(\mathscr{A} \to \mathscr{B}) \to (\neg\mathscr{B} \to \neg\mathscr{A})$;
2. $((\mathscr{A} \to \mathscr{B}) \to \mathscr{A}) \to \mathscr{A}$ (Закон Пирса);
3. $(\mathscr{A} \to \mathscr{B}) \vee (\mathscr{B} \to \mathscr{A})$ (Линейность импликации);
4. $(\mathscr{A} \wedge \mathscr{B}) \to (\mathscr{A} \vee \mathscr{B})$.

**Ex2.** Найдите оценку (присваивание значений 0/1 переменным $\mathscr{A}, \mathscr{B}, \mathscr{C}$), при которой следующие формулы ложны:

1. $(\mathscr{A} \vee \mathscr{B}) \to (\mathscr{A} \wedge \mathscr{B})$;
2. $(\mathscr{A} \to \mathscr{B}) \to \mathscr{A}$;
3. $(\mathscr{A} \vee \mathscr{B}) \wedge \mathscr{C} \to \mathscr{A} \wedge (\mathscr{B} \vee \mathscr{C})$.

**Ex3.** Используя законы Де Моргана и двойное отрицание, упростите:

1. $\neg(\mathscr{A} \vee \neg\mathscr{B})$;
2. $\neg(\mathscr{A} \to (\mathscr{B} \wedge \neg\mathscr{C}))$;
3. $\neg(\forall x \exists y(\varphi(x, y) \to \neg\psi(x)))$.

**Ex4.** Следуя соглашению этой книги (Раздел B1.2.1), свободные переменные (параметры) должны обозначаться буквами $a, b, c$, а связанные переменные — $x, y, z$. Перепишите следующие «сырые» формулы в соответствии с этим соглашением (переименуйте свободные переменные в $a, b$, а связанные — в $x, y$):

1. $\forall k(P(k) \to Q(m))$;
2. $(\forall x P(x)) \wedge Q(x)$ (Подсказка: второй $x$ свободен);
3. $\exists z(u < z \to \forall u(u = z))$ (Подсказка: разрешите коллизию переменных $u$);
4. $\int_0^x t^2 dt$ (Интерпретируйте верхний предел как параметр).

**Ex5.** Пусть $\varphi = \exists y(a < y)$ (где $a$ свободна).

1. Выполните подстановку $\varphi[a/b]$.
2. Выполните подстановку $\varphi[a/S(b)]$.
3. Объясните, почему подстановка $\varphi[a/y]$ запрещена (некорректна) в нашей логике.

**Ex6.** Используя Теорему о дедукции B1.1, докажите правило гипотетического силлогизма:

$$\mathscr{A} \to \mathscr{B},\ \mathscr{B} \to \mathscr{C} \vdash \mathscr{A} \to \mathscr{C}.$$

**Ex7.** Докажите закон сокращения (Law of Contraction):

$$\vdash (\mathscr{A} \to (\mathscr{A} \to \mathscr{B})) \to (\mathscr{A} \to \mathscr{B}).$$

(Подсказка: Используйте аксиому $(\mathscr{A} \to (\mathscr{B} \to \mathscr{C})) \to ((\mathscr{A} \to \mathscr{B}) \to (\mathscr{A} \to \mathscr{C}))$).

**Ex8.** Используя аксиомы логики предикатов (PC2) и правила Бернайса, докажите:

$$\forall x P(x) \vdash \exists x P(x).$$

(Подсказка: Используйте терм $a$ и аксиомы $(\forall)$ и $(\exists)$).

**Ex9.** Правило (R1) гласит: $\frac{\varphi \to \psi}{\varphi \to \forall x \psi}$. Почему необходимо ограничение «переменная $a$ не входит в $\varphi$»? Покажите, что если нарушить это правило (например, пусть $\varphi = P(a)$ и $\psi = P(a)$), можно вывести ложное утверждение, такое как $P(a) \to \forall x P(x)$.

**Ex10.** Используя эквивалентности $\neg \forall x \varphi \leftrightarrow \exists x \neg \varphi$ и $\neg \exists x \varphi \leftrightarrow \forall x \neg \varphi$, внесите отрицание внутрь:

1. $\neg \forall x (P(x) \to Q(x))$;
2. $\neg \exists x \forall y (R(x,y) \vee S(x))$;
3. $\neg (\exists x P(x) \to \forall y Q(y))$.

**Ex11.** Докажите (семантически или синтаксически), что если $x$ не входит свободно в $P$, то:

$$\forall x (P \vee Q(x)) \leftrightarrow P \vee \forall x Q(x).$$

**Ex12.** Опровергните $\exists x (P(x) \wedge Q(x)) \leftrightarrow (\exists x P(x) \wedge \exists x Q(x))$.

**Ex13.** Постройте модель (универсум и предикаты), в которой следующие формулы ложны:

1. $\exists x P(x) \to \forall x P(x)$;
2. $\forall x \exists y P(x,y) \to \exists y \forall x P(x,y)$;
3. $\forall x (P(x) \vee Q(x)) \to (\forall x P(x) \vee \forall x Q(x))$.

**Ex14.** Выполнимо ли следующее множество формул?

$$\{\forall x\ (x < x),\ \forall x \forall y \forall z (x < y \wedge y < z \to x < z),\ \forall x \exists y\ \neg (x < y) \wedge \neg (y < x)\}$$

**Ex15.** Запишите конкретные примеры Схемы аксиом конгруэнтности $(a = b) \to (\varphi[x/a] \leftrightarrow \varphi[x/b])$ для:

1. $\varphi(x) \equiv P(x)$ (унарного предиката);

2. $\varphi(x) \equiv (x < c)$ (бинарного предиката с параметром).

**Ex16.** Запишите формулу в логике первого порядка с равенством, выражающую:

1. «Существует по крайней мере 2 элемента»;
2. «Существует по крайней мере 3 элемента».

**Ex17.** Запишите формулу, выражающую:

1. «Существует ровно 1 элемент» ($\exists! x$);
2. «Существует ровно 2 элемента».

**Ex18.** Выразите следующие теоретико-множественные утверждения, используя логические связки и предикат принадлежности:

1. $A \subseteq B \cup C$;
2. $A \cap B = \varnothing$;
3. $A \setminus B \subseteq C$.

**Ex19.** Пусть универсум $U$ состоит из трех карандашей:

$$U = \{p_1(\text{Красный, Короткий}),\ p_2(\text{Красный, Длинный}),\ p_3(\text{Синий, Длинный})\}$$

Пусть предикат $R(x)$ означает «$x$ красный», а $L(x)$ означает «$x$ длинный». Определите истинностное значение следующих формул в этой модели:

1. $\forall x(R(x) \vee L(x))$;
2. $\exists x(R(x) \wedge \neg L(x))$;
3. $\forall x(L(x) \to \neg R(x))$;
4. $\forall x(R(x) \to \exists y(L(y) \wedge y \neq x))$.

**Ex20.** Рассмотрим формулу $\varphi = \forall x \exists y R(x, y)$. Определите её истинностное значение в следующих интерпретациях (моделях):

1. Модель 1 (Арифметика): Универсум $\mathbb{N}$, $R(x, y)$ означает «$x < y$».
2. Модель 2 (Генеалогия): Универсум Люди, $R(x, y)$ означает «$x$ является ребенком $y$».
3. Модель 3 (Шахматы): Универсум Шахматные фигуры на доске, $R(x, y)$ означает «$x$ атакует $y$». (Предполагается стандартная расстановка для определенности).

# Фундамент математики

*Бог создал натуральные числа, всё остальное — дело рук человеческих.*

— Леопольд Кронекер

## B2.1. Арифметика Пеано

В конце XIX века математика столкнулась с необходимостью более строгого обоснования своих разделов, в частности, арифметики натуральных чисел. Итальянский математик Джузеппе Пеано стал одной из ключевых фигур в этом процессе формализации.

*Джузеппе Пеано*

В 1889 году Пеано представил свою систему аксиом, призванную дать строгое и формальное определение натуральных чисел. Его подход опирался на минимальный набор неопределяемых терминов: понятие нуля (или единицы) и операцию «следующий за» (последователя).

Центральной идеей системы Пеано стал принцип математической индукции, включенный в аксиоматику. Этот принцип, наряду с аксиомами о нуле и последователе, заложил основу для строгого определения и доказательства свойств арифметических операций. В рамках этой аксиоматики стало возможным формально обосновать рекурсивные определения сложения и умножения и доказать их основные свойства.

Система Пеано стала важным шагом на пути к полной формализации математики. С последующим развитием и систематизацией первопорядковой логики предикатов в начале XX века, аксиомы Пеано были переформулированы в рамках этого мощного логического аппарата.

Сегодня под Арифметикой Пеано первого порядка (часто обозначаемой PA) понимается именно эта формальная теория. Она состоит из конечного числа аксиом, описывающих базовые свойства нуля и последователя, и схемы аксиом индукции. Последнее означает, что для каждой формулы языка арифметики существует отдельная аксиома индукции, соответствующая этой формуле. Несмотря на кажущуюся простоту исходных понятий, PA является достаточно богатой теорией, способной формализовать значительную часть элементарной теории чисел, но при этом, согласно теоремам Гёделя о неполноте, она не может быть полной и непротиворечивой одновременно.

Но начнем мы с описания концепции натурального числа. Ведь чтобы формализовать их определение (сделать его математическим), нам нужно максимально точно описать то, что мы хотим от этого понятия.

Итак, натуральные числа — это абстрактные сущности, необходимые для выполнения следующих функций: пересчета (нумерации) произвольных объектов и сравнения объемов понятий.

Пересчет предполагает, что каким-то произвольным объектам можно ставить в соответствие натуральные числа, начиная с какого-то одного конкретного, и далее по-

следовательно каждому следующему предмету ставить в соответствие следующее натуральное число. Отсюда возникает идея, что за каждым натуральным числом $n$ должно идти непосредственно следующее, именуемое последователем и обозначаемое $S(n)$, а также, что каждое число (за исключением одного начального) есть чей-то последователь. Так у нас возникает потребность в функциональном символе последователя $S$ с определенными свойствами.

Имея возможность перечислять (нумеровать) предметы, мы можем рассуждать о величине объема понятия в зависимости от того, на каком натуральном числе нумерация объема понятия была исчерпана (если это вообще возможно), принимая его за меру этого объема.

Для сравнения объемов понятий мы хотели бы уметь сравнивать эти меры объемов, т.е. определять, какой из них меньше. И на этом этапе сначала возникает концепция *порядка* на натуральных числах, причем линейного порядка, чтобы мы могли уверенно сравнивать любые два натуральных числа. Но из теоретико-множественных соображений мы также понимаем, что помимо ответа на вопрос, «содержится ли объем $A$ в объеме $B$», можно задавать и другие вопросы, например, «как велика разница между этими объемами?» или «сколько осталось добавить к объему $A$, чтобы получить объем $B$?»

Отсюда мы выходим на концепцию операции сложения (и вычитания) на натуральных числах. Мы понимаем, что прибавление числа $n$ к числу $m$ должно означать для нас $n$-кратное выполнение операции перехода к последователю, т.е. $m + n$ будет определяться рекурсивно через базовую операцию $S$. Отсюда же можно заметить, что через сложение объемов можно определить и сравнение: меньше тот объем, к которому надо что-то прибавить, чтобы получить больший. Поэтому часто сравнение натуральных чисел вводится уже после формализации арифметики как определение внутри формальной теории.

Наконец, натуральные числа можно рассматривать еще и как способ пересчитывать сами арифметические операции или, иначе говоря, определять кратность этих операций. Так, кратность операции сложения есть умножение. Поэтому мы можем (но не должны) включить в нашу концепцию операцию умножения. Эту тему можно развивать и дальше, переходя к операции возведения в степень, затем — к башне степеней, и так далее, вводя так называемую иерархию быстро растущих функций, но здесь мы ограничимся лишь первым шагом — умножением. Этого вполне достаточно, чтобы принципиально усилить свойства арифметики.

Итак, перейдем к формализации понятия натурального числа, следуя схеме из таблицы B1.1.

### B2.1.1 Язык и аксиомы

Для начала определимся с алфавитом, в который мы включим буквы $a, \dots, z$, а также их модификации с помощью штрихов и цифровых (имеются в виду цифры $0, \dots, 9$) индексов в качестве обозначений переменных, причем к свободным переменным отнесем символы из начала алфавита, а к связанным — из конца (обычно это $u, v, w, x, y, z$). Наличие штрихов у символов переменных позволяет производить потенциально сколь угодно много новых переменных, но мы постараемся обходиться лаконичными записями.

Далее мы включаем в алфавит круглые и квадратные скобки, как взаимозаменяемые

(чтобы иметь возможность некоторые скобки выделить на фоне остальных), а также знаки логических связок и кванторов.

Наконец, определим сигнатуру. Константы: 0. Функциональные символы: $S$ (унарный), $+, \cdot$ (бинарные). Предикатные символы: $=, <$ (бинарные). Также сразу оговоримся, что вместо $S(n)$ мы часто будем писать $Sn$, если это не вызывает путаницы, вместо $+(a,b)$ пишем $(a+b)$, вместо $\cdot(a,b)$ пишем $a\cdot b$ или еще короче $ab$, вместо $=(a,b)$ пишем $a=b$, вместо $\neg(a=b)$ пишем $a\neq b$, вместо $<(a,b)$ пишем $a<b$ или $b>a$. Таким образом у нас отпадает необходимость включать в алфавит языка знак запятой. Кроме того, сразу же введем два сокращения для нестрого неравенства: $(a\leqslant b)\overset{\text{def}}{\rightleftharpoons}(a<b)\vee(a=b)$, $(a\geqslant b)\overset{\text{def}}{\rightleftharpoons}(a>b)\vee(a=b)$.

Далее, мы принимаем все естественные правила редуцирования скобок в соответствии с приоритетами арифметических операций, чтобы сделать текст формул и термов более удобочитаемым.

Тем самым язык определен, осталось добавить аксиомы. Как уже отмечалось, аксиомы классической логики предикатов первого порядка и правила вывода предполагаются автоматически. И, как обычно, мы используем нетерминальные символы $\varphi, \psi$ (возможно, с добавлением цифровых индексов) для обозначения произвольных формул с указанием следом в скобках переменных, которые могут входить в текст этих формул (здесь нам потребуется запятая, но она уже будет элементом мета-языка).

Теперь выпишем список аксиом **первопорядковой арифметики Пеано**, после чего обсудим их смысл:

PA1 $a=a$; $(a=b)\to(b=a)$; $(a=b)\wedge(b=c)\to(a=c)$;

PA2 $a=b\to S(a)=S(b)$;

PA3 $S(a)=S(b)\to(a=b)$;

PA4 $S(a)\neq 0$;

PA5 $a+0=a$; $a+Sb=S(a+b)$;

PA6 $a\cdot 0=0$; $a\cdot Sb=ab+a$;

PA7 $\neg(a<0)$; $(a<Sb)\leftrightarrow(a<b)\vee(a=b)$;

PA8 $\varphi[a/0]\wedge[\forall x\,\varphi[a/x]\to\varphi[a/Sx]]\to\forall y\,\varphi[a/y]$.

Группа аксиом PA1 суть стандартные аксиомы равенства и включены, как мы уже говорили, потому что для предиката равенства они всегда должны быть включены в теорию (либо как аксиомы, либо как теоремы).

Аксиома PA2 есть воплощение аксиомы конгруэнтности для термов. Точнее, из этой аксиомы с помощью остальных аксиом, а также индукцией по сложности формулы можно вывести конгруэнтность в общем виде (B1.9).

Остальные аксиомы уже являются собственными аксиомами арифметики. PA3 говорит нам, что функция $S$ инъективна, т.е. что последователи разных чисел есть разные числа, что соответствует нашим представлениям о нумерации как о взаимно однозначном сопоставлении.

Аксиома PA4 утверждает, что ноль не является ничьим последователем, т.е. есть первый элемент среди чисел. Этим мы реализуем принцип особенности нуля как единственного стартового нумерала.

Кстати, термы вида $S\ldots S0$ принято называть *нумералами*. Нумералы являются записями всех натуральных чисел, которые можно построить за конечное число шагов (можно также сказать, что нумералы — это архимедовы натуральные числа).[1] Мы можем придумать для нумералов более привычные обозначения, дав такие определения:

$$1 \overset{\text{def}}{\rightleftharpoons} S(0), \quad 2 \overset{\text{def}}{\rightleftharpoons} S(1), \quad 3 \overset{\text{def}}{\rightleftharpoons} S(2), \quad 4 \overset{\text{def}}{\rightleftharpoons} S(3), \quad 5 \overset{\text{def}}{\rightleftharpoons} S(4), \quad \text{и т.д.}$$

Кстати говоря, символ $\overset{\text{def}}{\rightleftharpoons}$ можно понимать не только как оператор из мета-теории, но частично воспринимать его и как часть языка арифметики, т.е. как предикат, подчиненный аксиомам

$$(F \overset{\text{def}}{\rightleftharpoons} T) \to (F = T), \quad (P \overset{\text{def}}{\leftrightarrow} \varphi) \to (P \leftrightarrow \varphi), \tag{B2.1}$$

где $F$ — не использовавшийся в аксиоматике функциональный (или константный) символ, $T$ — произвольный терм, не содержащий символа $F$, $P$ — не использовавшийся в аксиоматике предикатный символ, $\varphi$ — произвольная формула, не содержащая предикат $P$. Выше таким способом были определены предикаты $(a \neq b)$, $(a \leqslant b)$. Таким образом те термы (формулы), которые равны по определению, равны (эквивалентны) и в смысле исходного языка (но не наоборот).

Однако не все наши прошлые и будущие переобозначения с помощью символа $\overset{\text{def}}{\rightleftharpoons}$ сводятся к данным правилам, поэтому в целом принято считать такого рода сокращения формальных текстов «синтаксическим сахаром» на уровне мета-теории и не включать данный символ в исследуемый формализм.

Группа аксиом PA5 определяет сложение рекурсивно через операцию последователя. Во-первых, задает базу $(a + 0 = a)$, во-вторых, определяет добавление последователя как последователь предыдущей суммы $(a+Sb = S(a+b))$. Если понимать оператор $S$ как прибавление единицы, то эти равенства становятся очевидными. Более того, используя уже введенные обозначения, получаем, что $a + 1 = a + S0 = S(a + 0) = Sa$, где мы воспользовались аксиомой PA5, PA2, а также транзитивностью равенства и правилом Modus Ponens.

Группа аксиом PA6 точно так же задает рекурсивно операцию умножения. Как уже отмечалось, можно добавлять аналогичные аксиомы для других производных операций, например, для степени, получая более продвинутые арифметические теории.[2]

Группа аксиом PA7, во-первых, говорит, что ноль есть минимальный элемент (меньше нуля ничего нет). Во-вторых, задает рекурсивное правило для сравнения любых двух чисел. В качестве упражнения можно попробовать доказать, например, что $2 < 5$.

Наконец, самая главная аксиома арифметики Пеано — аксиома индукции PA8. Точнее, это целая серия (схема) аксиом, а каждая конкретная аксиома индукции получается заменой $\varphi$ на конкретную формулу языка арифметики. При этом мы, как обычно,

[1] Ирония состоит в том, что архимедовость как раз через натуральные числа и определяется. Но в этом определении имеются в виду натуральные числа из стандартной модели. Построение нестандартных моделей лежит за пределами этой книги.

[2] На самом деле есть существенная разница между умножением и всеми остальными рекурсивными операциями, а именно: корректность рекурсивных определений невозможно доказать без привлечения умножения (т.к. при кодировании формул используется деление с остатком — см. раздел D3.4). Поэтому умножение можно определить через сложение, но нельзя доказать тотальность и корректность такого определения, в то время как степень и все более высокие рекурсии при наличии умножения определяются доказуемо корректно. Поэтому умножение принято сразу включать в аксиоматику.

отмечаем, что вместо переменной $a$ можно подставлять любую свободную переменную, а вместо $x$ и $y$ — любые связанные переменные, которых нет в исходной формуле $\varphi$.

Важность аксиомы индукции заключается в том, что она делает арифметику Пеано намного более сильной теорией, чем теория без индукции. Это видно по многочисленным свойствам разных арифметик, более слабых, чем рассматриваемая арифметика.

Теория, порожденная аксиомами PA1–8 в логике предикатов первого порядка, называется **арифметикой Пеано** и обозначается PA.

**Теорема B2.1.** *В теории* PA *верны следующие теоремы (с учетом универсального замыкания формул):*

1° $a + b = b + a$ [коммутативность сложения];

2° $a + (b + c) = (a + b) + c$ [ассоциативность сложения];

3° $ab = ba$ [коммутативность умножения];

4° $a(b + c) = ab + ac$ [дистрибутивность];

5° $a(bc) = (ab)c$ [ассоциативность умножения];

6° $(a < b) \leftrightarrow (Sa < Sb)$ [согласованность порядка с $S$];

7° $(a + c = b + c) \to (a = b)$ [правило сокращения для $+$];

8° $(a < b) \leftrightarrow (a + c < b + c)$ [согласованность порядка с $+$];

9° $<$ есть линейный порядок;

10° $(c \neq 0) \to [(a < b) \leftrightarrow (ac < bc)$ [согласованность порядка с $\cdot$];

11° $(ac = bc) \wedge (c \neq 0) \to (a = b)$ [правило сокращения для $\cdot$];

12° $(a \leqslant b) \wedge (b < Sa) \to (b = a)$ [дискретность порядка];

13° $a \cdot S0 = a$ [нейтральность единицы];

14° $(a \cdot b = 0) \to (a = 0 \vee b = 0)$ [отсутствие делителей нуля].

Доказательство этой теоремы мы будем разбирать во второй части книги (см. теорему D3.1). Смысл ее в том, что натуральные числа с операциями сложения и умножения и порядком $<$ образуют структуру, которая на алгебраическом языке называется *упорядоченным дискретным коммутативным полукольцом с единицей*. Стоит отметить, что далеко не все такие полукольца являются моделями PA, поскольку свойства такого кольца не гарантируют выполнения аксиомы индукции. Тем не менее, как видим, аксиомы PA являются достаточными для того, чтобы получить все базовые свойства чисел, которые мы помним и любим с детства.

Отметим также, что все перечисленные свойства суть теоремы формальной теории PA. Они формулируются и доказываются без привлечения внешних средств (метатеории). Продемонстрируем это на примере доказательства базы индукции для коммутативности сложения, т.е. на примере формулы $0 + a = a + 0$. Доказательство проведем индукцией по $a$.

1. База $0 + 0 = 0 + 0$ следует из PA1 подстановкой $[a/0 + 0]$;

2. Индуктивный переход: $(0 + a = a + 0) \to (0 + Sa = Sa + 0)$. align

2.1. $0 + a = a + 0$ (гипотеза) и $(0 + a = a + 0) \to S(0 + a) = S(a + 0)$ (подстановка $[a/a + 0; b/0 + a]$ в PA2);

2.2. $S(0 + a) = S(a + 0)$ (гипотеза и Modus Ponens);

2.3. $0 + Sa = S(0 + a)$ (подстановка $[a/0; b/a]$ в PA5);

2.4. $(0 + Sa = S(0 + a)) \wedge (S(0 + a) = S(a + 0))$ (тавтология $\mathscr{A} \to (\mathscr{B} \to (\mathscr{A} \wedge \mathscr{B}))$ и дважды MP, это правило называется «объединение посылок»[3] );

2.5. $0 + Sa = S(a + 0)$ (транзитивность равенства, MP);

2.6. $S(a + 0) = Sa$ (PA5, подстановка $[a/a + 0]$ в PA2, MP);

2.7. $0 + Sa = Sa$ (транзитивность равенства, MP);

2.8. $Sa = Sa + 0$ (PA5$[a/Sa]$, симметричность равенства, MP);

2.9. $0 + Sa = Sa + 0$ (объединение посылок, транзитивность равенства, MP);

2.10. $(0 + a = a + 0) \to (0 + Sa = Sa + 0)$ (теорема о дедукции).

3. $\forall x\ (0 + x = x + 0) \to (0 + Sx = Sx + 0)$ (введение квантора по правилу (R1))[4]

4. $(0 + 0 = 0 + 0) \wedge [\forall x\ (0 + x = x + 0) \to (0 + Sx = Sx + 0)]$ (объединение посылок);

5. $\forall y\ (0 + y = y + 0)$ (индукция для формулы $\varphi \overset{\text{def}}{\rightleftharpoons} (0 + a = a + 0)$).

Отправляясь от полученной формулы, уже можно доказывать коммутативность сложения $a + b = b + a$ индукцией по $b$.

Прежде чем пойти дальше, мы должны закрыть вопрос о конгруэнтности равенства в ее самом широком смысле, а именно, получить свойства (B1.9). Справедлива следующая

**Теорема B2.2** (Конгруэнтность). *Пусть $T, T_1, T_2$ — произвольные термы языка PA, $\varphi$ — произвольная формула языка PA, тогда*

$$(T_1 = T_2) \to T[a/T_1] = T[a/T_2]; \quad (T_1 = T_2) \to (\varphi[a/T_1] \leftrightarrow \varphi[a/T_2]),$$

*где $[a/T_i]$ означает замену всех вхождений свободной переменной $a$ на терм $T_i$, причем указанные формулы справедливы и для любой другой свободной переменной (не только $a$).*

Полное доказательство этой теоремы будет продемонстрировано в Части II, теорема D3.2.

Таким образом у нас нет необходимости включать в аксиоматику PA схемы аксиом конгруэнтности, вместо этого мы добавляем базовое правило конгруэнтности для оператора $S$ и используем всю мощь арифметической индукции.[5]

---

[3] Оно выглядит так: $\frac{\varphi \quad \psi}{\varphi \wedge \psi}$

[4] Используется упрощенный вариант правила Бернайса, называемый *правилом обобщения*: $\frac{\psi}{\forall x\ \psi[a/x]}$, где $x$ не входит в $\varphi$. Это правило легко выводится из правила Бернайса, если в нем вместо посылки $\varphi$ подставить любую общезначимую формулу.

[5] Под «всей мощью» здесь следует понимать тот факт, что многие теоремы доказываются так называемой вложенной, или многопараметрической, индукцией, когда база или шаг одной индукции получаются применением второй индукции, и т.д.

### B2.1.2 Порядок

В предыдущем разделе, обсуждая суть понятия «натуральные числа», мы говорили о том, что число $a$ можно считать меньшим (или не большим) числа $b$, если $b$ получается добавлением к $a$ какого-нибудь числа. Мы тогда оперировали словом «объем», подразумевая, что числа измеряют какие-то объемы понятий. Однако потом в аксиомах мы ввели определение неравенства рекурсивно в группе аксиом PA7.

Но ничто не мешает нам ввести еще одно определение неравенства, полагая

$$\text{PA7'} \qquad (a <_1 b) \leftrightarrow \exists x\ (b = a + Sx).$$

Оказывается, что в рамках аксиоматики PA эти два определения задают один и тот же порядок. Точнее, справедлива

**Теорема B2.3.** $(a < b) \leftrightarrow (a <_1 b)$.

Эта формула уже является собственной теоремой арифметики PA (с точностью до универсального замыкания). Доказательство теоремы будет дано в Части II, лемма D3.2.

С неравенством связаны два варианта упрощенной записи кванторов, так называемые *ограниченные кванторы*. Они определяются следующим образом:

$$\forall x < b:\ \varphi[a/x] \overset{\text{def}}{\leftrightarrow} \forall x\ (x < b) \to \varphi[a/x], \quad \exists x < b:\ \varphi[a/x] \overset{\text{def}}{\leftrightarrow} \exists x\ (x < b) \wedge \varphi[a/x], \tag{B2.2}$$

где $\varphi$ — арифметическая формула, $a, b$ — свободные переменные. Первая формула, как нетрудно видеть, возвращает истинное значение тогда и только тогда, когда формула $\varphi$ истинна для всех значений параметра $a$, меньших, чем параметр $b$. Вторая формула истинна тогда и только тогда, когда формула $\varphi$ истинна хотя бы при каком-то значении параметра $a$, меньшем, чем параметр $b$.

В логике предикатов несложно доказать, что

$$\neg(\forall x < b:\ \varphi[a/x]) \leftrightarrow (\exists x < b:\ \neg\varphi[a/x]),$$
$$\neg(\exists x < b:\ \varphi[a/x]) \leftrightarrow (\forall x < b:\ \neg\varphi[a/x]),$$

т.е. эти кванторы ведут себя точно так же, как и основные, что вполне соответствует здравому смыслу.

Ограниченные кванторы хороши тем, что для определения их истинности достаточно осуществить конечное количество вычислений формулы $\varphi$. По сути они воплощают реализацию цикла for в арифметике. Наличие таких кванторов сильно упрощает вычислимость формул с кванторами, поэтому формулы, в которых все кванторы ограничены, даже вынесены в отдельный класс формул и называются $\Delta_0$-формулами. [6]

Стоит отдельно отметить, что если мы отказываемся от введения в аксиоматику отношения $<$, но хотим использовать ограниченные кванторы, то мы, конечно, можем их определить, раскрыв определение неравенства в сильной форме, однако само по себе такое определение перестанет быть $\Delta_0$-формулой, поскольку будет использовать неограниченные кванторы. Таким образом введение в аксиоматику неравенства (хотя бы и в слабой форме) делает арифметику более сильной в том смысле, что оно позволяет определять класс $\Delta_0$-формул, хотя с точки зрения доказательной силы эти теории равносильны: теория PA без неравенства и теория PA с неравенством содержат одни и те же теоремы (с точностью до раскрытия знака $<$).

[6] Класс $\Delta_0$-формул — это лишь нижняя ступенька так называемой арифметической иерархии формул, в которой все формулы делятся на классы в зависимости от порядка и количества перемен типов канторов в формуле — см., например, [28].

### B2.1.3 Варианты индукции

Ранее уже отмечалось, что существует несколько утверждений, равносильных арифметической индукции. Здесь мы рассмотрим лишь некоторые. Пусть $\varphi$ — формула языка PA, и $a$ — свободная переменная, входящая в эту формулу. Введем следующие обозначения с помощью схемы определений:

$$\begin{aligned} Ind_a[\varphi] &\overset{\text{def}}{\leftrightarrow} \varphi[a/0] \wedge \forall x\ (\varphi[a/x] \to \varphi[a/Sx]) \\ Prog_a[\varphi] &\overset{\text{def}}{\leftrightarrow} \forall x\ ((\forall y < x:\ \varphi[a/y]) \to \varphi[a/x]) \\ Tot_a[\varphi] &\overset{\text{def}}{\leftrightarrow} \forall y\ \varphi[a/y] \end{aligned}$$

Первая схема выражает *индуктивность* формулы $\varphi$, вторая — *прогрессивность*, третья — *тотальность*. Аксиома индукции PA8 с помощью схемы индуктивности записывается, очевидно, так:

$$Ind_a[\varphi] \to Tot_a[\varphi], \tag{B2.3}$$

т.е. если формула $\varphi$ индуктивна, то она тотальна. Это вполне соответствует обычному представлению о математической индукции, когда речь идет не о формулах, а о множествах, т.е. по сути об объемах понятий. В арифметике, в которой мы допускаем использование понятия «множество» (второпорядковой арифметике), индукция формулируется так: если множество индуктивно, то оно тотально (т.е. содержит все натуральные числа). А индуктивность означает, что в этом множестве есть число 0, а также вместе с каждым числом есть его последователь.

В нашем случае та же идея просто записана формулами.

Используя формулу прогрессивности, можно записать так называемую **полную** (или *возвратную*) индукцию:

$$Prog_a[\varphi] \to Tot_a[\varphi]. \tag{B2.4}$$

Индукция в виде (B2.3), т.е. PA8, в таком случае называется *локальной*.

Свойство прогрессивности выглядит как более слабое, поскольку в нем мы говорим следующее: если *все* элементы, меньшие, чем $x$, удовлетворяют $\varphi$, тогда $x$ тоже удовлетворяет $\varphi$. Для множеств это можно сформулировать так: если все элементы меньшие $x$ принадлежат данному множеству, то и сам $x$ ему принадлежит. Посылка прогрессивности накладывает больше условий на $\varphi$, чем посылка индуктивности, а значит, прогрессивность не сильнее, чем индуктивность. И действительно, нетрудно проверить, что всегда верно $Ind_a[\varphi] \to Prog_a[\varphi]$.

А отсюда уже вытекает, что из полной индукции следует локальная, т.е. формально полная индукция выглядит сильнее, чем ее локальный вариант. Однако в арифметике PA обе эти индукции равносильны.

**Теорема B2.4.** *Схема полной индукции равносильна схеме локальной индукции по модулю остальных аксиом* PA.

За доказательством мы, как обычно, отсылаем ко второй части книги (теорема D3.3), но подчеркнем, что эта теорема является мета-теоремой, она вовсе не означает вывод эквиваленции формул (B2.3) и (B2.4) для *каждой конкретной* формулы $\varphi$. Она говорит, что если мы принимаем *всю* схему одной индукции, то можем вывести (средствами PA) *всю* схему другой индукции, и наоборот.

Проведем теперь следующие чисто формальные манипуляции с формулами, пользуясь лишь исчислением предикатов:

$$\begin{gathered} Prog_a[\varphi] \to Tot_a[\varphi] \equiv \neg Tot_a[\varphi] \to \neg Prog_a[\varphi] \equiv \\ \equiv (\exists y\ \neg\varphi[a/y]) \to \exists x\ \neg((\forall y < x\ \varphi[a/y]) \to \varphi[a/x]) \equiv \\ \equiv (\exists y\ \neg\varphi[a/y]) \to \exists x\ ((\forall y < x\ \varphi[a/y]) \wedge \neg\varphi[a/x]). \end{gathered}$$

Теперь обозначим $\psi \overset{\text{def}}{\leftrightarrow} \neg\varphi$ и получим:

$$Prog_a[\varphi] \to Tot_a[\varphi] \equiv (\exists y\ \psi(y)) \to \exists x\ (\psi(x) \wedge \forall y < x :\ \neg\psi(y)),$$

где мы убрали уже поднадоевшую нам подстановку связанной переменной вместо свободной, упростив запись на мета-уровне.

Таким образом мы видим, что если верна схема полной индукции (а она верна в PA), то верна и такая схема:

$$(\exists y\ \psi(y)) \to \exists x\ (\psi(x) \wedge \forall y < x :\ \neg\psi(y)), \tag{B2.5}$$

поскольку здесь формула $\psi$ может быть выбрана любая (ведь в схеме полной индукции стоит произвольная формула $\varphi$).

Схема (B2.5) называется **принципом фундированности** натуральных чисел.

Почему так? Дело в том, что среди частичных порядков (и даже предпорядков) принято выделять такие, которые обладают тем свойством, что каждое непустое множество имеет *минимальный элемент* (т.е. такой элемент, меньше которого в этом множестве элементов нет). В случае множеств (объемов понятий) это свойство формально записывается так:

$$(A \neq \varnothing) \to \exists(x \in A)\ \forall y < x :\ (y \notin A).$$

Но теперь представим себе, что множество $A$ есть объем понятия, определяемого формулой $\psi$, т.е. вместо $x \in A$ можно писать $\psi(x)$. Тогда наше теоретико-множественное определение фундированности превращается в формулу (B2.5).

Таким образом, чисто логико-предикатными выкладками мы показали, что принцип фундированности в языке PA (т.е. даже без участия каких-либо аксиом PA) равносилен принципу полной индукции. А в силу теоремы B2.4 он оказывается равносилен и обычной индукции, только уже в рамках аксиоматики PA.

Но и это еще не все. Преобразуем теперь принцип индукции чуть-чуть иначе, снова в чистом исчислении предикатов:

$$\begin{gathered} Prog_a[\varphi] \to Tot_a[\varphi] \equiv \neg Tot_a[\varphi] \to \neg Prog_a[\varphi] \equiv \\ \equiv (\exists y\ \neg\varphi(y)) \to \neg(\forall x\ ((\forall y < x :\ \varphi(y)) \to \varphi(x))) \equiv \\ \equiv (\exists y\ \neg\varphi(y)) \to \neg(\forall x\ (\neg\varphi(x) \to \exists y < x :\ \neg\varphi(y))) \end{gathered}$$

где мы воспользовались равносильностью $\mathscr{A} \to \mathscr{B} \equiv \neg\mathscr{B} \to \neg\mathscr{A}$. Теперь снова заменим $\neg\varphi$ на $\psi$ (выбор формулы остается произвольным), и получим такую схему, равносильную полной индукции:

$$(\exists y\ \psi(y)) \to \neg(\forall x\ (\psi(x) \to \exists y < x :\ \psi(y))). \tag{B2.6}$$

Вдумаемся в эту формулу, представив, что $\psi$ задает некий объем понятия $A$, и подменяя $\psi(x)$ на $(x \in A)$. Тогда этот принцип можно понять так: если $A$ не пусто, то не верно, что

для любого элемента $A$ найдется меньший его элемент $A$. Иначе говоря, внутри множества $A$ невозможно спускаться вниз по неравенству $<$ бесконечно долго (при каком-то $x$ нельзя будет найти меньший его элемент $A$).

Таким образом, (B2.6) реализует в арифметике Пеано еще один важный принцип — **невозможность бесконечного спуска**, использованный Ферма еще в 17-м веке для доказательства своей знаменитой теоремы в случае $n = 4$.

Итак, в рамках аксиоматики PA следующие четыре принципа равносильны (как схемы):

- локальная индукция;
- полная индукция;
- фундированность;
- невозможность бесконечного спуска,

причем последние три равносильны в чистом исчислении предикатов (т.е. определение значка $<$ в этом случае неважно).

### B2.1.4 Доказуемость и выразимость

Чтобы подчеркнуть в очередной раз значимость индукции для арифметики, посмотрим на нее с точки зрения мета-теории. Ведь индукция (в локальной форме) по сути заявляет, что если что-то верно в нуле, а также верен переход от $x$ к $x + 1$ (он же $Sx$), то оно верно для всех натуральных чисел.

Но теперь представим, что мы умеем доказывать отдельные теоремы вида $\varphi(\underline{n}) \to \varphi(\underline{n+1})$ для каждого конкретного $n$, т.е. для каждого нумерала $\underline{n} \overset{\text{def}}{\rightleftharpoons} \underbrace{S \ldots S}_{n} 0$. Будет ли тогда доказуема формула тотальности свойства $\varphi$? Оказывается нет. И в этом скрывается очень тонкое свойство квантора всеобщности, зашитого в формулу $Tot_a[\varphi]$.

Это тонкое свойство заключается в том, что если с точки зрения мета-теории верна формула $\forall n\ \varphi(\underline{n})$, то внутри самой теории PA формула тотальности $\forall n\ \varphi(n)$ не обязана быть верной (напоминание: красный квантор написан в языке мета-теории). Тому есть многочисленные примеры, вытекающие из теории рекурсивных функций.

Рассмотрим это на примере. Пусть $G(n)$ — функция Гудстейна.[7] Для каждого конкретного нумерала $\underline{n}$ мы можем доказать в PA, что значение функции Гудстейна в точке $\underline{n}$ определено:

$$\forall n\ \mathrm{PA} \vdash \exists y\ (G(\underline{n}) = y),$$

т.е. существует конечная цепочка формул (очень длинная для больших $n$), которая является доказательством формулы $\exists y\ G(\underline{n}) = y$ для каждого конкретного нумерала, изображающего число $n$.

Однако уже формула тотальности функции $G$ не имеет доказательства (как и опровержения) в PA:

$$\mathrm{PA} \nvdash \forall x\ \exists y\ (G(x) = y).$$

Иначе говоря, как только мы захотели внести квантор всеобщости в запись теоремы PA, она перестала быть теоремой.

[7] Сейчас не важно, что это такое, важно только понимать, что равенство $y = G(x)$ можно записать арифметической формулой.

Поэтому, несмотря на кажущуюся бесхитростность принципа локальной индукции, который мы часто воспринимаем как нечто само собой разумеющееся, он вносит существенный вклад в доказательную силу теории. Более того, принцип индукции можно ослаблять различными способами (запрещая вложенные индукции или применяя схему индукции не ко всему классу формул, а только к некоторому подклассу, например, только к $\Delta_0$-формулам), получая при этом великое разнообразие арифметических теорий в одном и том же языке.

Наконец, существует возможность классифицировать арифметические теории по их доказательной силе путем нахождения класса рекурсивных функций, для которых эта теория умеет доказывать их тотальность. Приведенный выше пример функции Гудстейна показывает, что есть такие рекурсивные функции, тотальность которых не может доказать даже PA со схемой индукции без ограничений по параметрам и классам формул.

Стоит добавить, что арифметику можно, наоборот, усиливать, добавляя к ней ранее недоказуемые принципы (например, теорему Гудстейна), либо же усиливая ее язык путем перехода к так называемой второпорядковой арифметике, допускающей наличие произвольных арифметических множеств. В такой арифметике индукция приобретает привычные со школы черты, т.к. формулируется как свойство множеств, а не формул. И в такой арифметике теоремы, подобные теореме Гудстейна, а также многие теоремы математического анализа становятся доказуемыми.

Наряду с доказуемостью какого-либо математического факта нужно также говорить и о его выразимости в той или иной арифметике. Действительно, возможность записать формулой произвольный умозрительный факт не всегда оказывается доступной в каждом конкретном языке.

Например, в случае упоминавшейся функции Гудстейна, мы в состоянии записать формулу ее тотальности $\forall x\ \exists y\ G(x) = y$, поскольку вычисление функции Гудстейна представляет собой понятную алгоритмическую процедуру вычисления (вообще, любая программируемая на компьютере функция может быть определена достаточно простой (с точки зрения кванторной структуры) формулой языка PA, см. теорему D3.8).

Однако если посмотреть на натуральные числа с общей математической точки зрения, то можно заметить, что существует более чем счетное (континуальное) множество подмножеств натурального ряда, в то же время в языке PA есть лишь счетное множество формул. Следовательно, далеко не всякое подмножество натурального ряда можно описать формулой.

Например, мы можем определенным способом закодировать все предложения языка PA, присвоив им т.н. геделевы номера. Это делается довольно просто примерно так же, как в компьютере любой текст представляется последовательностью битов, т.е. каким-то огромным числом. Затем мы можем выделить среди геделевых номеров только те, которые соответствуют истинным (с точки зрения общей математики, т.е. метатеории) предложениям. Множество всех таких номеров, очевидно, есть подмножество натурального ряда, однако известно, что в языке PA не существует формулы $True(x)$, которая была бы истинной на всех номерах истинных предложений, и только на них. Это утверждение является содержанием *теоремы Тарского о невыразимости истины*.

Арифметика, тем не менее, является очень мощным языком в плане того, какие математические факты в ней можно выразить. Это касается не только теоремы Гудстейна или таких теорем, как Великая теорема Ферма или китайская теорема об остатках.

Поэтому проще всего приводить примеры невыразимости для более слабых языков. Так, если мы возьмем теорию абелевых групп без кручения (например, целые числа с

операцией сложения), то в такой теории нельзя выразить отношение $<$ (хотя, как мы видели выше, в натуральных числах это возможно). Но если мы добавим умножение, то в кольце целых чисел (но не в любом кольце!) порядок уже можно выразить следующим способом:

$$a < b \overset{\text{def}}{\leftrightarrow} \exists x_1, x_2, x_3, x_4 :\ Sa + x_1 \cdot x_1 + x_2 \cdot x_2 + x_3 \cdot x_3 + x_4 \cdot x_4 = b,$$

что является следствием теоремы Лагранжа.

Еще пример (без детализации): в сигнатуре языка первопорядковой геометрии невыразимы такие объекты как: единичный отрезок; любая фигура, кроме всей плоскости; направление вдоль какой-то оси и т.п.

Таким образом мы видим, что у формальных языков и теорий есть существенные ограничения по сравнению с общей математикой (наивной теорией множеств):

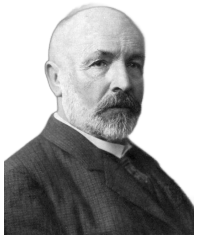
- не любое понятие из модели языка/теории может быть выражено (определено) в этом языке;
- даже если какой-то истинный в модели факт удалось выразить формулой языка, его не всегда можно доказать или опровергнуть в соответствующей формальной теории.

Всеми этими вопросами занимается комплекс дисциплин в основаниях математики под общим названием **теория доказательств**. Это не просто искусство составления доказательств, а целая наука, которая изучает сами доказательства как математические объекты. Подобно тому как лингвистика изучает структуру языка, теория доказательств, начиная с работ Герхарда Генцена, анализирует «анатомию» формальных выводов, их сложность и выразительную силу.

Именно в рамках теории доказательств получают строгую оценку «силы» той или иной аксиоматической системы. Например, чтобы доказать непротиворечивость арифметики Пеано, требуются методы, выходящие за рамки самой этой арифметики. Одним из центральных направлений здесь является *ординальный анализ*, который сопоставляет каждой теории некоторый трансфинитный ординал, служащий мерой ее «доказательной силы». Так, силе PA соответствует ординал $\varepsilon_0 = \omega^{\omega^{\omega^{\cdots}}}$, что наглядно показывает, насколько далеко за пределы «обычной» индукции нужно выйти, чтобы охватить ее с мета-математической высоты. Таким образом, столкнувшись с границами формализма, математики превратили изучение этих границ в новую, глубокую и активно развивающуюся область исследований.

## B2.2. Пролегомены к теории множеств

Прежде чем мы перейдем к строгой аксиоматической теории, необходимо отдать дань уважения ее создателю — **Георгу Кантору**. Именно он в конце XIX века совершил революцию, предложив рассматривать бесконечные совокупности не как потенциальный, незавершенный процесс, а как полноценные математические объекты — **множества** (нем. *Mengen*). Его подход, который сегодня называют *наивной теорией множеств*, основывался на интуитивно ясном принципе: *любому свойству $\mathscr{A}(a)$ соответствует множество всех объектов $a$, обладающих этим свойством*.



*Георг Кантор*

Вооружившись этим мощным принципом, Кантор разработал инструменты для сравнения бесконечных множеств. Он предложил считать два множества (конечных или бесконечных) равномощными, если между их элементами можно установить взаимно-однозначное соответствие (биекцию). Это привело его к ошеломляющему открытию: существуют разные «размеры» бесконечности. С помощью своего знаменитого *диагонального аргумента* он доказал, что множество всех подмножеств натуральных чисел (континуум) является «более мощным», чем само множество натуральных чисел. Так родилась теория транфинитных кардинальных и ординальных чисел — арифметика бесконечности.

Именно этот первоначальный, интуитивный и чрезвычайно плодотворный подход и есть тот «рай», который, по выражению Гильберта, создал для математиков Кантор. Однако очень скоро выяснилось, что в этом раю есть свои червоточины. Неограниченное применение принципа свертывания (любое свойство задает множество) привело к обнаружению логических парадоксов, самый известный из которых — парадокс Рассела (см. ниже). Стало ясно, что для спасения теории множеств от противоречий необходимо ограничить способы построения множеств, явно перечислив разрешенные операции в виде аксиом. Эту задачу и взялся решить Цермело.

В разделе A2.3 мы уже ввели ряд теоретико-множественных обозначений для операций и предикатов, связанных с понятием множества. В разделе A2.7 мы немного расширили этот аппарат, добавив такие важные понятия, как отношение и функция. Теперь же наша задача состоит в том, чтобы в максимально упрощенном виде дать определение математическому понятию «множество» и затем сформулировать язык и теорию, которые соответствовали бы этому понятию.

Итак, под множеством в широком смысле мы понимаем объем понятия, т.е. любую определяемую совокупность сущностей. Для записи множества как совокупности, определяемой каким-то свойством $\mathscr{A}(a)$, обычно используется сверточная лексема

$$\{x \mid \mathscr{A}[a/x]\},$$

которая читается так: «множество всех $x$, соответствующих свойству $\mathscr{A}$». Чисто логически данная свертка обладает определяющим свойством:

$$a \in \{x \mid \mathscr{A}[a/x]\} \leftrightarrow \mathscr{A}(a). \tag{B2.7}$$

Иначе говоря, сверточная лексема $\{x \mid \mathscr{A}[a/x]\}$ представляет собой специального вида терм, который строится на основе формулы, что в языках первого порядка недопустимо.

Но с другой стороны, сам по себе терм $\{x \mid \mathscr{A}[a/x]\}$ можно рассматривать как синтаксический сахар, определение которого дается на уровне мета-теории. Ведь во всех формулах про множества терм как таковой участвует лишь как операнд предиката. Следовательно, если мы разберемся с тем, как такой терм можно раскрывать в предикатах теории множеств, то мы устраним его из языка как формально ненужную лексему.

Какие же предикаты нужны в теории множеств? В разделе A2.3 было определено несколько предикатов: $\in, =, \subseteq$. На самом деле бывают и другие, но здесь можно заметить, что все они могут быть сведены к одному базовому предикату — *принадлежности*. Действительно, $A \subseteq B$ представляет собой переобозначение формулы $\forall x\ (x \in A) \to (x \in B)$ (всякий элемент $A$ есть элемент $B$), а равенство множеств $A = B$ означает, что всякий элемент $A$ есть элемент $B$ и наоборот, т.е. $\forall x\ (x \in A) \leftrightarrow (x \in B)$.

Принадлежность удобнее всего выбрать как первоначальный предикат, т.к. через нее легко выразить все остальные.

Таким образом мы подходим к тому, что в языке минималистической теории множеств, которую мы хотим построить, можно оставить лишь один (бинарный) предикат: $\in$. Кстати, сразу же добавим определение $(a \notin b) \overset{\text{def}}{\rightleftharpoons} \neg(a \in b)$.

Но в таком случае, если в каком-то месте будет написана формула $a \in \{x \mid \mathscr{A}[a/x]\}$, то мы сможем написать ее существенно короче и, главное, без использования второпорядковых термов, а именно как $\mathscr{A}(a)$. Если же мы встречаем формулу вида $\{x \mid \mathscr{A}[a/x]\} \in b$, то мы можем заменить ее формулой

$$\exists z((z \in b) \wedge \forall x\ (x \in z \leftrightarrow \mathscr{A}(x)))$$

т.е. вместо одной атомарной формулы мы напишем конъюнкцию атомарной формулы и формулы с квантором (вместо терма-свертки появляется формула-свертка, разрешенная в логике предикатов). Это усложнение текста можно рассматривать как плату за избавление от второпорядковых конструкций. Ведь в целом хоть формула и стала длиннее, но она теперь записана в более простом языке. А чем проще язык, тем легче анализировать его возможности.

Избавление от терма $\{x \mid \mathscr{A}[a/x]\}$ не избавляет, тем не менее, от парадоксов теории множеств, в частности, парадокса Рассела, который заключается в следующем. Рассмотрим множество $R$, определяемое формулой $x \notin x$, т.е. $R \overset{\text{def}}{\rightleftharpoons} \{x \mid x \notin x\}$. Иначе говоря, элементами множества $R$ являются те и только те множества $x$, которые не являются элементами самих себя (здесь не принципиально, существуют ли вообще множества-циклы, т.е. являющиеся своими собственными элементами). Вопрос — верно или не верно, что $R \notin R$? Как нетрудно видеть, любое из предположений приводит логически к обратному. Действительно, попробуем избавиться здесь от свертки по правилам, описанным выше: так как $R = \{x \mid x \notin x\}$, то $R \in R$ равносильно $R \notin R$ по правилу (B2.7), что уже дает противоречие, т.к. формула $\mathscr{A} \leftrightarrow \neg\mathscr{A}$ есть тождественная ложь. При этом мы так и не избавились от второпорядкового терма $R$. Это происходит из-за того, что поскольку мы считаем $R$ множеством, то мы вправе подставлять его вместо любой переменной, пробегающей множества, в том числе в формуле $x \notin x$, которая его же и определяет. Возникает так называемое *самореферируемое определение*, когда некоторый объект определяется в том числе и через самого себя. Именно эта возможность переменной $x$ в формуле $x \notin x$ пробегать значение самого множества $R$, которое этой формулой и определяется, создает порочный круг.

Этот пример показателен не только наличием противоречия, но также и тем, что нам не удается корректно избавиться от терма-свертки и перейти к первопорядковому языку из-за зацикленности определения. Если бы мы не предполагали, что $\{x \mid x \notin x\}$ есть корректный терм и, значит, не может быть подставлен в формулу $a \in a$ вместо переменной, то и парадокса бы не было.

Таким образом получается, что наше достаточно свободное определение понятия множества как произвольной определяемой совокупности приводит к очевидным проблемам. Что же делать?

В начале XX века предлагалось несколько решений, одно из которых принадлежит Расселу и представляет собой теорию типов, когда каждый терм вида $\{x \mid \mathscr{A}[a/x]\}$ является множеством более высокого типа, чем те множества $x$, которые используются в его определении. Тем самым сама запись $R \in R$ невозможна, т.к. элементами множеств

какого-либо типа не могут быть множества того же или более высокого типа. Эта конструкция оказалась довольно сложной, к тому же она неявным образом апеллировала к понятию натурального числа, которое требуется для сравнения рангов множеств.

В итоге все сошлись на том, что вместо того, чтобы признавать право быть множеством за любой определяемой совокупностью объектов, проще написать ряд правил, по которым разрешено строить те или иные множества, отправляясь от некоторых атомарных множеств, не имеющих элементов.[8] Отсюда же мы выходим на главный тезис теории множеств: «Все должно быть множеством!». Его следует понимать так, что в этой теории у нас нет никаких других объектов, кроме множеств. Соответственно, формальная теория получается бестиповая, а в атомарном предикате ($a \in b$) оба операнда обязательно являются множествами.

Это ко многому обязывает, т.к. теперь становится затруднительно образовывать, например, множество карандашей, птиц, людей и т.д. Однако ведь и с точки зрения физики все вещи в конце концов являются множествами элементарных частиц, пусть и связанными некоторыми дополнительными соотношениями. Так что вопрос сводится лишь к тому, как эти элементарные частицы считать множествами. А здесь уже вступает в действие некоторая условность. Подобно тому, как в современных ПК существуют таблицы символов (сопоставления букв некоторым числам), созданные однажды произвольным образом, точно так же мы можем считать, что элементарные частицы *закодированы* какими-то произвольно выбранными раз и навсегда множествами.

Более того, нам и атомарное множество достаточно взять всего лишь одно — пустое. Точнее, все атомарные множества пусты по определению (у них нет элементов), но в силу определения равенства они все оказываются попарно равными, т.е. с точки зрения того равенства множеств, о котором мы уже говорили выше, существует лишь одно пустое (атомарное) множество.

Есть модификации теории множеств со многими атомами, равенство которых исключается по определению, поскольку атомам запрещено стоять справа в предикате принадлежности. Однако такая теория является излишне сложной и ничего существенно нового в эту науку не приносит, поскольку может быть легко интерпретирована в классической теории множеств с единственным атомом.

Наличие единственного множества-атома, однако, не избавляет нас от необходимости сопоставлять разным элементарным частицам разные множества. Поэтому моделировать элементарные частицы придется неэлементарными множествами, лишь бы у нас был достаточный запас таковых.

Итак, в сухом остатке мы имеем следующие потребности к языку и теории множеств:

1. единственный тип объектов — множества;
2. единственный атомарный предикат ($a \in b$), где оба операнда — любые множества без ограничений;
3. единственное атомарное множество — пустое;
4. все множества определяются по конечному списку правил, запрещающих идею самореферирования;
5. множеств должно быть потенциально бесконечно много.

[8] Примерно так же, как в физике все строится из элементарных частиц в стандартной модели.

Для того, чтобы выполнить все эти требования, воспользуемся следующей умозрительной концепцией. Будем представлять себе всякое множество в виде дерева (или, если угодно, в виде папки файловой системы, содержащей другие папки, но не файлы!). Само множество — это корень дерева, а его элементы — непосредственные потомки (дочерние узлы) корня, которые также представляются деревьями. В листьях такого дерева всегда стоит пустое множество (см. рис. B2.1). При такой схеме получается, что пустых множеств как бы много — столько, сколько листьев. Однако ничто не запрещает нам считать, что «физически» лист есть только один, а дерево — это развертка (или дерево разбора) множества вдоль отношения принадлежности. Таким образом различные листья на самом деле являются указателями или ссылками на один и тот же уникальный объект — пустое множество. То же самое можно сказать и про другие возможные дубликаты множеств в нашей схеме. Заметим, что если ребра дерева считать не прямым воплощением отношения $\in$, а ссылками на соответствующие элементы (подобно ссылкам на папки в файловой системе), то никаких проблем с единственностью каждого множества не возникнет, несмотря на то, что древовидная развертка может на это указывать.

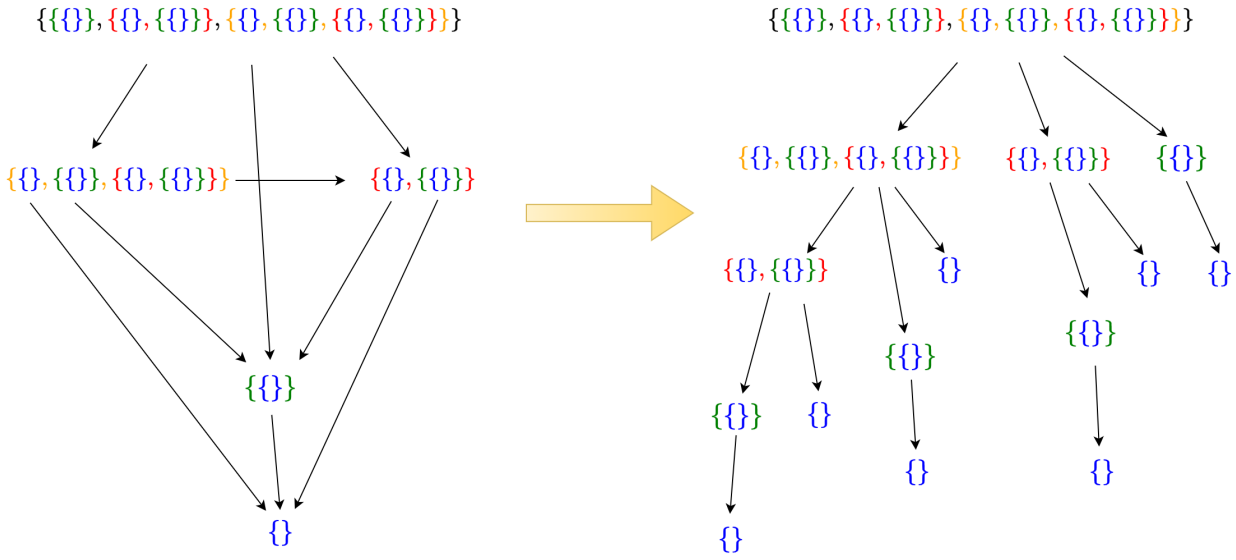


Рис. B2.1. Множество и его развертка деревом.

В рамках данной концепции все описываемые объекты однородны — это деревья (ветви деревьев). Имеется также единственный атомарный объект — дерево, состоящее из одной вершины-корня, и единственное отношение: ребра-ссылки. Здесь также исключены проблемы самореферирования, т.к. если предположить, что имеет место ситуация вида $x \in x$ или более сложная $x \in y \in z \in \cdots \in x$ (цикл по принадлежности), то в дереве множества $x$ будут присутствовать бесконечные пути. В принципе такое, конечно, можно себе представить, но мы будем исходить из финитарной концепции, а бесконечности появятся лишь как надстройки над конечными структурами.

Нетрудно видеть, что и принципы построения множеств с помощью деревьев также ограничены некоторым конечным набором правил, которые по существу сводятся к единственному: возможности линковать уже готовые деревья посредством соединения ребрами листьев одних деревьев и корней других.

Конечно, такой теоретико-графовый подход далек от привычных нам операций над

множествами, однако в данной финитарной концепции понятия «множество» все они могут быть выражены через эту единственную операцию линковки. Действительно, объединение двух деревьев означает по-просту отождествление их корней, в результате чего получается, что все элементы объединяемых множеств становятся потомками одного общего корня вместо многих. Пересечение означает выбор только общих корневых ветвей, а множество всех подмножеств (булеан) означает, напротив, что мы вместо одного корня добавляем много корней, группирующих корневые ветви в различных сочетаниях, а затем линкуем эти новые корни в один общий корень. И так далее.

Заметим, что древовидные объекты преследуют нас на протяжении всей книги, поскольку эта концепция лежит в основе всех регулярных конструкций: лексем, термов и формул, грамматики, логического вывода. Деревья преследуют нас и в жизни всякий раз, когда мы пользуемся файловой системой, каталогами и иерархиями, изучаем генеалогические деревья, строим сценарии развития событий и т.д.

Теперь, имея в виду древовидную концепцию множеств, мы можем проще себе представить, как следует формализовать идею множества в формальном языке. Будем считать, что древовидная концепция является неформальным описанием понятия «множество».

Перейдем к формальной части. Что касается языка, то он оказывается чрезвычайно прост: в нем нет констант, нет функциональных символов, но есть лишь один бинарный предикат $\in$ и два класса переменных — свободные и связанные (здесь мы будем использовать как заглавные, так и строчные латинские буквы, возможно, с цифровыми индексами, по-прежнему считая, что в начале алфавита находятся свободные переменные, а в конце — связанные). Все формулы в таком языке — это комбинации переменных (одного типа), предиката $\in$, логических связок и кванторов. Поразительно, что в таком примитивном языке (но при наличии правильных аксиом) удается выразить любые математические теоремы!

Какие же правила построения множеств нам могут быть полезны в качестве аксиом? Для этого вспомним те операции над множествами, которые мы уже определяли ранее в разделах A2.3 и A2.7:

$$\cap, \cup, \setminus, \Delta, \times,$$

кроме того, нам нужно уметь образовывать множества и упорядоченные наборы из заданных термов путем их перечисления:

$$\{a, b, \dots, c\}, \quad \langle a, b, \dots, c\rangle.$$

Непосредственно формализовать неформальное правило линковки деревьев довольнотаки проблематично, однако мы можем формализовать некоторые следствия такой линковки, о которых шла речь чуть выше. Кроме того, нам еще потребуется добавить определение предиката равенства множеств, поскольку без равенства невозможно представить себе математику.

Оказывается, что для построения всех математических объектов достаточно постулировать несколько простых вещей:

1. два множества равны тогда и только тогда, когда они состоят из одних и тех же элементов;
2. из любого множества можно выделить определяемую часть;
3. должно существовать пустое множество;

4. для каждого множества должно существовать множество всех его подмножеств;
5. для каждого множества должно существовать объединение всех его элементов-множеств;
6. из любых двух множеств можно составить пару, как упорядоченную, так и неупорядоченную.

Когда мы здесь пишем, что «можно составить» или «должно существовать», мы имеем в виду, что существует множество, являющееся результатом такой операции.

Рассмотрим эти идеи чуть подробнее. Пункт 2 говорит нам, что если уже имеется какое-то множество $A$, то можно с помощью формулы определить его подмножество. Иначе говоря, можно составить множество $\{x \mid (x \in A) \wedge \varphi(x)\}$, если пользоваться сверточной лексемой. В этой свертке есть одно существенное ограничение: $x$ берутся только те, что уже есть в $A$, а не произвольные множества, как в парадоксе Рассела. Тем самым мы как бы реализуем древнеримский правовой принцип — если позволено большее ($A$), то позволено и меньшее (подмножество $A$). Формально эта идея выражается **схемой аксиом выделения**:

$$\forall X\ \exists Y\ \forall z((z \in Y) \leftrightarrow (z \in X) \wedge \varphi[a/z]), \tag{B2.8}$$

где, как обычно, $\varphi$ — произвольная формула рассматриваемого языка, не содержащая переменной $Y$. Кстати, если переменной $a$ в формуле $\varphi$ нет, то замена $\varphi[a/z]$ никак не меняет формулу, и в этом случае либо получим $X = Y$, когда $\varphi$ истинно, либо $Y = \varnothing$, когда $\varphi$ ложно.

Пункт 3. Почему должно существовать пустое множество? Напомним, пустое множество — это такое множество $\varnothing$, которое обладает свойством $\forall x\ (x \notin \varnothing)$. Можно было бы даже ввести в наш язык константу $\varnothing$ и добавить определение пустого множества в качестве аксиомы (многие авторы так и делают). Но мы не хотим обременять себя даже таким пустяком.

Существование пустого множества довольно легко объяснить (и в некотором смысле даже доказать без прямого постулирования). Дело в том, что если мы считаем теорию множеств непротиворечивой, то у нее должна быть модель (да-да, непустое множество, только уже в мета-теории), а значит, формула $\exists x\ (x = x)$ истинна. Но из этой формулы, а также из аксиомы выделения по правилам логики предикатов выводится формула $\exists y\ (\forall z\ (z \notin y))$, т.е. выводится существование пустого множества. Для этого достаточно взять $y$, заданный как часть $x$ с помощью любой ложной формулы, например, такой: $z \neq z$, и тогда из существования хоть какого-нибудь множества неизбежно следует существование пустого.

Пункт 4 — это что-то вроде декларации равных возможностей. Точнее, если у нас имеется некоторое множество $A$, то перед нами открывается огромное количество возможностей вырезать из него часть (подмножество), редуцировать или схлопнуть его до чего-то меньшего (примерно как редукция волновой функции после произведенного измерения). Еще это можно мыслить себе так: у вас есть 100 долларов, и на эти деньги потенциально можно купить очень много разных вещей, суммарная стоимость которых измеряется триллионами долларов, но как только вы купили что-то (произвели измерение), ваши потенциальные возможности реализовались в одну-единственную. Так вот, множество всех подмножеств — это совокупность всех потенциальных возможностей, всех таких множеств, до которых может коллапсировать исходное множество $A$. Почему же мы должны отказывать этому выбору в праве на существование? Именно выбору,

а не только результатам каждого конкретного выбора. Получается даже что-то вроде Многомировой интерпретации Эверетта Квантовой механики, когда все возможности априори существуют, но в параллельных мирах.

А у нас они будут существовать в множестве всех подмножеств, именуемом также **булеаном** множества $A$ или степенью множества $A$. Используя ранее определенный предикат вложения множеств, аксиому булеана легко сформулировать:

$$\forall X\ \exists Y\ \forall z\ ((z \in Y) \leftrightarrow (z \subseteq X)). \tag{B2.9}$$

Заметим, что если $z$ есть часть множества $A$, то в его булеане $z$ является элементом (или, как еще говорят, точкой).

Если пункт 4 генерирует множества по восходящей в смысле отношения $\in$ (было подмножество — стал элемент), то пункт 5 предлагает обратный, нисходящий процесс (был элемент — стал подмножеством), поскольку, имея множество $A$, мы конструируем некое новое множество, в котором собираем все элементы всех элементов $A$.

Если множество мыслить себе как дерево, где корень — само это множество, а элементы — непосредственные потомки корня, то дальше можно раскручивать это определение, переходя к следующему слою дерева (элементам элементов), и т.д. Принцип под номером 5 разрешает нам выкинуть в этом дереве первый слой (прямых потомков) и сразу перейти от корня ко второму слою.

Здесь сложно придумать какие-то физико-юридические аналоги, разве что вспомнить какое-нибудь право наследования. Но убедительность сюжета из теории графов кажется достаточной мотивацией для **аксиомы объединения**. Кстати, ее формулировка:

$$\forall X\ \exists Y\ \forall x\ ((x \in Y) \leftrightarrow \exists y\ ((x \in y) \wedge (y \in X))). \tag{B2.10}$$

Наконец, пункт 6 реализует идею, что из любых двух множеств $A$ и $B$ можно составить пару $\{A, B\}$, т.е. такое множество, которое можно определить лексемой-сверткой $\{x \mid (x = A) \vee (x = B)\}$ или **аксиомой пары**:

$$\forall x \forall y \exists Z\ \forall z\ ((z \in Z) \leftrightarrow (z = x) \vee (z = y)). \tag{B2.11}$$

Здесь у нас уже появляется справедливое подозрение: не наткнемся ли мы снова на какой-нибудь парадокс вроде расселовского? Ведь мы просто составляем произвольную совокупность, не вырезая часть чего-то уже известного.

Но, во-первых, как и в мире людей, мы не лишаем никаких индивидов права составлять пары (и более крупные коалиции, что уже будет следовать из возможности составить пару), а во-вторых, получаемое множество не такое уж всеохватывающее, как в известных парадоксах: мы можем не просто точно указать его элементы, но даже написать их, так сказать, поименно. А все, что можно написать за конечно число шагов, мы принимаем как существующее безоговорочно, иначе мы не смогли бы работать даже с простейшими формальными языками.

Что касается упорядоченной пары, то мы просто выразим ее через неупорядоченные пары некоторым специальным (но разрешенным теорией) способом, а через нее уже сможем реализовать и прямое произведение множеств. Так что неупорядоченную пару множеств можно считать чем-то более фундаментальным, чем эти конструкции.

Впрочем, как мы увидим в дальнейшем, аксиому пары и аксиому выделения можно вывести из другой, более общей аксиомы, мотивация которой тоже не безосновательна, и при наличии такой аксиомы даже неупорядоченная пара множеств станет вторичным объектом.

Тем не менее, вопрос о том, не возникнет ли самореференция в определении пары, остается открытым. Действительно, ничто не мешает нам представить себе уравнение $A = \{A, B\}$ с зацикленным отношением $A \in A$. Такие вещи мы не одобряем, и потому привлекаем для борьбы с ними уже специальную аксиому, постулирующую фундированность отношения $\in$. Она называется **аксиомой регулярности** и утверждает, что в каждом множестве $X$ есть наименьший по принадлежности элемент (такой $x \in X$, что все меньшие его по принадлежности $y$ не будут элементами того же $X$, либо их вообще не будет, т.е. $x$ пусто). На диаграмме B2.1 это свойство выражается в том, что не все двухшаговые корневые пути можно сократить (на картинке это путь $\to \{\{\}\} \to \{\}$).

Аксиома регулярности запрещает циклы вида $a \in b \in c \in \cdots \in d \in a$, что прекрасно согласуется с представленной выше древовидной концепцией, из которой очевидным образом вытекает запрет на самореференцию, т.к. все вышестоящие узлы дерева не могут совпадать с нижестоящими, если мы не допускаем бесконечные зацикленные деревья (фрактальные структуры). Формально, аксиома регулярности постулирует, что у любой нисходящей по $\in$ цепочки должен быть конец, что в точности соответствует требованию конечности всех путей в древовидной развертке от корня к листьям. На самом деле суть и предназначение аксиомы регулярности состоит в том, чтобы весь универсум множеств был очень хорошо упорядочен, т.е. чтобы не только каждое множество имело вид некого регулярного дерева, но и весь универсум был бы по сути таким единым деревом, растущим из пустого множества. Аксиома регулярности приведет нас позже к определению кумулятивных универсумов фон Неймана, показывающих строгую иерархичность класса всех множеств. Но этим мы займемся уже на уровне C1 (см. раздел C1.3).

Таким образом мы почти полностью сформулировали и объяснили аксиомы теории множеств, хотя все еще оставляем за кадром возможности формирования привычных нам теоретико-множественных конструкций: $\cup, \cap, \setminus, \times$ и т.д. Перейдем же теперь непосредственно к практике использования упомянутых аксиом.

## B2.3. Наследственно-конечные множества

Здесь мы построим формальную теорию множеств, которая описывает так называемую финитную математику, или математику конечного. В этой теории мы по сути в точности реализуем идею представления множеств в виде конечных графов.[9]

### B2.3.1 Язык и аксиомы

Язык теории, как уже отмечалось, строится на основе единственного предикатного символа $\in$, однако мы рассматриваем теорию множеств как теорию с равенством (и, следовательно, привлекаем стандартные аксиомы равенства из логики предикатов), так что предикатный символ $=$ здесь также имеется, однако его можно считать вторичным по отношению к $\in$ в силу аксиомы экстенсиональности. Во всех формулах его можно заменить, пользуясь этой аксиомой, но при этом как формулировка, так и само наличие аксиомы конгруэнтности перестанут быть очевидными. Так что для удобства записей и согласованности с идеями логики предикатов с равенством мы будем считать, что язык теории множеств строится из двух атомарных бинарных предикатов: $\in, =$. В качестве

[9] Обозначение теории HF происходит от англ. *hereditarily finite sets*.

переменных мы допускаем использование строчных и заглавных латинских букв (как обычно, разделяя свободные и связанные переменные). Кроме того, мы используем все введенные ранее сокращения первопорядковых формул, а именно:

$$A \subseteq B \overset{\text{def}}{\leftrightarrow} \forall x\ ((x \in A) \to (x \in B)), \quad (a \notin b) \overset{\text{def}}{\leftrightarrow} \neg(a \in b), \quad (a \neq b) \overset{\text{def}}{\leftrightarrow} \neg(a = b),$$
$$\exists x \in A:\ \varphi(x) \overset{\text{def}}{\leftrightarrow} \exists x\ ((x \in A) \wedge \varphi(x)), \quad \forall x \in A:\ \varphi(x) \overset{\text{def}}{\leftrightarrow} \forall x\ ((x \in A) \to \varphi(x)). \tag{B2.12}$$

Аксиомы:

HF0 Отрицание аксиомы бесконечности.

HF1 Конгруэнтность: $(a = b) \to ((a \in M) \leftrightarrow (b \in M))$.

HF2 Экстенсиональность: $(A = B) \leftrightarrow (\forall x\ ((x \in A) \leftrightarrow (x \in B)))$.

HF3 Выделение $[\varphi]$: $\exists X\ \forall x\ ((x \in X) \leftrightarrow (x \in A) \wedge \varphi(x, \vec{p}))$.

HF4 Степень: $\exists P\ \forall x\ ((x \in P) \leftrightarrow (x \subseteq A))$.

HF5 Объединение: $\exists U\ \forall x\ ((x \in U) \leftrightarrow (\exists a \in A:\ x \in a))$.

HF6 Элементарные множества: $\exists X\ \forall y\ (y \notin X)$; $\exists X\ \forall x\ ((x \in X) \leftrightarrow (x = a) \vee (x = b))$.

HF7 Регулярность: $(\exists x \in A) \to \exists X \in A:\ \forall y \in X:\ (y \notin A)$.

Здесь, как обычно, мы приводим формулы аксиом без замыкающих кванторов общности для удобства восприятия. Мы пока опускаем здесь формулировку аксиомы бесконечности (и ее отрицания), т.к. посвятим ей отдельный раздел. Более того, ее вообще можно не рассматривать в списке аксиом теории HF, но тогда эта теория будет допускать более сложные модели, чем мы хотим себе представлять в контексте рассмотрения финитной математики. Кроме того, HF с отрицанием аксиомы бесконечности является взаимно интерпретируемой с арифметикой PA, что также важно для лучшего понимания оснований финитной математики.

С другой стороны, в дополнение к озвученным ранее аксиомам мы ввели здесь аксиому конгруэнтности равенства, которая обычно подразумевается для предиката равенства автоматически. Однако выделить ее необходимо, т.к. она имеет тот же смысл, что аксиома PA2 в арифметике, которую мы обсуждали ранее. Аксиома HF1 выражает лишь конгруэнтность по левому аргументу предиката $\in$, т.к. конгруэнтность по правому аргументу уже зашита в аксиоме экстенсиональности, а общую конгруэнтность (B1.9) можно доказать на уровне мета-теории индукцией по сложности формул языка теории множеств.

Действуя по канонам построения теории в языке первого порядка, мы могли бы расщепить аксиому экстенсиональности на две отдельные аксиомы:

$$(A = B) \to (\forall x\ ((x \in A) \leftrightarrow (x \in B))), \quad (\forall x\ ((x \in A) \leftrightarrow (x \in B))) \to (A = B),$$

тогда первая из них была бы недостающей частью аксиомы конгруэнтности (для второго аргумента предиката $\in$), а вторая была бы собственно аксиомой, связывающей равенство и принадлежность. Но наша формулировка наглядно демонстрирует, как равенство множеств выражается через принадлежность (что по сути является определением равенства в теории множеств).

Далее следует схема аксиом выделения, зависящая от формулы $\varphi$, в которой в качестве $\vec{p}$ обозначен набор параметров, т.е. свободных переменных $p_1, \ldots, p_n$, т.к. выделение части множества может быть параметризовано. Затем идут привычные нам аксиома степени (булеана) и объединения, затем аксиома, постулирующая существование пустого множества и пары и, наконец, аксиома регулярности, утверждающая, что в любом непустом множестве имеется минимальный по принадлежности элемент.

Как уже отмечалось, существование пустого множества напрямую следует из предположения о непротиворечивости теории и аксиомы выделения, поэтому такое требование можно опускать. Но, опять же, для исторической преемственности мы оставляем эту аксиому. Аксиома пары является прямым конструктивным способом создавать новые множества не как части уже определенных, т.е. частично (в финитарном контексте) реализуя принцип произвольной совокупности.

Как и в случае арифметики Пеано, для системы HF нужно вывести основные привычные нам с детства теоретико-множественные соотношения.

**Теорема B2.5.** *В теории* HF *выводимы следующие теоремы (с учетом универсального замыкания формул):*

1° *равенство рефлексивно, симметрично, транзитивно;*

2° $\exists X\ \forall x\ ((x \in X) \leftrightarrow (x \in A) \wedge (x \in B))$;

3° $\exists X\ \forall x\ ((x \in X) \leftrightarrow (x \in A) \vee (x \in B))$;

4° $\exists X\ \forall x\ ((x \in X) \leftrightarrow (x \in A) \wedge (x \notin B))$;

5° $\exists X\ \forall x\ ((x \in X) \leftrightarrow ((x \in A) \wedge (x \notin B)) \vee ((x \notin A) \wedge (x \in B)))$;

6° $\exists X\ \forall x\ ((x \in X) \leftrightarrow (x = a_1) \vee (x = a_2) \vee \ldots \vee (x = a_n))$;

7° *существует упорядоченная пара и прямое произведение множеств.*

*Доказательство.* Первое свойство утверждает, что наше равенство удовлетворяет стандартным аксиомам равенства:

$$a = a, \quad (a = b) \to (b = a), \quad (a = b) \wedge (b = c) \to (a = c).$$

Это прямо следует из экстенсиональности в чистой логике предикатов.

Второе свойство получается прямо из аксиомы выделения, если подставить $\varphi \equiv (x \in B)$, где $B$ — это параметр. Следующее свойство более трудное, оно требует использовать сразу две аксиомы — пары и объединения. Чтобы их использование было наглядным, лучше прибегнуть к использованию расширенной сигнатуры языка, обогатив ее новыми бинарными функциональными символами $\{\}, \cup, \cap, \setminus, \triangle, \langle\rangle, \times$, унарными функциональными символами $\mathscr{P}, \bigcup$ и константой $\varnothing$.

Язык в такой расширенной сигнатуре потребует новых аксиом, которые будут определять правила использования новых символов. Однако все теоремы расширенного языка можно перевести обратно в первоначальный язык, в котором они также окажутся теоремами. Такое расширение языка и теории называется *консервативным*. К этому приему часто прибегают, чтобы улучшить визуальное восприятие языка и теорем, ничего не изменив по сути.

Но для этого придется выполнить определенную синтаксическую работу, которой мы сейчас и займемся. Итак, сначала мы введем переобозначения для функциональных

символов, чтобы уйти от стандартной для исчисления предикатов польской записи вида $F(a,b)$, а именно, положим:

$$\{a,b\} \rightleftharpoons^{\text{def}} \{\}(a,b), \quad a \cup b \rightleftharpoons^{\text{def}} \cup(a,b), \quad a \cap b \rightleftharpoons^{\text{def}} \cap(a,b), \quad a \setminus b \rightleftharpoons^{\text{def}} \setminus(a,b),$$
$$a \triangle b \rightleftharpoons^{\text{def}} \triangle(a,b), \quad \langle a,b\rangle \rightleftharpoons^{\text{def}} \langle\rangle(a,b), \quad a \times b \rightleftharpoons^{\text{def}} \times(a,b). \tag{B2.13}$$

Подчеркнем еще раз, что это — не аксиомы, а всего лишь синтаксические переобозначения на уровне мета-теории, в самом формальном языке их по-прежнему нет.

HF8 Аксиомы для символов $\{\}, \cup, \cap, \setminus, \triangle, \langle\rangle, \times, \mathscr{P}, \bigcup, \varnothing$:

$$c \in \{a,b\} \overset{\text{def}}{\leftrightarrow} (c = a \vee c = b), \qquad c \in a \setminus b \overset{\text{def}}{\leftrightarrow} (c \in a \wedge c \notin b),$$
$$c \in a \cup b \overset{\text{def}}{\leftrightarrow} (c \in a \vee c \in b), \qquad c \in a \triangle b \overset{\text{def}}{\leftrightarrow} (c \in a \setminus b) \vee (c \in b \setminus a),$$
$$c \in a \cap b \overset{\text{def}}{\leftrightarrow} (c \in a \wedge c \in b), \qquad c \in \langle a,b\rangle \overset{\text{def}}{\leftrightarrow} (c = \{a,a\} \vee c = \{a,b\}),$$
$$c \in \mathscr{P}(a) \overset{\text{def}}{\leftrightarrow} c \subseteq a, \qquad c \in \bigcup a \overset{\text{def}}{\leftrightarrow} \exists x \in a :\ c \in x,$$
$$c \notin \varnothing \qquad c \in A \times B \overset{\text{def}}{\leftrightarrow} \exists x \in A : \exists y \in B :\ c = \langle x,y\rangle.$$

Заметим, что здесь мы воспользовались неопределенными ранее предикатами $c = \{a,b\}$ и $c = \langle x,y\rangle$. Синтаксически они, конечно, верно устроены, но как определить их истинность или ложность? Оказывается, это легко сделать. Из имеющихся аксиом мы можем вывести свойства для новых термов при их подстановке в предикат равенства и в предикат принадлежности слева (а не справа, как в определении).

**Теорема B2.6.** *Пусть терм $t(\vec{p})$ определяется формулой $\varphi(a,\vec{p})$, т.е.*

$$a \in t(\vec{p}) \overset{\text{def}}{\leftrightarrow} \varphi(a,\vec{p}), \tag{B2.14}$$

*где $\vec{p}$ — набор параметров (свободных переменных). Тогда имеют место теоремы теории* HF*:*

$$C = t(\vec{p}) \leftrightarrow \forall x\ ((x \in C) \leftrightarrow \varphi(x,\vec{p})). \tag{B2.15}$$
$$(t(\vec{p}) \in A) \leftrightarrow \exists x \in A :\ (x = t(\vec{p})), \tag{B2.16}$$

*Доказательство.* Для доказательства первой эквиваленции сначала воспользуемся экстенсиональностью

$$C = t(\vec{p}) \leftrightarrow \forall x\ ((x \in C) \leftrightarrow (x \in t(\vec{p}))),$$

а затем заменим формулу на эквивалентную под квантором, пользуясь (B2.14). На самом деле, верен и обратный переход от первой теоремы к определению. Для этого достаточно вместо переменной $C$ в (B2.15) подставить терм $t(\vec{p})$ и воспользоваться рефлексивностью равенства, а также аксиомой логики предикатов для квантора всеобщности.

Для доказательства второй эквиваленции мы воспользуемся теоремой D2.6 (Часть 2), где в качестве формулы $\varphi(a)$ подставим формулу $(a \in A)$, а в качестве терма $t$ — терм $t(\vec{p})$. □

Из теоремы (B2.15) мы можем заметить, что если вместо $C$ подставить лексему-свертку $\{x \mid \varphi(x, \vec{p})\}$, то слева мы получим привычное *прямое определение* терма $t(\vec{p})$ через эту свертку, а справа — в точности определение терма-свертки (B2.7), что, в общем, позволяет нам вводить определения новых функциональных символов с помощью свертки, но проблема такого определения состоит ровно в том, что оно не является первопорядковой формулой, а значит, его нельзя воспринимать как запись аксиомы в языке теории множеств (как в исходном, так и в расширенном).

Поэтому если где-то в тексте мы встречаем прямое определение вида $t(\vec{p}) \overset{\text{def}}{\rightleftharpoons} \{x \mid \varphi(x, \vec{p})\}$ с первопорядковой формулой $\varphi$, то мы должны сразу мысленно сконвертировать его в первпорядковую аксиому $a \in t(\vec{p}) \overset{\text{def}}{\leftrightarrow} \varphi(a, \vec{p})$, тем самым узаконив это прямое определение.

В группе аксиом HF8 особняком стоит аксиома символа пустого множества, поскольку она не имеет вида (B2.14), но мы можем легко привести ее к такому виду. Аксиома $c \notin \varnothing$ означает, что формула $c \in \varnothing$ должна быть ложной, стало быть, ее можно переписать в виде

$$c \in \varnothing \overset{\text{def}}{\leftrightarrow} \varphi(c) \wedge \neg\varphi(c),$$

где $\varphi$ — любая формула исходного языка теории HF. А отсюда мы получаем и прямое определение пустого множества через свертку: $\varnothing \overset{\text{def}}{\rightleftharpoons} \{x \mid \varphi(x) \wedge \neg\varphi(x)\}$. Заметим также, что это определение не зависит от выбора формулы $\varphi$ в силу законов логики высказываний. Если же мы хотим использовать в нашем языке логические константы, то определение можно упростить до $\varnothing \overset{\text{def}}{\rightleftharpoons} \{x \mid \bot\}$.

Стоит отметить, что при расширении сигнатуры языка мы не только ввели определения для новых символов, но также расширили на них действие аксиом конгруэнтности (B1.9). Это важно всегда помнить при расширении языка теории с равенством!

Мы можем применить еще одно сокращение, полагая $\{a\} \overset{\text{def}}{\rightleftharpoons} \{a, a\}$, так что с учетом этого сокращения, предъявленных аксиом и транзитивности равенства мы можем получить прямое определение упорядоченной пары по Куратовскому:

$$\langle a, b\rangle = \{\{a\}, \{a, b\}\}.$$

Заметим также, что часто вместо $\varnothing$ пишут $\{\}$, фактически рассматривая этот функциональный символ как 0-арный.

Коль скоро мы расширили язык новыми функциональными символами, термами становятся не только переменные, но и все возможные композиции этих новых символов и переменных. Поэтому нужно было бы оговорить поведение вновь определенных функциональных символов при подстановке в них разных термов. К счастью, приведенных аксиом достаточно, поскольку у нас имеются аксиомы исчисления предикатов, которые позволяет любые свободные переменные заменять любыми термами. Так что, например, имея формулу $c \in \{a, b\}$ и два произвольных терма $t_1, t_2$, мы можем подставить их в аксиому и получить определение для $c \in \{t_1, t_2\}$, которое сводит использование более сложного терма $\{t_1, t_2\}$ к равенствам с двумя менее сложными термами: $c = t_1$ и $c = t_2$. И так как дерево разбора любого терма конечно, очевидно, что мы можем раскрутить исходную формулу до конца, т.е. до формул с переменными, а для них у нас работают приведенные аксиомы HF8.

Таким образом получается, что все формулы в более богатом языке теории множеств с сигнатурой, включающей символы $\{\}, \cup, \cap, \setminus, \triangle, \langle\rangle, \times, \mathscr{P}, \bigcup, \varnothing$, могут быть однозначно переведены в более бедный язык без этих символов.

Пользуясь таким богатством, мы можем переписать некоторые аксиомы теории HF более приятным образом:

HF4 Степень: $\exists P\ (P = \mathscr{P}(a))$.

HF5 Объединение: $\exists U\ (U = \bigcup a)$.

HF6 Элементарные множества: $\exists X\ X = \varnothing$; $\exists X\ X = \{a, b\}$.

Кстати, формулу вида $\exists x\ (x = t)$, где $t$ — произвольный терм, принято сокращать так: $\exists t$. Что сделает запись аксиом еще проще.

Определение пары $\{a, b\}$ мы можем обобщить до определения произвольного конечного набора $\{a, b, \dots, c\}$, где многоточие является мета-символом и означает, что здесь располагается произвольная последовательность переменных конечной длины. Иначе говоря, мы должны ввести в обращение отдельные функциональные символы $\{\}(\dots)$ для каждой конечной арности и для каждого из них написать аксиомы, аналогичные представленным выше. Но мы не будем этого делать, т.к. такие термы удобнее задавать с помощью пар и объединения путем прямого определения, например, так:

$$\{a, b, c\} \overset{\text{def}}{\rightleftharpoons} \{a, b\} \cup \{c\}, \quad \{a, b, c, d, e\} = \bigcup \{\{a, b, c\}, \{d, e\}\}. \tag{B2.17}$$

Одновременно это позволяет установить существование таких множеств, ссылаясь на аксиомы.

Наконец, мы можем вернуться к заявленной выше теореме и переписать проще некоторые ее пункты:

2° $\exists A \cap B$;

3° $\exists A \cup B$;

4° $\exists A \smallsetminus B$;

5° $\exists A \triangle B$;

6° $\exists \{a_1, \dots, a_n\}$;

7° $\exists \langle a, b\rangle$, $\exists A \times B$.

Существование $A \cap B$ следует из аксиомы выделения, как уже отмечалось.

Существование $A \cup B$ следует из того, что $A \cup B = \bigcup \{A, B\}$, т.е. множество $A \cup B$ есть составной терм из тех, что мы уже определили и существование которых гарантировано аксиомами пары и объединения.

Существование $A \smallsetminus B$ есть прямое следствие аксиомы выделения с формулой $\varphi(x, B) \equiv (x \notin B)$.

Существование $A \triangle B$ следует из того, что $A \triangle B = (A \smallsetminus B) \cup (B \smallsetminus A)$.

Существование произвольного конечного множества $\{a_1, \dots, a_n\}$ следует из его построения, о котором было сказано выше, и остальных аксиом.

Существование упорядоченной пары $\langle a, b\rangle$ следует из ее определения по Куратовскому. Вопрос о том, почему она удовлетворяет свойству упорядоченной пары

$$(\langle a, b\rangle = \langle c, d\rangle) \leftrightarrow (a = c) \wedge (b = d),$$

мы оставляем в качестве упражнения читателю.

Что касается прямого произведения $A \times B$, то его существование вытекает из того, что его можно определить как часть множества $\mathscr{P}(\mathscr{P}(A \cup B))$, которое существует в силу аксиом. □

### B2.3.2 Скобочная модель

В расширенном языке теории множеств (с учетом использования выражений $\{a, b, \dots, c\}$), который был задан выше, допустимо описывать множества термами, запись которых содержит только скобки и запятые:

$$\{\}, \quad \{\{\}\}, \quad \{\{\},\{\{\}\}\}, \quad \{\{\{\}\}\},\{\{\}\},\{\}$$

Множества, которые можно описать такими термами, называются **наследственно-конечными**. Общематематическое (рекурсивное) определение у них таково: наследственно конечные множества — это конечные множества, элементы которых также являются наследственно конечными.

Основная идея этих множеств состоит в том, что это конечные объекты, определяемые рекурсивно. Более того, нетрудно написать разрешающий алгоритм в любом универсальном языке программирования, который по любой скобочной записи сможет за конечное число шагов сказать, является ли данная запись корректной записью множества или нет.

Правила построения скобочных записей в форме Бэкуса-Наура таковы. Мы используем два нетерминальных символа *список* и *множество*, и терминальные символы $\{, \}, \Lambda$, тогда

P1 *список* $\to$ $\Lambda$ | *список множество*;

P2 *множество* $\to$ $\{$*список*$\}$,

где символ $\Lambda$ обозначает пустую строку. Таким образом список есть пустая строка либо последовательность множеств, а множество есть список, заключенный в фигурные скобки. Получаются записи множеств вида

$$\{\Lambda\}, \quad \{\Lambda\{\}\}, \quad \{\Lambda\{\Lambda\{\}\}\}, \quad \{\Lambda\{\Lambda\{\}\}\Lambda\{\}\Lambda\{\}\},$$

которые легко преобразовать к более привычному виду, удалив $\Lambda$ и заменив все вхождения пары символов "}{"на тройку символов "}, {":

$$\{\}, \quad \{\{\}\}, \quad \{\{\{\}\}\}, \quad \{\{\{\}\},\{\},\{\}\}.$$

Определив таким образом универсум скобочных записей, мы будем интерпретировать их как множества. Для произвольной записи $s$ обозначим через $s_1, \dots, s_n$ список ее элементов (подстрок), содержащихся внутри внешних скобок записи $s$. Аналогично, пусть запись $t$ содержит элементы $t_1, \dots, t_m$. Тогда определим предикаты $\in$ и $=$ одновременной рекурсией по глубине вложенности скобок (или по длине строки):

$$s = t \iff (\forall i \leqslant n\ \exists j \leqslant m : s_i = t_j) \wedge (\forall j \leqslant m\ \exists i \leqslant n : t_j = s_i), \tag{B2.18}$$

$$s \in t \iff \exists j \leqslant m : s = t_j. \tag{B2.19}$$

В этом определении кванторы пробегают конечное множество индексов непосредственных элементов записей. Такое определение сводит равенство множеств к равенству их

элементов, которые являются строго более короткими строками, что обеспечивает завершение рекурсии.[10]

Почему же при таком определении $\in, =$ выполняются аксиомы HF0–7? Отсутствие бесконечных множеств автоматически следует из финитности самой конструкции скобочных записей. Экстенсиональность выполняется очевидным образом, т.к. она зашита в определение равенства (B2.18). Отсюда, в частности, следует, что равенство рефлексивно, симметрично и транзитивно. Конгруэнтность очевидным образом следует из того, что если $a = b$ и $a \in M$ то в записи $M$ есть подстрока $t$, равная $a$, и она же будет равна $b$, следовательно $b \in M$ в силу (B2.19).

Аксиомы степени и выделения выполняются в силу того, что в скобочной модели существуют все подмножества любого множества $M$, независимо от того, определяются они формулами или нет. Мы можем написать алгоритм, который перечислит нам все возможные подмножества $M$, соберет их в список и упакует в фигурные скобки, тем самым построив $\mathscr{P}(M)$, после чего несложно будет найти среди них подмножество, соответствующее формуле $\varphi$, т.е. осуществить выделение. Еще проще строится объединение $\bigcup M$: нужно просто удалить фигурные скобки, образующие по правилу P2 множества, входящие в список множества $M$ (т.е. скобки второго уровня вложенности), тогда получится множество, список которого есть конкатенация списков элементов множества $M$.

Заметим, что наша скобочная модель как нельзя лучше воплощает древовидный принцип построения множеств, о котором говорилось в предыдущем разделе. Собственно, синтаксические деревья разбора скобочных записей реализуют ровно те же самые деревья множеств.

Пустое множество, как уже отмечалось, записывается строкой {} (в нашем исходном формализме это $\{\Lambda\}$). Пара $\{A, B\}$ существует непосредственно в силу построения скобочных записей. А проверка аксиомы регулярности осуществляется индукцией по глубине вложенности скобок.

Таким образом описанные выше скобочные записи представляют собой *модель* множеств, подчиняющихся аксиомам теории HF в ее исходном языке. Такую модель называют *стандартной моделью наследственно конечных множеств*.[11]

Более того, среди всех скобочных записей мы можем выделить *канонические*, которые будут обладать определенными свойствами уникальности, а именно: у каждой канонической записи будет свой собственный код (натуральное число), а элементы образующего списка канонической записи будут расположены в порядке убывания этого кода и не будут дублироваться.

Предположим, что запись $S$ обладает наследственным свойством уникальности элементов. Это означает, что в списке ее элементов $L(S) = \{s_1, \dots, s_n\}$ все $s_i$ попарно различны (если $i \neq j$, то $s_i \neq s_j$ согласно формуле (B2.18)), и это свойство рекурсивно выполняется для всех элементов $s_i$. Тогда положим, следуя Аккерману,

$$\mathrm{Code}(S) = \sum_{s\in S} 2^{\mathrm{Code}(s)}, \quad \mathrm{Code}(\{\}) = 0. \tag{B2.20}$$

[10] Определение понятия *глубина вложенности скобок*, реализацию разбиения записи на список непосредственных элементов, а также основанную на них проверку сходимости описанного алгоритма мы оставим за рамками этой книги. Но с точки зрения программирования это более-менее очевидно и реализуется в любой модели рекурсивных функций, например, с помощью машины Тьюринга или арифметических предикатов.

[11] Более точно, стандартной моделью называется универсум $V_\omega$, но его множества — это в точности такие множества, которые отвечают нашим скобочным записям.

При таком кодировании получается, что $a \in b$ тогда и только тогда, когда бит с номером $\mathrm{Code}(a)$ в двоичной записи кода $\mathrm{Code}(b)$ равен 1.

Несложно доказать (индукцией по построению множества), что разным множествам соответствуют разные коды, а в силу свойства уникальности элементов все слагаемые в этой сумме будут различными. Более того, имея произвольное натуральное число $N$, мы можем найти множество с кодом, равным $N$. Для этого число $N$ нужно представить в виде суммы степеней двоек (записать в двоичной системе), а затем проделать то же самое со степенями двоек, и т.д. пока не упремся в нулевые степени. После чего мы вместо нулей напишем {}, вместо $2^s$ напишем $s$, а вместо + поставим запятые и обернем слагаемые в фигурные скобки (см. рис. B2.2).

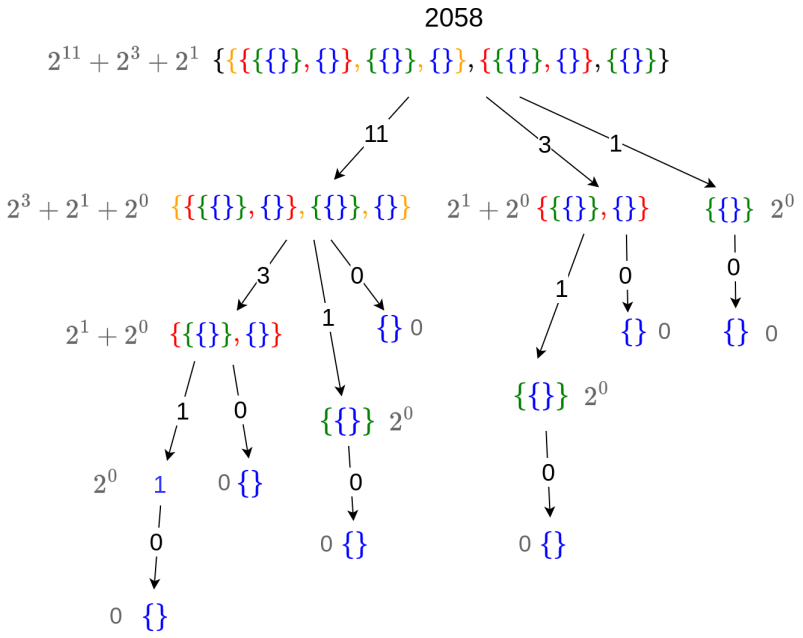



Рис. B2.2. Кодирование канонической записи множества.

Данные алгоритмы (кодирования и декодирования записей) сходятся в силу чисто арифметических причин. Наконец, чтобы определиться, в каком порядке располагать элементы множества в такой записи, мы условимся, что они идут в порядке убывания их кодов. Тем самым мы определим канонические записи наследственно конечных множеств и установим взаимно однозначное соответствие между ними и натуральными числами. На этом факте основывается возможность взаимной интерпретации теории наследственно конечных множеств и арифметики Пеано (см. Часть II, раздел D4.5).

Интересно отметить, что существует и совершенно иной, алгебраический подход к кодированию конечных множеств натуральных чисел. Любое конечное множество $S \subseteq \mathbb{N}$ можно представить его характеристической функцией, которая по сути является конечной двоичной последовательностью (словом). Для однозначности кодирования такая последовательность должна заканчиваться единицей, соответствующей максимальному элементу множества; например, множество $\{2, 5\}$ представляется словом 00101, а не 001010, которое содержит ту же информацию, но привело бы к другой матрице. С другой стороны, известно, что моноид матриц $SL_2(\mathbb{N})$ с целочисленными неотрицательными элементами и определителем, равным 1, является свободной полугруппой

с двумя генераторами:

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Это означает, что любая матрица из $SL_2(\mathbb{N})$ единственным образом представляется в виде произведения этих двух матриц. Таким образом, устанавливается биекция между двоичными словами, заканчивающимися на единицу (и пустым словом), и матрицами, что позволяет закодировать любое конечное множество натуральных чисел в виде одной матрицы $2 \times 2$. Этот пример ярко иллюстрирует, как глубокие результаты из теории групп и теории чисел могут предоставлять неожиданные инструменты для решения задач в основаниях математики.

Построенная нами скобочная модель, или стандартная модель теории наследственно конечных множеств в языке скобочных записей иллюстрирует возможность реализации и тем самым непротиворечивость аксиом HF. Хотя сама HF говорит только о конечных множествах, ее стандартная модель опирается на более сильную теорию, принимающую актуальную бесконечность (ведь сама модель бесконечна). Это указывает на тонкое взаимодействие между финитарными рассуждениями (которые, казалось бы, воплощает HF) и инфинитарными предположениями, необходимыми для изучения ее метатеории.

Наконец, стоит отметить, что в универсуме наследственно конечных множеств доказуемы аналоги аксиомы подстановки и аксиомы выбора для конечного случая, но их полная мощь проявляется только в теориях с бесконечными множествами.

Этот факт говорит о том, что в такой достаточно примитивной (примитивно рекурсивной) конструкции мы умеем моделировать практически весь арсенал обычной теории ZFC, за исключением аксиомы бесконечности. Но так как сами по себе эти модели, очевидно, бесконечны, а точнее, счетны, то сомнениям в непротиворечивости по крайней мере счетного фрагмента ZFC (где действие аксиомы степени ограничено лишь конечными множествами) места практически не остается.

На самом деле все наши рассуждения про наследственно конечные множества и подробный разбор теории HF направлены как раз на то, чтобы убедиться в достаточной надежности этой теории, чтобы в дальнейшем можно было считать ее нашей метатеорией, в рамках которой можно реализовать арифметику Пеано, рекурсивные функции и, следовательно, кодировать формальные языки и выводимость.

Таким образом замыкается круг, идущий от первых робких попыток описать наивную теорию множеств через дебри формализации логики первого порядка к определению уже достаточно точных и богатых математическими следствиями конструкций, таких как арифметика Пеано PA и теория HF.

С этого момента мы можем считать, что твердо стоим на фундаменте теории формальных систем, и можем давать точные математические определения всем тем объектам и умозаключениям, которые нам встретятся в дальнейшем.

Заметим дополнительно, что аксиомы HF1–6 (исключая регулярность), которые мы привели выше, были изобретены и опубликованы Эрнстом Цермело еще в 1908 году. Причем он сразу присоединил к ним аксиому бесконечности и аксиому выбора. Такая теория обычно обозначается Z по первой букве фамилии автора. Авраамом Френкелем и Туральфом Скулемом в начале 1920-х были введены в обращение аксиома регулярности и аксиома подстановки, и теперь теория Цермело без аксиомы выбора, но с аксиомами регулярности и подстановки обозначается ZF, а если мы в ней оставляем и аксиому выбора, то ZFC.

## B2.4. Вопросы для самоконтроля

**Q1** Какова основная цель и ключевые идеи при формальной аксиоматизации натуральных чисел? [стр. 114]

**Q2** Кратко опишите язык PA. Каков концептуальный смысл аксиом, определяющих операцию следования, нуль, сложение и умножение? [стр. 115]

**Q3** Объясните суть принципа математической индукции в PA. Почему он представлен как схема аксиом? Как концептуально связаны с ним другие формы индукции, такие как полная индукция или принцип фундированности? [стр. 121]

**Q4** Как обычно определяется отношение порядка в арифметике Пеано? В чем заключается концептуальное различие и значение слабого и сильного определений неравенства? [стр. 120]

**Q5** Поясните различие между истинностью утверждения для всех натуральных чисел (в метатеории) и его формальной доказуемостью как универсального утверждения $(\forall x\ \varphi(x))$ внутри PA. Какие выводы о доказательной силе PA можно сделать из этого? [стр. 123]

**Q6** Почему интуитивное понимание термина «множество» приводит к проблемам (например, парадокс Рассела)? Какие общие принципы лежат в основе аксиоматического подхода к определению множеств? [стр. 125]

**Q7** Объясните концептуальное назначение основных аксиом теории HF, позволяющих конструировать множества. Как они способствуют построению универсума наследственно-конечных множеств? [стр. 133]

**Q8** Опишите концептуальную идею «наследственно-конечных множеств». Что означает, что множество является наследственно конечным, и как это связано с древовидным представлением множеств? [стр. 139]

**Q9** Какова концептуальная связь или взаимная интерпретируемость между HF и PA? [стр. 141]

## B2.5. Упражнения

**Ex1.** Выразите утверждение «Каждое натуральное число является либо нулем, либо последователем» на языке PA.

**Ex2.** Формализуйте определение «квадратного числа» (полного квадрата), используя только умножение.

**Ex3.** Выразите следующие арифметические понятия на языке PA:

- «$x$ — четное число».
- «$x$ является делителем $y$» $(x \mid y)$.
- «$x$ — простое число».
- Гипотеза Гольдбаха: «Каждое четное целое число, большее 2, является суммой двух простых чисел».

**Ex4.** Запишите определение простого числа, используя *только* предикат делимости $(x \mid y)$ и предикат обратимости (быть делителем единицы) $Inv(x) \overset{\text{def}}{\leftrightarrow} \exists y(xy = 1)$.

**Ex5.** Выразите «Гипотезу о числах-близнецах»: существует бесконечно много пар простых чисел $p, q$, таких что $q = S(S(p))$.

**Ex6.** Формализуйте утверждение: «Для любых двух чисел существует общее кратное».

**Ex7.** Запишите формулу для отношения «Наибольший общий делитель» $G(a, b, d)$ ($d$ является НОД $a$ и $b$).

**Ex8.** Используя аксиомы PA, докажите транзитивность отношения делимости:

$$\forall x, y, z\ ((x \mid y) \wedge (y \mid z) \to (x \mid z)).$$

**Ex9.** Используя схему индукции, докажите, что $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.

**Ex10.** Докажите по индукции, что для каждого $n \geqslant 0$ число $n^3 - n$ делится на 3.

**Ex11.** Докажите неравенство Бернулли $(1 + x)^n \geqslant 1 + nx$ для натурального $n$ и вещественного $x > -1$.

**Ex12.** Докажите по индукции, что сумма первых $n$ нечетных чисел равна $n^2$.

**Ex13.** Используя полную (возвратную) индукцию, докажите, что каждое натуральное число $n > 1$ может быть представлено как произведение простых чисел.

**Ex14.** Используя принцип бесконечного спуска, докажите, что $\sqrt{2}$ иррационален (предположите, что $a^2 = 2b^2$ ведет к меньшему решению).

**Ex15.** Нарисуйте дерево разбора для скобочной записи ординала фон Неймана $3 = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$.

**Ex16.** Дайте рекурсивное определение ранга наследственно конечного множества.

**Ex17.** Пусть $\sim$ — отношение эквивалентности на множестве $A$. Выразите формулу, определяющую предикат принадлежности к фактор-множеству $(x \in A/_{\sim})$.

**Ex18.** В теории HF запишите формулу, выражающую тот факт, что множество $A$ является упорядоченной парой $\langle x, y\rangle$ (используя определение Куратовского).

**Ex19.** Пусть $n \in \mathbb{N}, n > 1$. Докажите, что отношение $a \equiv b \pmod{n}$ является конгруэнцией относительно сложения.

**Ex20.** Докажите, что отношение $a \equiv b \pmod{n}$ является конгруэнцией относительно умножения.

**Ex21.** Вычислите код Аккермана для:

1. пустого множества $\varnothing$.
2. синглетона $\{\varnothing\}$.
3. множества $\{\{\varnothing\}\}$.
4. множества $\{\varnothing, \{\varnothing\}\}$.
5. упорядоченной пары $\langle\varnothing, \varnothing\rangle$ (используя определение Куратовского).

**Ex22.** Определите наследственно конечное множество, закодированное числом a) 11; b) 15.

# Рай для математиков

*Из рая, который создал для нас Кантор, никто не сможет нас изгнать.*

— Давид Гильберт

## C1.1. Теория множеств Цермело-Френкеля

### C1.1.1 Аксиоматика ZFC

*Эрнст Цермело*

Итак, переходим к строительству самой фундаментальной математической теории — теории множеств Цермело-Френкеля. Язык этой теории в ее основном варианте включает лишь переменные (свободные и связанные) и два бинарных предиката $\in, =$. Однако мы сразу же расширим его так же, как делали это для теории HF: добавим бинарные функциональные символы $\cup, \cap, \smallsetminus, \triangle, \langle\rangle, \times$, унарные функциональные символы $\mathscr{P}, \bigcup$, константу $\varnothing$, а также схему функциональных символов $\{\dots\}$ с конечными арностями для формирования записей конечных множеств.

Разумеется, мы принимаем такие же переобозначения для формул (B2.12) и функциональных символов (B2.13), а также определения HF8 и (B2.17) для функциональных символов. Кроме того, введем в обращение еще несколько новых кванторов:

$$\exists! x\ \varphi[a/x] \overset{\text{def}}{\leftrightarrow} \exists x\ \varphi[a/x] \wedge \forall y\ (\varphi[a/y] \to (y = x)),$$

$$\exists! x \in A:\ \varphi[a/x] \overset{\text{def}}{\leftrightarrow} \exists x \in A:\ \varphi[a/x] \wedge \forall y \in A:\ (\varphi[a/y] \to (y = x)),$$

$$\exists x \subseteq A:\ \varphi[a/x] \overset{\text{def}}{\leftrightarrow} \exists x:\ (x \subseteq A) \wedge \varphi[a/x],$$

$$\forall x \subseteq A:\ \varphi[a/x] \overset{\text{def}}{\leftrightarrow} \forall x:\ (x \subseteq A) \to \varphi[a/x],$$

где формула $\varphi$ может иметь и другие свободные переменные (параметры), кроме $a$.

Первые два квантора выражают существование и единственность свидетеля формулы $\varphi$ (глобально или только в множестве $A$). Такое синтаксическое сокращение не менее полезно, чем определенные в (B2.12) ограниченные кванторы. Третий и четвертый кванторы являются вариациями ограниченных кванторов.

Теперь мы готовы сформулировать аксиоматику ZFC в полном объеме:

ZF1 Конгруэнтность: $(a = b) \to ((a \in M) \leftrightarrow (b \in M))$.

ZF2 Экстенсиональность: $(A = B) \leftrightarrow (\forall x\ (x \in A) \leftrightarrow (x \in B))$.

ZF3 Степень: $\exists \mathscr{P}(A)$.

ZF4 Объединение: $\exists \bigcup A$.

ZF5 Регулярность: $(A \neq \varnothing) \to (\exists x \in A : \forall y \in A : \ y \notin x)$.

ZF6 Подстановка $[\varphi]$: $(\forall x \in A : \exists! y : \varphi(x, y, \vec{p})) \to (\exists Y \ \forall y \ (y \in Y) \leftrightarrow \exists x \in A : \varphi(x, y, \vec{p}))$.

ZF7 Бесконечность: $\exists X \ (\varnothing \in X) \wedge (\forall x \in X : \ x \cup \{x\} \in X)$.

ZF8 Выбор (AC): $(\varnothing \notin A) \to \exists f \subseteq A \times \bigcup A : \ (\forall x \in A : \ \exists! y \in x : \ \langle x, y \rangle \in f)$.

Как легко видеть, у нас пропали из списка аксиома выделения HF3 и аксиома элементарных множеств (пустого и пары) HF6. Дело в том, что теперь мы можем их доказать.

Появившаяся здесь аксиома бесконечности прямо постулирует существование множества $X$, одним из элементов которого является пустое множество, следовательно, пустое множество существует.

Пусть теперь имеется формула $\varphi(a, \vec{p})$ и множество $A$, и мы хотим построить его определяемую часть $\{x \mid (x \in A) \wedge \varphi(x, \vec{p})\}$. Во-первых, заметим, что если $\varphi(x, \vec{p})$ ложно для всех $x \in A$ или если $A = \varnothing$, то ответ мы уже знаем — пустое множество. Предположим, что $A$ не пусто и существует $s \in A$ такой, что $\varphi(s, \vec{p})$. Рассмотрим следующую формулу

$$\psi(a, b, s, \vec{p}) \overset{\text{def}}{\leftrightarrow} (\varphi(a, \vec{p}) \to (b = a)) \wedge (\neg\varphi(a, \vec{p}) \to (b = s)).$$

Нетрудно видеть, что формула $\psi$ удовлетворяет посылке аксиомы ZF6. Эта формула задает, как говорят, *определяемое отображение* типа $a \mapsto b$ множества $A$ в себя так, что оно тождественно там, где $\varphi(a, \vec{p})$ истинно, и постоянно и равно $s$ в остальных точках $A$, так что оно отображает $A$ в область истинности формулы $\varphi$ на $A$. В обычной математике мы записали бы такое отображение следующей лексемой:

$$f(a) = \begin{cases} a, & \varphi(a, \vec{p}), \\ s, & \neg\varphi(a, \vec{p}). \end{cases}$$

Теперь по аксиоме подстановки получаем, что существует множество $Y$, которое можно записать лексемой-сверткой как

$$\{y \mid \exists x \in A : \ \psi(x, y, s, \vec{p})\},$$

а это в точности множество $\{x \mid (x \in A) \wedge \varphi(x, \vec{p})\}$, поскольку

$$(a \in A) \wedge \varphi(a, \vec{p}) \leftrightarrow \exists x \in A : \ \psi(x, a, s, \vec{p}).$$

Следовательно, схема выделения выводима в нашей системе аксиом.[1]

Для обоснования аксиомы пары определим сначала одну уникальную пару: $\{\varnothing, \{\varnothing\}\}$. Она существует как множество $\mathscr{P}(\mathscr{P}(\varnothing))$. После чего нам остается придумать определяемое отображение, которое элементы этой пары будет однозначно переводить в произвольные множества $B$ и $C$. Формула такого отображения:

$$\varphi(g, f, B, C) \overset{\text{def}}{\leftrightarrow} (g = \varnothing) \wedge (f = B) \vee (g = \{\varnothing\}) \wedge (f = C).$$

[1] Дополнительно стоит отметить, что она выводима непосредственно из аксиомы подстановки, аксиомы существования $\varnothing$ и аксиом равенства, т.е. остальные аксиомы здесь не используются.

Отметим, что $\varnothing \neq \{\varnothing\}$, так что формула $\varphi$ будет удовлетворять посылке аксиомы ZF6, где $A = \{\varnothing, \{\varnothing\}\}$, тогда заявленное этой аксиомой множество $Y$ будет совпадать с парой $\{B, C\}$.

Таким образом аксиоматика ZFC расширяет аксиоматику HF без аксиомы HF0, которая есть отрицание аксиомы ZF7. Отметим также, что часто при изучении теории множеств используется аксиоматика без аксиомы выбора ZF8, обозначенной AC. Такой вариант аксиоматики теории множеств обозначается ZF. Если же мы из ZFC исключим аксиому регулярности и аксиому подстановки, но оставим ее следствия — аксиому выделения и аксиому пары, то полученная теория называется аксиоматикой Цермело и обозначается Z. Связь между теориями можно выразить таблицей C1.1.

Таблица C1.1. Сравнение аксиоматик теории множеств

| **Аксиома** | HF | Z | ZF | ZFC |
|---|---|---|---|---|
| Конгруэнтность | ✓ | ✓ | ✓ | ✓ |
| Экстенсиональность | ✓ | ✓ | ✓ | ✓ |
| Пара | ✓ | ✓ | теорема | теорема |
| Степень | ✓ | ✓ | ✓ | ✓ |
| Объединение | ✓ | ✓ | ✓ | ✓ |
| Выделение | ✓ | ✓ | теорема | теорема |
| Пустое множество* | ✓ | теорема | теорема | теорема |
| Регулярность | ✓ | –*** | ✓ | ✓ |
| Подстановка | – | – | ✓ | ✓ |
| Бесконечность | x** | ✓ | ✓ | ✓ |
| Выбор (AC) | – | – | – | ✓ |

* обычно аксиому пустого множества выводят из выделения или бесконечности
** отрицание аксиомы бесконечности
*** прочерк означает, что аксиома отсутствует в списке аксиом теории

Первые 7 аксиом мы выделили как некую *абсолютную теорию множеств*, которую всегда хотелось бы иметь под рукой, но у которой нет специального обозначения. Ее моделью будут, например, наследственно конечные множества и скобочные записи, но в то же время и другие, более сложные универсумы множеств. Мы даем это определение по аналогии с абсолютной геометрией, включающей только первые четыре постулата Эвклида.

Во всех этих теориях множеств, включая абсолютную теорию множеств, существование множеств $a \cap b, a \cup b, a \setminus b, a \triangle b, \langle a, b\rangle, a \times b$ доказывается ровно так же, как мы уже делали ранее, опираясь на схему выделения, объединение и пару.

Посмотрим теперь, что нам дает аксиома бесконечности. Для начала введем обозначение $S(a) \overset{\text{def}}{\rightleftharpoons} a \cup \{a\}$, аналогичное арифметической операции последователя, выражающей добавление единицы. Здесь мы тоже в каком-то смысле добавляем единицу, а именно, одну новую точку $a$ к множеству $a$. В силу аксиомы регулярности, как мы уже видели в теории HF, $a \notin a$, так что это действительно новая точка относительно

$a$ как множества. И теперь мы точно так же, как в арифметике, можем задать серию определений *нумералов*:

$$0 \overset{\text{def}}{\rightleftharpoons} \varnothing, \quad 1 \overset{\text{def}}{\rightleftharpoons} S(0), \quad 2 \overset{\text{def}}{\rightleftharpoons} S(1), \quad 3 \overset{\text{def}}{\rightleftharpoons} S(2), \ldots$$

Это — так называемые натуральные числа фон Неймана, которые являются характерным признаком вселенной множеств фон Неймана, отвечающей аксиоме регулярности.

Аксиома бесконечности говорит нам, что существует некое множество $X$, элементами которого являются числа фон Неймана. По сути этой аксиомой заявляется существование множества натуральных чисел, как объекта теории. Иными словами, постулируется актуальная бесконечность. Множество $a$, которое удовлетворяет свойству $Ind(a) \overset{\text{def}}{\leftrightarrow} (0 \in a) \wedge (\forall x \in a : S(x) \in a)$, называется **индуктивным**. Взяв произвольное индуктивное множество $a$ (которое существует по аксиоме бесконечности), мы можем выделить его часть по правилу:

$$\omega \overset{\text{def}}{\rightleftharpoons} \{x \mid (x \in a) \wedge (\forall y\ Ind(y) \to (x \in y))\}.$$

Множество $\omega$ существует по аксиоме выделения и является не чем иным, как пересечением всех индуктивных множеств, поэтому его еще можно записать так:

$$\omega = \bigcap_{Ind(x)} x.$$

Последнее выражение является лексемой-сверткой, для которой можно ввести следующее первопорядковое определение-аксиому

$$a \in \bigcap_{\varphi(y,\vec{p})} y \overset{\text{def}}{\leftrightarrow} \exists x\ \varphi(x,\vec{p}) \wedge \forall y\ (\varphi(y,\vec{p}) \to (a \in y))$$

с первопорядковой формулой $\varphi$. При этом если формула $\varphi$ тождественно ложна (при данных значениях параметров $\vec{p}$), то получаем, что $\bigcap_{\varphi(y,\vec{p})} y = \varnothing$, а если формула $\varphi$ имеет хотя бы одного свидетеля, то, как было сказано выше, лексема $\bigcap_{\varphi(y,\vec{p})} y$ будет обозначать множество, существование которого гарантировано аксиомой выделения. Довесок $\exists x\ \varphi(x,\vec{p})$ в данном определении свертки нужен именно для случая тождественно ложной формулы $\varphi(x,\vec{p})$, т.к. если его убрать, то в этом случае импликация $\varphi(y,\vec{p}) \to (a \in y)$ окажется истинной для всех $a$, и наша лексема-свертка перестанет обозначать множество (это будет класс всех множеств).

Таким образом множество $\omega$ является минимальным (в смысле отношения $\subseteq$) индуктивным множеством. Это множество состоит в точности из натуральных чисел фон Неймана.

## C1.1.2 Отношения, функции и классы

Отметим, что теперь определение математического понятия, данного на стр. 47, можно переформулировать в языке теории ZF следующим образом:

▶ Определение понятия (*интенсионал*) — это формула $\varphi(a,\vec{p})$ в языке ZF, которая выражает совокупность свойств (признаков) множеств, поименованных переменной $a$ и зависящих от параметров $\vec{p}$.

- Объем понятия (*экстенсионал*) — это все множества $a$, удовлетворяющие формуле $\varphi(a, \vec{p})$, и только они. Объем понятия зависит от параметров $\vec{p}$.
- Термин понятия — это закрепленное за ним название на разговорном языке (он может включать в себя ссылку на параметры).
- Обозначение понятия — это лексема языка (не обязательно исходного языка ZF), введенная определением-аксиомой как сокращенная запись либо определяющей формулы $\varphi(a, \vec{p})$, либо терма, обозначающего объем понятия, либо это переменная, пробегающая только элементы объема понятия.

Например, понятие «натуральное число фон Неймана» задается формулой $\forall y \ (Ind(y) \rightarrow (a \in y))$ без параметров, его объем содержит все натуральные числа фон Неймана и только их, а его обозначение — это константа $\omega$.[2]

Другой пример: понятие «прямое произведение множеств $A$ и $B$» задается формулой $\exists x \in A : \exists y \in B : (a = \langle x, y \rangle)$ с параметрами $A$ и $B$. В строгом соответствии с указанным выше определением математического понятия объем данного понятия представляет собой множество всех упорядоченных пар Куратовского $\langle x, y \rangle$, в которых $x \in A$ и $y \in B$, и только их, а соответствующее обозначение — это терм $A \times B$.

Неформально в теории множеств ZF используется понятие класс. На уровне метатеории **класс** — это математическое понятие в языке ZF. Чаще всего класс отождествляется со своим объемом. Таким образом, если мы имеем математическое понятие, заданное формулой $\varphi(a, \vec{p})$, то класс отождествляется с термом $\{a \mid \varphi(a, \vec{p})\}$. Если при конкретизации параметров $\vec{p}$ класс не совпадает ни с каким множеством, то он называется *собственно классом*.

Как мы только что заметили, объем понятия «прямое произведение $A$ и $B$» при конкретизации параметров представляет собой конкретное множество $A \times B$ и не является собственно классом. Однако если посмотреть на понятие «прямое произведение двух множеств» в общем виде, не имея в виду конкретизацию параметров, то мы имеем дело с собственно классом, состоящим из всех прямых произведений произвольных множеств. Такой класс уже не будет множеством, а будет собственно классом.

Собственно классом также будет класс Рассела $R = \{x \mid x \notin x\}$, так как в противном случае мы бы получили известное противоречие.

Для формального узаконивания понятия *класса множеств* используется формальная система с двумя типами объектов — множества и классы, где всякое множество есть класс, но не наоборот. Это теория Гёделя-Бернайса (GB), являющаяся двухтиповой формальной теорией множеств в языке первого порядка. Она характеризуется тем, что список ее аксиом конечен (нет схем аксиом), допускаются кванторы по классам, но сама теория при этом является консервативным расширением ZF (ZFC).[3]

В дальнейшем мы не будем столь тщательно показывать все необходимые компоненты математического понятия, но будем вводить их так, как это принято в математике, выделяя термин курсивом или жирным шрифтом, понимая под этим понятием соответствующий ему класс или множество объектов, зависящие от параметров, если таковые есть в определении.

[2] Тут нужно отличать обозначение объема понятия и общее обозначение его элементов. Обычно элементы $\omega$ обозначают латинскими буквами из середины алфавита: $l, m, n, k$ и т.п.

[3] Это означает, что любая теорема, формулируемая исключительно в терминах множеств, доказуема в GB тогда и только тогда, когда она доказуема в ZF.

Теперь настало время окончательно формализовать теоретико-множественные понятия, введенные в разделе A2.7.

*Отношением* между множествами $A$ и $B$ называется любое подмножество $R \subseteq A \times B$. Если $R$ — отношение, то вместо формулы $\langle a, b\rangle \in R$ принято писать $aRb$. Если $A = B$, то отношение между $A$ и $B$ называется отношением на $A$. Например, мы можем определить отношение $\leqslant$ на элементах $\omega$ так:

$$a < b \overset{\text{def}}{\leftrightarrow} a \in b.$$

В Части II мы докажем, что данное отношение $<$ будет отношением строго линейного порядка (и даже вполне упорядочением) на натуральных числах фон Неймана (см. теорему D4.4). В соответствии с принятым обозначением мы можем теперь написать, например, $3 < 5$ или $n < S(n)$ при $n \in \omega$.

Соответственно, мы можем воспроизвести виды отношения $R$ на множестве $A$:

- *рефлексивное* — $\forall x \in A :\ xRx$;
- *антирефлексивное* — $\forall x \in A :\ \neg(xRx)$;
- *симметричное* — $\forall x, y \in A :\ xRy \to yRx$;
- *обратное* к $R$ отношение — $\forall x, y\ \langle x, y\rangle \in R \leftrightarrow \langle y, x\rangle \in R^{-1}$
- *антисимметричное* — $\forall x, y \in A :\ xRy \wedge yRx \to x = y$;
- *транзитивное* — $\forall x, y, z \in A :\ xRy \wedge yRz \to zRz$;
- *связное* — $\forall x, y \in A :\ (xRy) \vee (x = y) \vee (yRx)$;[4]
- *предпорядок* — рефлексивное и транзитивное;
- *отношение эквивалентности* — рефлексивное, симметричное, транзитивное;
- *частичный (нестрогий) порядок* — антисимметричный предпорядок;
- *строгий частичный порядок* — антирефлексивное и транзитивное;
- *линейный порядок* — связный частичный порядок.
- *вполне упорядочение* на $A$ — линейный порядок, для которого

$$\forall X \subseteq A : (X \neq \varnothing) \to \exists x \in X : \forall y \in X : (xRy)$$

(такой элемент $x$ называется минимумом множества $X$ и обозначается $\min_R X$).

Соответственно, множество вместе с заданным на нем отношением (частичного/линейного/вполне) порядка называется (частично/линейно/вполне) *упорядоченным множеством*. Здесь слово «вместе» подразумевает, что мы рассматриваем пару, включающую множество и отношение на нем.

А также виды отношения $R \subseteq A \times B$:

[4] В теории порядков это свойство иногда называют *тотальностью* или *линейностью*. Однако, поскольку слово «тотальность» у нас уже занято свойством всюду определенности, во избежание путаницы мы используем термин «связность». Такая терминология стандартна для общей алгебры и логики (см., напр., [52]).

- *всюду определенное* — $\forall x \in A : \exists y \in B :\ xRy$;
- *однозначное (функциональное)* — $\forall x \in A : \forall y, z \in B :\ xRy \wedge xRz \to y = z$;
- **функция из $A$ в $B$** — всюду определенное однозначное.

Тот факт, что отношение $f$ есть *функция* из $A$ в $B$ записывается сокращенной формулой $f : A \to B$. Заметим, что это формула с тремя параметрами, а не терм.

Если имеет место функция $f : A \to B$, то $A$ называется ее областью определения, а множество $\{y \mid (y \in B) \wedge \exists x \in A : \langle x, t\rangle \in f\}$ называется областью значений функции $f$ и обозначается термом $\mathrm{ran}(f)$.

Эти определения можно расширить, предполагая, что вместо множеств $A, B, R$ используются первопорядковые формулы $\varphi_A, \varphi_B, \varphi_R$ и вместо предиката принадлежности всюду в определениях стоят формулы $\varphi_A(x), \varphi_B(y), \varphi_R(x, y)$. Это позволяет говорить об *определяемом отношении на классе* (между классами). Так, например, мы можем ввести в рассмотрение класс $\mathfrak{V}$ всех множеств, определяющей формулой которого будет $(x = x)$. Более того, пользуясь лексемой-сверткой мы могли бы сказать, что $\mathfrak{V} = \{x \mid x = x\}$, однако здесь уже нам следует вспомнить о парадоксе Рассела и о том, что у нас нет аксиом, позволяющих доказать, что $\mathfrak{V}$ есть множество. Поэтому, хотя часто и используется понятие класса, нужно всегда понимать, что класс $\mathfrak{C}$, определенный формулой $\varphi(a, \vec{p})$, можно подставлять в предикат принадлежности только справа $a \in \mathfrak{C}$ и под этой формулой понимать всякий раз не что иное, как формулу $\varphi(a, \vec{p})$.

Теперь, если у нас имеется формула $\varphi(x, y, \vec{p})$, которая определяет функциональное отношение на универсуме всех множеств $\mathfrak{V}$ и если оно всюду определено на некотором классе $\mathfrak{C}$, то мы говорим, что формула $\varphi$ задает **определяемое отображение** на $\mathfrak{C}$, что можно записать сокращенно в виде $\varphi : \mathfrak{C} \to \mathfrak{V}$. Но при этом мы не используем термин *функция*, т.к. он зарезервирован строго за функциональными отношениями между множествами!

Однако если у нас имеется функциональное отношение, всюду определенное на множестве, то уже в силу аксиомы подстановки оно-таки является функцией, поскольку аксиома подстановки гарантирует, что область значений такого отображения является множеством.

Наконец, определим *значение функции в точке $a$* для функции $f : A \to B$:

$$f(a) \overset{\text{def}}{\rightleftharpoons} \bigcup \{y \mid (y \in B) \wedge \langle a, y\rangle \in f\}.$$

Поскольку такой $y$ существует и единственный в силу всюду определенности и функциональности $f$, множество $\{y \mid (y \in B) \wedge \langle a, y\rangle \in f\}$ состоит из единственной точки, которая и обозначается термом $f(a)$. Таким образом

$$b = f(a) \leftrightarrow \langle a, b\rangle \in f.$$

Пусть далее имеется функция $f : A \to B$ и два подмножества $X \subseteq A$ и $Y \subseteq B$. Дадим такие определения: **образом** множества $X$ (относительно $f$) называется множество $f[X] \overset{\text{def}}{\rightleftharpoons} \{b \mid \exists a \in X : (b = f(a))\}$, **прообразом** множества $Y$ (относительно $f$) называется множество $f^{-1}[Y] \overset{\text{def}}{\rightleftharpoons} \{a \mid (a \in A) \wedge (f(a) \in Y)\}$.

Для того, чтобы отличать значение функции в точке от образа множества, мы используем в первом случае круглые скобки, а во втором — квадратные.

Из приведенных определений, в частности, следует, что для всякой функции $f : A \to B$

$$\mathrm{ran}(f) = f[A], \quad f^{-1}[B] = A.$$

### C1.1.3 Зачем нужны функции

Понятие функции является, пожалуй, одним из центральных математических понятий, т.к. используется повсеместно в различных математических науках. Поэтому терминологический аппарат вокруг функций чрезвычайно развит, и мы обязаны рассмотреть здесь хотя бы основные виды функций:

- $f : A \to B$ — **постоянная**, если существует такой $b \in B$, что $\forall x \in A : f(x) = b$;
- $f : A \to A$ — **тождественная** на $A$, если $\forall x \in A : f(x) = x$, в этом случае она обозначается как $\mathrm{id}_A$;
- $f : A \to \{0, 1\}$ — **индикаторная функция** множества $S \subseteq A$, если $\forall x \in A : f(x) = 1 \leftrightarrow (x \in S)$, в этом случае она обозначается $\chi_A$;
- $f : A \to B$ — **инъекция** (*вложение*), если $f(a) = f(b) \to a = b$;
- $f : A \to B$ — **сюръекция** (*отображение «на»*), если $\forall y \in B : \exists x \in A : y = f(x)$;
- $f : A \to B$ — **биекция** (*взаимно однозначная*), если она инъекция и сюръекция одновременно, предикат функции в этом случае пишется так: $f : A \leftrightarrow B$;
- если $f : A \to B$ и $g : B \to C$, то композицией $g \circ f$ называется функция $h : A \to B$ такая, что $h(a) = g(f(a))$ (в терминах отношений: $g \circ f = \{\langle x, z\rangle \mid \exists y \in B : \langle x, y\rangle \in f \wedge \langle y, z\rangle \in g\}$);
- функция $g : B \to A$ называется **обратной** к $f : A \to B$, если $\forall x \in A : g(f(x)) = x$ и $\forall y \in B : f(g(y)) = y$, при этом обратная функция обозначается $f^{-1}$.

Наличие биекции $f : A \leftrightarrow B$ указывает на то, что между этими множествами существует взаимно однозначное соответствие (примерно как застежка-молния), т.е. в них как бы «поровну» элементов. Конечно, это представление сложно перенести на бесконечные множества, но без наличия на множествах какой-либо дополнительной структуры трудно себе представить, как бы еще можно было что-либо сказать о их «одинаковости», кроме как предъявив биекцию.

Поэтому существует следующее определение: два множества $A$ и $B$ **равномощны** ($A \simeq B$), если существует биекция $f : A \leftrightarrow B$. Отсюда возникают вторичные определения: множество **конечно**, если оно равномощно некоторому $n \in \omega$, бесконечно — в противном случае,[5] **счетно** — если оно равномощно $\omega$, **не более чем счетно** — если оно конечно или счетно.

Отношение равномощности $\simeq$ является отношением эквивалентности на классе всех множеств, т.е. на универсуме $\mathfrak{V}$, это — определяемое отношение-класс. Кроме того, класс всех множеств, равномощных множеству $A$, часто обозначается как $\mathrm{Card}(A)$ и называется кардинальностью множества $A$.[6]

Приведем лишь малое количество примеров использования понятия функции в математике.

[5] Надо заметить, что существует несколько разновидностей определения этих терминов, например, конечные по Тарскому (наше определение) и по Дедекинду, которые в рамках ZFC эквивалентны, но в более слабых теориях могут отличаться.

[6] Кантор определял кардинальность так: это — то общее, что есть у всех множеств, равномощных данному.

- Векторы, понимаемые как кортежи элементов, — это функции, определенные на конечном носителе (обычно на множестве $\{1, \dots, n\}$).
- Функцию, заданную на произведении натуральных чисел фон Неймана $n \times m$, можно понимать как матрицу размера $nm$.
- Множество всех биекций множества $H$ образует группу относительно операции композиции $\circ$. Единицей такой операции является функция $\mathrm{id}_H$. В частности, если $H$ конечно, то такая группа биекций называется симметрической группой, или группой подстановок.
- Последовательности, ряды и интегралы в основе своей используют понятие функции. В частности, такие понятия, как гильбертовы пространства (используемые также в квантовой механике) есть множества функций с определеными свойствами.
- Норма, метрика, функционал, линейный оператор, мера, случайная величина, тензор, скалярное произведение — все это различные виды функций.

## C1.2. Аксиома выбора

Перейдем теперь к обсуждению последней аксиомы из нашего списка — аксиоме выбора. Приведем еще раз ее формулировку:

$$(\varnothing \notin A) \to \exists f \subseteq A \times \bigcup A : \ (\forall x \in A : \ \exists! y \in x : \ \langle x, y \rangle \in f).$$

Первое, что в ней заявляется — в $A$ нет пустого элемента. Второе — что $f$ есть отношение между множествами $A$ и $\bigcup A$. Третье — что это отношение всюду определено и функционально. Наконец, четвертое — что $f(x) \in x$. И главный тезис аксиомы заключается в том, что такое $f$ существует. С учетом функциональных обозначений аксиому выбора можно переформулировать так:

$$(\varnothing \notin A) \to \exists f \ (f : A \to \bigcup A) \wedge \forall x \in A : \ f(x) \in x.$$

Иначе говоря, каким бы ни было множество $A$ без пустого элемента, всегда найдется функция $f$, которая в каждом его элементе выбирает один элемент. Эта формулировка интуитивно понятна: если у вас есть «мешок с мешками», и каждый мешок не пуст, то вы можете выбрать по одному предмету из каждого мешка.

Такая функция $f$ называется **функцией выбора** на множестве $A$. Отметим, что единственным требованием к множеству $A$ является отсутствие пустого элемента. Это требование не слишком существенно, поскольку если в каком-то множестве $B$ есть пустой элемент, то мы всегда можем перейти к множеству $A = B \setminus \{\varnothing\}$ и применить к нему аксиому. Тем не менее, нужно помнить, что когда речь идет о функции $f : A \to \bigcup A$, она должна быть всюду определенной на $A$. Это значит, что на множестве, имеющем пустой элемент, функции выбора не существует (т.к. невозможно выполнить требование $f(\varnothing) \in \varnothing$).

Логика и здравый смысл требуют от нас проверить также, не получится ли какое-нибудь противоречие, если множество $A$ окажется пустым. Во-первых, заметим, что

$$c \in \bigcup \varnothing \leftrightarrow \exists x \in \varnothing : \ c \in x,$$

где справа стоит ложная формула, а значит, $\bigcup \varnothing = \varnothing$. Во-вторых,

$$c \in \varnothing \times \varnothing \leftrightarrow \exists x \in \varnothing : \ \exists y \in \varnothing : \ c = \langle x, y \rangle,$$

где справа опять ложная формула, а значит, $\varnothing \times \varnothing = \varnothing$. Более того, верны также и равенства $A \times \varnothing = \varnothing$ и $\varnothing \times B = \varnothing$, так что пустое множество является нулевым элементом операции прямого произведения множеств.

Очевидно, что если $f \subseteq \varnothing \times \varnothing$, то $f = \varnothing$ и, следовательно, предикат $\langle x, y \rangle \in f$ ложный. Но в аксиоме стоит квантор $\forall x \in A$, который раскрывается по определению так:

$$\forall x \ (x \in A) \to \exists! y \in x : \langle x, y \rangle \in f.$$

В случае $A = \varnothing$ посылка импликации будет ложной, а значит, вся импликация будет истинной, и никакого противоречия не появится. Т.е. в данном случае функция выбора будет пустой, что не противоречит ее основному свойству. Вообще, про пустое множество можно сказать, что для него выполняется любое свойство, начинающееся с квантора всеобщности («все элементы пустого множества пусты», «все элементы пустого множества бесконечны» и т.д.). Это — прямое следствие применения *материальной импликации*.

Примеры: на множестве $\{\varnothing\}$ не существует функции выбора, а на множестве $\varnothing$ функция выбора существует и равна $\varnothing$.

У аксиомы выбора существует иная, часто более удобная формулировка

$$(I : A \to B) \wedge (\forall x \in A : I_x \neq \varnothing) \to \exists f : A \to \bigcup_{x \in A} I_x : \forall x \in A : f(x) \in I_x. \tag{C1.1}$$

Для начала прокомментируем вольности, которые мы допустили при написании формулы. Во-первых, значение функции $I$ в точке $x$ мы обозначили как $I_x$ вместо $I(x)$. Это — распространенный в математике способ записи значения функции с использованием индекса. Во-вторых, мы немного сократили синтаксически корректную запись $\exists f \ f : A \to \bigcup_{x \in A} I_x$, удалив двойное написание подряд буквы $f$. Такие сокращения тоже допустимы (на мета-уровне), поскольку не вызывают разночтений. В-третьих, мы ввели в обращение лексему-свертку, которую можно задать прямым определением

$$\bigcup_{x \in A} I_x \stackrel{\text{def}}{\rightleftharpoons} \bigcup \operatorname{ran}(I),$$

поскольку область значений функции есть множество по аксиоме подстановки.

Формулировка AC в виде (C1.1) говорит, что если у нас есть проиндексированное семейство множеств (которое является множеством в силу аксиомы подстановки), то мы можем выбрать проиндексированное семейство элементов этих множеств, взяв по одному из каждого. Интуитивно, если у нас имеется ряд пронумерованных ящиков, то мы можем взять из каждого по предмету, приклеить к ним бирки с номерами ящиков и положить в один мешок.

Функция $f$, существование которой указано в (C1.1), тоже называется *функцией выбора*, но не на множестве $A$, а *для семейства множеств* $I_x$.

**Теорема C1.1.** *Формулировки аксиомы выбора в форме* ZF8 *и в форме* (C1.1) *эквивалентны в* ZF.

*Доказательство.* Из (C1.1) аксиома в форме ZF8 следует тривиально: просто положим $I(x) = x$.

Обратно. Пусть $I : A \to B$ и всякий $I_x$ не пуст при $x \in A$. Применим аксиому выбора в форме ZF8 к множеству $\operatorname{ran}(I)$: пусть $f : \operatorname{ran}(I) \to \bigcup \operatorname{ran}(I)$ — функция выбора. Тогда функция $g : A \to \bigcup_{x \in A} I_x$, определяемая правилом композиции $g(x) = f(I_x)$, является искомой функцией выбора в (C1.1). □

Аксиома выбора AC впервые явно сформулирована Эрнстом Цермело в 1904 году в ходе попытки доказать теорему о вполне упорядочении любого множества, однако она использовалась математиками интуитивно задолго до своего формального введения, поскольку казалась очевидным фактом. Сразу после явной формулировки AC вызвала значительные споры из-за своей неконструктивной природы: она постулирует существование функции выбора, не предоставляя конкретного способа ее построения.

Курт Гёдель в 1938 году доказал, что если остальные аксиомы Цермело-Френкеля непротиворечивы, то добавление к ним AC не приводит к противоречию (то есть AC относительна непротиворечива с ZF).

Пол Коэн в 1963 году доказал, что AC нельзя вывести из аксиом ZF (то есть AC независима от ZF), используя метод форсинга. Это означает, что существуют модели теории множеств, где AC истинна, и модели, где она ложна.

AC имеет огромное значение во многих разделах математики, позволяя доказывать важные теоремы, которые невозможно или крайне сложно доказать без нее в рамках ZF. Она эквивалентна нескольким другим важным утверждениям, таким как теорема Цермело о вполнеупорядочивании и лемма Цорна.

**Теорема C1.2.** *Следующие утверждения эквивалентны в теории ZF:*

(1) *аксиома выбора;*

(2) *теорема Цермело: любое множество можно вполне упорядочить;*

(3) *лемма Цорна: если в частично упорядоченном множестве любая цепь ограничена сверху, то в нем существует максимальный элемент.*

(4) *принцип максимума Хаусдорфа: в любом частично упорядоченном множестве существует максимальная по вложению цепь.*

С точки зрения языка математики нам важно уметь конвертировать слова в формулы и наоборот, поэтому вместо доказательства этой теоремы, за которым мы опять-таки отсылаем к Части II (см. теорему D4.13), покажем, как эти три формулировки теорем переводятся на (обогащенный) язык ZF.

С теоремой Цермело нет особых проблем, поскольку мы вводили определение вполне упорядоченного множества. Это — линейно упорядоченное множество, каждое непустое подмножество которого имеет минимум. Теперь перевод:

$$\exists R \subseteq A \times A : [\forall x, y, z \in A : (xRx) \wedge (xRy \wedge yRz \to xRz) \wedge (xRy \wedge yRx \to x = y) \wedge$$
$$\wedge (xRy \vee x = y \vee yRx)] \wedge (\forall X \subseteq A : (X \neq \varnothing) \to \exists y \in X : \forall x \in X : yRx)$$

Разберем эту формулу. Во-первых, в ней есть одна свободная переменная $A$, которая отвечает за «любое множество». Далее заявляется наличие некоторого отношения $R$ на $A$ ($R \subseteq A \times A$), которое обладает рядом свойств. Свойства, перечисленные в квадратных скобках, — это свойства нестрогого линейного порядка: рефлексивность, транзитивность, антисимметричность и связность. Чтобы лучше представлять себе смысл

формулы, нужно мысленно заменить $R$ на $\leqslant$. Наконец, последнее условие на $R$ говорит нам, что в любом непустом подмножестве $X \subseteq A$ существует элемент $y$, который меньше либо равен любого $x \in X$, т.е. является минимумом этого подмножества.

Кстати, дадим определение. Если $\leqslant$ — частичный (нестрогий) порядок на $X$ и $A \subseteq X$, то *минимальным* (*максимальным*) элементом множества $A$ называется такой $m \in A$, что в $A$ нет элементов меньше (больше) его, а *минимумом* (*максимумом*) — такой $M \in A$, что $M \leqslant x$ ($x \leqslant M$) для всех $x \in A$.

Заметим: нет элементов — не значит, что он меньше (больше) всех остальных. В этом есть принципиальная разница между понятиями минимального элемента и минимума. Например, если в качестве $\leqslant$ мы рассматриваем отношение делимости на натуральных числах, начиная с 2 (исключаем 1 и 0), то все простые числа будут минимальными элементами, т.к. нет чисел, делящих их, кроме их самих. Однако если мы вернем в это множество 1, то она будет минимумом, поскольку она делит все положительные натуральные числа.

В линейно упорядоченном множестве, где все элементы попарно сравнимы друг с другом, разница между этими понятиями исчезает.

Добавим также определения граней и точных граней. Элемент $b \in X$ называется верхней (нижней) **гранью** множества $A$, если $\forall x \in A : x \leqslant b$ ($\forall x \in A : b \leqslant x$). Верхняя (нижняя) грань называется точной, если она является минимумом (максимумом) множества всех верхних (нижних) граней множества $A$. Точная верхняя грань множества $A$ обозначается $\sup A$, точная нижняя — $\inf A$. Из определения ясно, что они не всегда могут существовать.

Заметим также, что если $A = \varnothing$, то его верхними и нижними гранями будут все элементы множества $X$, что немного странно, поскольку некоторые нижние грани могут быть больше, чем некоторые верхние. Поэтому как правило предполагается, что понятия граней определяются только для непустого множества $A$.

Данные определения позволяют ввести новые обозначения и новые кванторы:

$$m = \min_{\leqslant} A \overset{\text{def}}{\leftrightarrow} (m \in A) \wedge \forall x \in A : m \leqslant x, \quad M = \max_{\leqslant} A \overset{\text{def}}{\leftrightarrow} (M \in A) \wedge \forall x \in A : x \leqslant M,$$

$$\exists \min_{\leqslant} A \overset{\text{def}}{\leftrightarrow} \exists m \in A : m = \min_{\leqslant} A, \quad \exists \max_{\leqslant} A \overset{\text{def}}{\leftrightarrow} \exists M \in A : M = \max_{\leqslant} A.$$

В таких обозначениях последнее условие на $R$ в теореме Цермело можно переписать короче: $\forall X \subseteq A : \exists \min_R X$. А если еще добавить специальный предикат

$$Lin(A, R) \overset{\text{def}}{\leftrightarrow}$$
$$\forall x, y, z \in A : (xRx) \wedge (xRy \wedge yRz \to xRz) \wedge (xRy \wedge yRx \to x = y) \wedge (xRy \vee x = y \vee yRx),$$

который означает, что $R$ есть линейный порядок на $A$, то теорема Цермело примет уже вполне респектабельный вид:

$$\exists R \subseteq A \times A : Lin(A, R) \wedge \forall X \subseteq A : (X \neq \varnothing) \to \exists \min_R X.$$

Стоит заметить также, что если множество $A$ пусто, то оно является вполне упорядоченным единственным возможным на нем отношением $\varnothing$.

Лемма Цорна потребует большего напряжения для перевода на язык ZF, т.к. нам нужно сначала дать определения. Во-первых, скажем, что отношение $Q$ есть *индуцированное* (*ограниченное*) на множество $B$ отношение $R \subseteq A \times A$ (обозначение: $R \restriction B$), если

$Q = R \cap (B \times B)$. Во-вторых, *цепью* в частично упорядоченном множестве называется такое его подмножество, что индуцированный на него частичный порядок является линейным.[7] Если представлять себе частичный порядок в виде дерева, то цепью будет любой путь (причем этот путь может пропускать некоторые вершины, пользуясь транзитивностью). Наконец, мы говорим, что цепь $C \subseteq A$ *ограничена сверху* (снизу), если в $A$ существует верхняя (нижняя) грань $C$.

Введем еще предикат частичного порядка:

$$Part(A,R) \overset{\text{def}}{\leftrightarrow} \forall x,y,z \in A : (xRx) \wedge (xRy \wedge yRz \to xRz) \wedge (xRy \wedge yRx \to x = y).$$

Переходим к записи леммы Цорна:

$$Part(A,R) \wedge (\forall C \subseteq A : Lin(C, R \restriction C) \to \exists m \in A : m = \max_R(C \cup \{m\})) \to$$
$$\to \exists m \in A : \forall x \in A : (mRx) \to (m = x).$$

Последняя подформула $\forall x \in A : (mRx) \to (m = x)$ означает, что $m$ есть максимальный элемент, т.е. нет больших его элементов (это записано так: если есть больше либо равный, то он равен, т.к. мы здесь пользуемся нестрогим частичным порядком).

Как видим, формулировки сколько-нибудь содержательных теорем в языке ZF даже с кучей сокращений приобретают вид поэмы. Трудно представить, как эти формулировки будут выглядеть в «ассемблере» математики — в исходном языке теории множеств, основанном только на одном предикате $\in$. Тем не менее, все наши предыдущие построения однозначно свидетельствуют о том, что такой перевод возможен.

Принцип максимума Хаусдорфа мы предлагаем записать читателю самостоятельно.

Аксиома выбора дает многочисленные полезные следствия в самых разных областях математики, например:

- теорема* Тихонова о произведении компактных пространств,
- теорема* о существовании базиса в векторном пространстве,
- теорема* о том, что каждое подпространство векторного пространства имеет прямое дополнение,
- теорема* Крулля о максимальном идеале в кольце с единицей,
- теорема* о существовании максимального идеала в решетке с максимумом,
- теорема** о простом идеале булевой алгебры (BPI),
- теорема** Тарского об ультрафильтре,
- теорема** Гёделя о полноте логики предикатов (для несчетных языков),
- теорема** Стоуна о представлении булевых алгебр,
- теорема** Артина-Шрайера об упорядочении формально вещественного поля.
- теорема Хана-Банаха о продолжении линейного функционала,

[7] Двойственным к понятию цепи является понятие антицепи: такое подмножество, все элементы которого попарно не связаны индуцированным порядком. Принцип максимальной антицепи также равносилен аксиоме выбора.

- теорема об алгебраическом замыкании поля,
- теорема Нильсена-Шрайера о том, что подгруппа свободной группы свободна,
- теорема Шпильрайна о продолжении частичного порядка до линейного,

Отмеченные * теоремы равносильны аксиоме выбора, отмеченные ** теоремы равносильны друг другу и строго слабее AC. Теорема Нильсена-Шрайера влечет аксиому выбора для семейств конечных множеств, но не известно, равносильна ли она полной аксиоме выбора.

Теорема Хана – Банаха строго слабее BPI. Теорема Шпильрайна (она же — принцип расширения порядка) также строго слабее BPI, однако если к ней добавить принцип конфинальности (любой линейный порядок содержит в себе конфинальное вполне упорядоченное подмножество), то вместе они влекут AC.

Теорема об алгебраическом замыкании поля следует из BPI, она не считается эквивалентной BPI (но это пока не точно).

Для того, чтобы пронаблюдать всю эту великолепную картину зависимостей различных математических утверждений, так или иначе связанных с аксиомой выбора, рекомендуем обратиться к книге [51].

Некоторые следствия AC могут показаться контринтуитивными. Наиболее известным примером является парадокс Банаха-Тарского, утверждающий, что трехмерный шар можно разделить на конечное число частей, из которых можно собрать два шара того же размера (понятие шара предполагает, что в нем нет пустот). Разумеется, эти части шара будут неизмеримы по Лебегу.

Несмотря на споры и контринтуитивные следствия, аксиома выбора широко принимается большинством математиков как стандартный инструмент и является частью стандартной аксиоматики.

Тем не менее изучение математики без AC также является активной областью исследований. Здесь предлагаются различные варианты ослабления общей аксиомы выбора до, например, ее счетной версии $AC_\omega$, утверждающей наличие функции выбора лишь для счетных семейств непустых множеств, а также альтернативные аксиомы: аксиома зависимого выбора, аксиома детерминированности и т.д.

Надо отметить, что $AC_\omega$ обладает хорошим запасом полезных следствий, прежде всего, в теориях, не выходящих за пределы континуума (таких, как математический анализ и арифметика второго порядка), и в то же время она не имеет известных парадоксальных следствий вроде теоремы Банаха-Тарского или примера Витали.

В рамках счетной аксиомы выбора можно доказать, например, такие следствия:

- любое бесконечное множество содержит счетное подмножество (см. теорему D4.11);
- каждое бесконечное множество является бесконечным по Дедекинду (см. теорему D4.11);
- счетное объединение счетных множеств счетно;
- бесконечная теорема Рамсея (с произвольными параметрами);
- множество всех вещественных чисел не является счетным объединением счетных множеств;
- любое подпространство сепарабельного метрического пространства сепарабельно;

- мера Лебега счетно аддитивна,
- сильная лемма Кенига: в любом бесконечном дереве с конечным ветвлением существует бесконечный путь.

Все приведенные утверждения слабее аксиомы $\mathrm{AC}_\omega$, но могут быть равносильны некоторым более слабым вариантам аксиомы выбора. Например, лемма Кенига а такой формулировке (без указания на счетность дерева и нумерацию вершин) равносильна аксиоме $\mathrm{AC}_\omega^{fin}$ (счетный выбор из конечных множеств), бесконечная теорема Рамсея слабее, чем $\mathrm{AC}_\omega$, но сильнее, чем $\mathrm{AC}_\omega^{fin}$, а теорема о том, что счетное объединение счетных множеств счетно, равносильно счетному выбору из счетных множеств.

После приведенных примеров про AC и $\mathrm{AC}_\omega$ может сложиться впечатление, что все известные теоремы либо равносильны одной из форм аксиомы выбора, либо слабее их, а то и вовсе доказываются в ZF. Однако это не так. Можно привести «повышающий список» принципов (теорем, аксиом), из которых следует AC, но которые ей не равносильны. К таковым относится, например, обобщенная континуум-гипотеза GCH (она строго сильнее AC), аксиома конструктивности Гёделя $V = L$ (она строго сильнее, чем GCH и, следовательно, чем AC).

А также существует некоторое количество альтернатив аксиомы выбора. Достаточно указать, например, *аксиому детерминированности* AD, обладающую многими полезными следствиями (в частности, $\mathrm{ZF} + \mathrm{AD} \vdash \mathrm{AC}_\omega$), но не дающую известных парадоксов.

Таким образом, от точки AC в языке ZF можно ходить как вдоль дедуктивного течения ($\vdash$), так и вверх по нему, а также в сторону. И каждый раз будут возникать различные по своей доказательной силе и разнообразию фактов версии математики.

Функция выбора позволяет ввести обобщение прямого произведения множеств: $\prod\limits_{i\in I} A_i$ есть множество всех функций выбора для множеств $A_i$, $i \in I$. Например, если $I = \{1, 2, 3\}$, то элементами прямого произведением множеств $A_1, A_2, A_3$ будут последовательности $\langle a_1, a_2, a_3\rangle$, где $a_i \in A_i$, каждую из которых мы считаем сокращенной записью множества самой функции выбора $f = \{\langle 1, a_1\rangle, \langle 2, a_2\rangle, \langle 3, a_3\rangle\}$.

Таким образом функция выбора — это обобщение понятия упорядоченного набора: он может быть какой угодно «длины», которая определяется лишь размерами индексирующего множества, и с компонентами какой угодно природы, которая определяется конкретными множествами $A_i$.

Поэтому конечные упорядоченные наборы принято определять как частный случай функции выбора с конечным множеством индексов, которое обычно представляет собой отрезок натурального ряда (числа фон Неймана). Конечно, сразу возникает вопрос — как быть с упорядоченной парой $\langle a, b\rangle$? Ее мы определяли по Куратовскому, но можно определить и как функцию из множества $\{0, 1\}$. Проблема в том, что само определение функции уже основано на упорядоченной паре, и поэтому выбросить определение по Куратовскому не получится (разве что заменить его на какое-то другое, не связанное с функциями). Так что для упорядоченных пар у нас имеется некая дихотомия в выборе их определения там, где мы хотим их использовать.

Представляется правильным считать, что когда речь идет о каких-то фундаментальных структурах, не подразумевающих мультивалентных отношений или многомерных векторов, об анализе оснований теории множеств, о выразимости каких-то предикатов в теории множеств и т.п., то в этом случае лучше оперировать нативными парами (по Куратовскому) и, более того, конечные наборы порождать как композиции бинарных, полагая, например, $\langle a, b, c\rangle = \langle\langle a, b\rangle, c\rangle$ и т.д.

В более отдаленных от Оснований местах, скажем, в линейной алгебре, топологии, анализе, геометрии и т.д. проще всего использовать однородные упорядоченные наборы, заданные функциями выбора, а в случае конечных наборов вообще не думать о способе их определения, ведь, в конце концов, мы можем обогатить язык теории множеств $n$-арными операторами $\langle\rangle$ и для каждого из них дать соответствующую аксиому упорядоченного набора длины $n$. В этом случае нам не придется думать об их внутренней структуре и об индексирующем множестве, а их существование можно доказать, пользуясь аксиомой подстановки и упорядоченной парой по Куратовскому.

Часто также используется понятие *последовательности*, как функции вида $f : \omega \to A$, которая в таком случае записывается сверточной лексемой $\{f_k\}_{k=0}^{\infty}$. Такой терм легко легализуется в ZF аксиомой

$$a \in \{f_k\}_{k=0}^{\infty} \overset{\text{def}}{\leftrightarrow} \exists k \in \omega : a = f(k),$$

что по сути совпадает с определением множества $\operatorname{ran}(f)$, но чисто графически указывает на его природу. В качестве альтернативы используют также термы вида $(f_i)_{k=0}^{\infty}$ или $\langle f_i\rangle_{k=0}^{\infty}$, которые за счет использования других скобок указывают на «кортежную» суть этой записи и попросту заменяют терм $f$ и его определение как функции натурального числа (без указания множества значений).

В случае конечного индексирующего множества терм $\prod\limits_{i\in I} A_i$ также принято писать более развернуто, например:

$$A \times B \times C, \quad A_1 \times A_2 \times \cdots \times A_n, \quad A^n.$$

Последнее означает, что все $A_i$ равны одному и тому же множеству $A$, а индексирующее множество есть $\{1, 2, \dots, n\}$.

Лексема $A^n$ выводит нас на еще одно распространенное обозначение: $A^B$, которое обозначает множество всех функций из $B$ в $A$. Но на самом деле это частный случай $\prod\limits_{i\in B} A_i$, поскольку если все $A_i$ равны $A$, то функции выбора становятся просто функциями из $B$ в $A$.

Примечательно и другое использование степенной конструкции: $2^A$ часто обозначает то же самое, что $\mathscr{P}(A)$. Имеется в виду, что $2 = \{0, 1\}$ в соответствии с определениями чисел фон Неймана и, следовательно, всякий элемент $f \in 2^A$ есть *индикаторная функция* подмножества $A$. Действительно, каждой функции $f$ соответствует единственное множество $\{x \mid f(x) = 1\}$ и наоборот, для всякого подмножества $B \subseteq A$ можно задать его индикаторную функцию по правилу

$$f(x) = \begin{cases} 1, & x \in B, \\ 0, & x \in A \setminus B. \end{cases}$$

Иначе говоря, множество $2^A$ есть множество индикаторных функций элементов $\mathscr{P}(A)$. Но все-таки это не одно и то же.

Наконец, интересно посмотреть на алгебраические свойства операции $A^B$.

Перечислим без доказательства следующие свойства[8] степени множеств, используя отношение равномощности $\simeq$:

[8] Все они легко следуют из теоремы D4.10, доказанной в Части II.

1. $2^A \simeq \mathscr{P}(A)$;
2. $(A^B)^C \simeq A^{B\times C}$;
3. $A^{B\cup C} \simeq A^B \times A^C$, если $B \cap C = \varnothing$;
4. $(A \times B)^C \simeq A^C \times B^C$;
5. $\varnothing^B = \varnothing$, если $B \neq \varnothing$;
6. $A^\varnothing = \{\varnothing\} = 1$ для любого $A$;
7. $\{a\}^B \simeq \{a\}$ (а также $1^B \simeq 1$);

Мы уделили столь подробный обзор аксиоме выбора по нескольким причинам. Во-первых, это действительно очень значительная аксиома, лежащая в основаниях математики, и если читателю хочется лучше постичь не только язык математики, но самую ее суть, то без аксиомы выбора это понимание будет откровенно неполным. Аксиома выбора в логике и математике играет роль, схожую с пятым постулатом Эвклида в геометрии: она тоже независима от основных аксиом, она тоже долго пряталась от математиков под маской очевидности, без нее или ее альтернатив чистая теория ZF становится такой же бледной и робкой, как и геометрия без какой-либо формы аксиомы о параллельных.

Во-вторых, сама по себе формулировка аксиомы выбора и зависимых от нее принципов является поучительным примером для постижения Lingua Mathematika, для умения конвертировать абстрактные образы в точные формулы, и в конечном счете, для понимания процесса математического мышления.

В-третьих, если мы все-таки смотрим на математику, как на иностранный язык, мы должны не только учить словарь и грамматику, но также вникать в релевантный культурный и идиоматический обвес этого языка. А аксиома выбора представляет собой столь же глубинное явление нашего разума, как универсальная грамматика в лингвистике, подчеркивая самую суть, а иногда и концептуальную хрупкость оснований математики.

В-четвертых, этот раздел имеет вторичную цель донести до широкого круга читателей максимально точное определение аксиомы выбора и ее влияние на математику, чтобы нивелировать имеющиеся в популяризаторских кругах спекуляции на данную тему, а также различного рода неверные интерпретации принципа выбора.

Наконец, в-пятых, отдельно хочется подчеркнуть, что даже при возможности доказать какую-то теорему без использования аксиомы выбора (скажем, теорему Гильберта о нулях), как правило оказывается, что с аксиомой выбора доказательство становится намного короче и проще, т.е. аксиома выбора предоставляет нам еще и некоторый дедуктивный сахар (по аналогии с синтаксическим сахаром), позволяет сложное выразить просто и красиво, а это свойство можно считать проявлением выразительности математического языка.

## C1.3. Универсум фон Неймана

*Джон фон Нейман*

Когда мы обсуждали общую концепцию определения множеств в разделе B2.2, мы представляли себе множество в виде направленного графа, его древовидной развертки или же каталога файловой системы. Такой взгляд хорошо согласуется с реализацией финитарной части теории множеств, а именно — наследственно конечных множеств и их скобочных записей. Но затем мы добавили аксиому бесконечности, в результате чего нам стало доступно множество $\omega$, дерево которого представляет собой корень, из которого идут ребра во все корни деревьев всех натуральных чисел. Иначе говоря, это дерево со счетным ветвлением в корне, у которого каждая собственная ветвь конечна. Более того, каждая следующая ветвь есть соединение всех предыдущих ветвей, поскольку $n+1 = \{0, \dots, n\}$. В то же время такой граф сложно назвать фрактальным, поскольку у него нет бесконечных цепей самоповторения, таких, которые возникают, если отказаться от аксиомы регулярности. В дереве множества $\omega$ все пути конечны!

Таким образом появление бесконечных множеств приводит к тому, что для графического изображения множеств мы вынуждены использовать бесконечное ветвление соответствующих деревьев, но нисходящие по отношению принадлежности пути в таком дереве все равно остаются конечными. При этом надо понимать, что длина этих путей тоже не ограничена, в том же множестве $\omega$ хотя все пути конечны, но мы можем найти путь любой, сколько угодно большой длины.

Эти рассуждения призваны навести нас на мысль, что все множества можно классифицировать по их «глубине», т.е. по той потенциальной возможной длине путей от корня к листьям в дереве-развертке отношения принадлежности.

Такое понятие действительно есть в теории множеств, и оно называется *рангом множества*. Однако для того, чтобы его ввести, сначала потребуется определить шкалу, из который мы эти ранги будем выбирать. Самый простой подход — взять шкалу натуральных чисел, т.е. множество $\omega$. Действительно, раз все пути конечны, то либо существует максимальная длина пути, и ее-то мы назовем рангом множества, либо максимальной длины нет, и тогда ранг множества будет бесконечным.

Однако такой подход хорошо работает лишь для наследственно конечных множеств и бесконечных множеств, элементами которых являются наследственно конечные (например, $\omega$). Но рассмотрим, например, множество $\{\omega\}$. В его графе принадлежности появляется новая вершина, стоящая на 1 шаг выше предыдущего корня. Как при этом изменятся пути в таком графе? Мы попросту получим на единицу более длинные пути, чем имели до этого. Но фокус в том, что если к натуральным числам добавить единицу, они все равно останутся натуральными числами (о чем и говорит нам аксиома бесконечности), т.е. предел длин таких путей не будет отличаться от предела длин путей у множества $\omega$.

В то же время для наследственно конечных множеств конструкция $\{a\}$ явно повышает ранг множества на 1. Почему же в случае одних множеств мы видим разницу в рангах при навешивании скобок, а в случае других — нет? Отсюда возникает потребность в более точной шкале, умеющей различать ранги бесконечных множеств.

Такая шкала есть — это класс ординалов.

Концепция ординала состоит в том, чтобы распространить идею вполне упорядочения с натуральных чисел на все бесконечные множества, или хотя бы на некоторые.

Вполне упорядочение множества подразумевает, что в этом множестве за каждым элементом всегда стоит следующий (если там вообще еще есть какие-то элементы), т.е. последователь. Поэтому, не вдаваясь в теорию упорядоченных множеств, перейдем сразу к основному ее результату: построению эталонных вполне упорядочений, т.е. ординалов.

От ординалов мы хотим выполнения свойства индуктивности с возможностью преодоления предельных точек. Напомним, что индуктивное множество замкнуто относительно операции последователя $S(x) = x \cup \{x\}$. Таково, например, множество $\omega$. Однако само оно не получается как результат этой операции, а является пределом возрастающей цепочки натуральных чисел фон Неймана: $\omega = \bigcup\{n \mid n \in \omega\}$. Получив $\omega$, мы можем продолжить процесс добавления новых точек, используя оператор $S$: $S(\omega)$, $S(S(\omega))$ и т.д. Проделав эти шаги $\omega$ раз, нам снова придется перейти к пределу, чтобы получить множество

$$\omega + \omega = \bigcup\{\omega, S(\omega), S(S(\omega)), \dots\}.$$

На этом мы не останавливаемся и продолжаем снова использовать оператор $S$. *Et cetera ad infinitum*.

Приведенные умозрительные построения, однако, не являются формальными с точки зрения языка ZF. К счастью, у нас есть альтернативный подход, который одним махом даст нам все ординалы.

Итак, скажем, что множество $a$ *транзитивно*, если для него выполнено свойство

$$Tr(a) \overset{\text{def}}{\leftrightarrow} \forall x \in a : \ x \subseteq a.$$

После чего скажем, что множество $a$ есть **ординал**, если оно транзитивно и отношение $\in$ индуцирует на нем вполне упорядочение:

$$\mathrm{Ord}(a) \overset{\text{def}}{\leftrightarrow} Tr(a) \wedge Lin(a, \in) \wedge \forall x \subseteq a : (x \neq \varnothing) \to \exists \min_{\in} x,$$

где $\mathrm{Ord}(a)$ — это предикат, определяющий класс ординалов, который также обозначается Ord. Оказывается, что так определенные ординалы обладают всеми необходимыми нам свойствами.

Прежде чем перейти к формулировкам теорем, обогатим наш язык ZF новыми переменными — греческими буквами, возможно, с добавлением цифровых индексов и акцентов. За этими переменными закрепим свойство быть ординалом, введя в употребление два новых квантора по следующим правилам:

$$\exists\alpha : \varphi(\alpha) \overset{\text{def}}{\leftrightarrow} \exists\alpha \ \ \mathrm{Ord}(\alpha) \wedge \varphi(\alpha), \quad \forall\alpha : \varphi(\alpha) \overset{\text{def}}{\leftrightarrow} \forall\alpha \ \ \mathrm{Ord}(\alpha) \to \varphi(\alpha).$$

Конечно, более правильным было бы дать новые обозначения этим кванторам, например, $\forall^{ord}$ и $\exists^{ord}$, однако в нашем случае их логическая новизна очевидна уже из того, что мы ставим под ними греческие буквы, а также используем двоеточие, как в ограниченных кванторах (каковыми эти кванторы по сути и являются). Кстати, нетрудно проверить, что новые кванторы удовлетворяют аналогичным аксиомам и правилам вывода для кванторов стандартной логики предикатов. Заметим далее, что мы формально считаем все греческие переменные связанными, поскольку нас интересуют теоремы об ординалах, т.е. формулы без свободных переменных. Однако, как и в случае написания аксиом, мы оставляем за собой право снимать с теорем замыкающий универсальный

квантор (как обычный, так и ординальный), оставляя связанную греческую переменную в формуле на месте, где она становится синтаксически свободной, но по соглашению понимается как универсально квантифицированная по ординалам.

Поясним на примере, как это работает. Допустим, мы доказали, что для всех ординалов $\alpha$ выполняется формула $\varphi(\alpha)$. Этот факт можно записать в замкнутом виде так: $\forall\alpha : \varphi(\alpha)$, что по определению раскрывается как $\forall\alpha\ \ \mathrm{Ord}(\alpha) \to \varphi(\alpha)$. Опустить замыкающий квантор мы можем двумя способами: либо просто написать $\varphi(\alpha)$, предполагая при этом посылку $\mathrm{Ord}(\alpha)$, т.к. $\alpha$ — греческая переменная, либо написать явным образом формулу $\mathrm{Ord}(\alpha) \to \varphi(\alpha)$. Естественно, первый способ предпочтительнее, хоть и является синтаксическим сахаром, а не стандартной формулой ZF. Во втором же способе записи мы можем заменить $\alpha$ на $a$, тем самым вернувшись в стандартный язык ZF.

**Теорема C1.3.** *В ZF доказуемы следующие теоремы:*

1° *элемент ординала есть ординал;*

2° *для любых ординалов $\alpha, \beta$: $\alpha \in \beta \leftrightarrow (\alpha \subsetneq \beta)$;*

3° *для любых ординалов $\alpha, \beta$: $\alpha \subseteq \beta$ или $\beta \subseteq \alpha$;*

4° *объединение и пересечение любого множества ординалов есть ординал;*

5° *класс всех ординалов вполне упорядочен отношением $\in$ и является собственно классом;*

6° *для любого ординала $\alpha$: $S(\alpha)$ есть ординал;*

7° *натуральные числа фон Неймана и $\omega$ являются ординалами;*

8° *индукция [$\varphi$]: $[\forall\alpha : (\forall x \in \alpha : \varphi(x, \vec{p})) \to \varphi(\alpha, \vec{p})] \to \forall\alpha : \varphi(\alpha, \vec{p})$;*

9° *рекурсивное определение [$\varphi$]: пусть $\varphi(a, b, \vec{p})$ определяет отображение типа $a \mapsto b$, т.е. $\forall x \exists! y :\ \varphi(x, y, \vec{p})$, тогда для любого ординала $\alpha$ существует функция $f$, определенная на $\alpha$ и такая, что для любого $\beta < \alpha$:*

$$\varphi(f \restriction \beta, f(\beta), \vec{p}). \tag{C1.2}$$

Свойство 5 говорит нам, что принадлежность на ординалах ведет себя так же, как на натуральных числах фон Неймана: во-первых, линейно упорядочивает их, во-вторых, во всяком непустом подклассе класса ординалов существует наименьший элемент. Заметим, что мы здесь говорим о подклассе, т.е. об определяемой части класса всех ординалов, т.е. по сути о произвольном выразимом в ZF свойстве ординалов.

Свойство 2 демонстрирует эквивалентность принадлежности и строгого вложения ординалов как множеств. Это значит, что ординалы образуют цепь вложенных множеств в соответствии с порядком на них. И поскольку принадлежность выполняет роль порядка, обычно вместо $\alpha \in \beta$ пишут $\alpha < \beta$, кроме тех случаев, когда ординал нужно воспринимать как множество, а не как число.

Свойство 4 (учитывая свойства 2 и 3) дает возможность находить минимум и супремум множества ординалов, выполняя базовые операции теории множеств — пересечение и объединение:

$$\min A \overset{\text{def}}{\rightleftharpoons} \bigcap A, \quad \sup A \overset{\text{def}}{\rightleftharpoons} \bigcup A,$$

если $A$ — непустое множество ординалов. Появление min здесь непосредственно связано с тем, что отношение принадлежности на ординалах фундировано.[9]

Здесь мы обзавелись еще одним полезным предикатом $x \subsetneq y$, являющимся сокращением для формулы $(x \subseteq y) \wedge (x \neq y)$. Иногда вместо него используют символ $\subset$, но в источниках он часто понимается и как нестрогое вложение, из-за чего его употребление не желательно.

Ординалы принято разделять на три подкласса: нулевой ординал, последующий ординал (последователь) и предельный ординал. Последователь имеет вид $S(\alpha)$, а к предельным ординалам относят все ординалы, не являющиеся нулем и последующими ординалами. Класс всех последователей обозначается Succ, класс всех предельных ординалов — Lim.

Свойство 8 называется **трансфинитной индукцией** и обобщает полную индукцию (B2.4) из арифметике Пеано. Оно заявляет, что если истинность формулы переходит с элементов ординала на сам ординал, то такая формула истинна тотально на всем классе ординалов.

Последний пункт теоремы дает нам в руки мощный инструмент построения множеств и классов с помощью рекурсии. Эта теорема обобщает арифметическую рекурсию на класс ординалов. Чтобы разобраться в сложной формулировке, добавим в наш язык еще немного синтаксического сахара.

Во-первых, если у нас имеется определяемое $a \mapsto b$ отображение, заданное формулой $\varphi$, то вместо $\varphi(a, b, \vec{p})$ будем писать $b = \Phi_{\vec{p}}(a)$ (ясно, что соответствие между буквами $\varphi$ и $\Phi$ здесь условное, т.к. это мета-теоретические обозначения, и в каждом конкретном случае нужно точно знать, какая формула $\varphi$ была использована). Такая функциональная запись гораздо проще воспринимается. Отображение $\Phi_{\vec{p}}$ при этом принято называть *генератором рекурсии*.[10]

Во-вторых, напомним, что если у нас задана некая функция $f : A \to B$, то через $f \restriction S$ мы обозначаем **ограничение** этой функции на множество $S \subseteq A$, т.е. множество пар $\{\langle x, f(x)\rangle \mid x \in S\}$. Тогда формула (C1.2) может быть записана следующим способом:

$$f(\beta) = \Phi_{\vec{p}}\left(f \restriction \beta\right), \tag{C1.3}$$

т.е. значение $f$ в точке $\beta$ есть значение определяемого формулой $\varphi$ отображения, примененного к ограничению $f$ на $\beta$ (истории значений). Рекурсия здесь состоит ровно в том, что значения функции $f$ на следующих ординалах определяются всеми ее значениями на предыдущих ординалах.

Учитывая принятые сокращения, мы можем весь последний пункт теоремы переписать одной формулой:

$$(\forall x \exists! y :\ \varphi(x, y, \vec{p})) \to \forall \alpha \exists f : \alpha \to \mathfrak{V} :\ \forall \beta < \alpha :\ f(\beta) = \Phi_{\vec{p}}(f \restriction \beta).$$

На самом деле можно показать, что все функции $f$, существование которых здесь утверждается, являются ограничениями одного отображения-класса $F$ с тем же самым свойством $F(\alpha) = \Phi_{\vec{p}}\left(F \restriction \alpha\right)$, и в теории множеств с классами теорема о рекурсивных определениях была бы сформулирована проще:

$$(\Phi_{\vec{p}} : \mathfrak{V} \to \mathfrak{V}) \to \exists F : \mathrm{Ord} \to \mathfrak{V} :\ \forall \alpha : F(\alpha) = \Phi_{\vec{p}}(F \restriction \alpha),$$

[9] Здесь даже аксиома регулярности не нужна, т.к. в определение ординала сразу зашита фундированность.

[10] Это не общепринятое обозначение, но оно кажется мне удачным.

где Ord — класс всех ординалов.

В теории ZF приходится говорить о том, что первопорядковая формула

$$\psi(\alpha, d, \vec{p}) \overset{\text{def}}{\leftrightarrow} \exists f : S(\alpha) \to \mathfrak{V} : \ \forall \beta < S(\alpha) : \ f(\beta) = \Phi_{\vec{p}}(f \restriction \beta) \wedge (d = f(\alpha))$$

задает отображение типа $\alpha \mapsto d$ с таким свойством. За доказательством приведенной теоремы мы, как обычно, отсылаем к Части II (см. теорему D4.6), а теперь примемся ее усердно применять.

Во-первых, отметим, что как правило действие генератора $\Phi_{\vec{p}}$ определяется поразному для всех трех типов ординалов: нуля, последующего и предельного ординала. Так формулы получаются проще и нагляднее. Можно здесь задаться вопросом: а как генератор распознает, на каком ординале он работает? Для этого мы можем модернизировать вычисление функции $F(\alpha)$ так, чтобы ее значениями были не просто множества, а пары вида $\langle y, \alpha\rangle$, т.е. по сути мы вместо нужной нам функции $F(\alpha)$ будем вычислять функцию $G(\alpha) = \langle F(\alpha), \alpha\rangle$, и тогда в образе $G[\alpha]$ будут находиться не только значения $F$ на множестве $\alpha$, но еще и их ординальные номера. В этом случае генератор сможет распознать, с каким ординалом он имеет дело, и в зависимости от этого вернуть правильный ответ. Поэтому типичное рекурсивное определение выглядит так:

$$F(0) = f_0, \quad F(S(\alpha)) = \Phi_{\vec{p}}(F(\alpha)), \quad F(\lambda) = \bigcup\{\Phi_{\vec{p}}(F(\gamma)) \mid \gamma < \lambda\},$$

где $\lambda$ — предельный ординал. Кстати, в таких определениях всегда подразумевается, что $\lambda$ обозначает предельный ординал. И снова мы используем упрощение синтаксиса, типичное для математиков, но не вполне формальное с точки зрения языка ZF. Именно, мы пишем лексему-свертку $\{\Phi_{\vec{p}}(F(\gamma)) \mid \gamma < \lambda\}$ нестандартным образом, помещая на место связанной переменной сразу же то значение, которому она приравнивается в последующей формуле. Сравните:

$$\{\Phi_{\vec{p}}(F(\gamma)) \mid \gamma < \lambda\} \quad \text{vs.} \quad \{x \mid \exists \gamma < \lambda : \ x = \Phi_{\vec{p}}(F(\gamma))\}.$$

Однако на уровне C1 языка математики мы уже должны хорошо уметь считывать подобного рода «переделки» формальной конструкции, понимая, как она трансформируется в исходный язык теории множеств (или любой другой формальной теории).

Как видим, мы здесь ушли от подстановки ограничения $F \restriction \alpha$, заменив его объединением всех точечных значений. Это — *частный*, но очень часто встречающийся вид рекурсивных определений, применяемый в основном к определению монотонных отображений из Ord в Ord. И мы в дальнейшем будем им пользоваться неоднократно.

Предлагаем в качестве упражнения подумать, как такое частное определение формально сводится к (C1.3) с учетом выше описанного трюка с использованием $\langle F(\alpha), \alpha\rangle$.

Во-вторых, определим сложение и умножение на ординалах рекурсивным способом:

$$\begin{aligned} &\alpha + 0 = \alpha, && \alpha \cdot 0 = 0, \\ &\alpha + S(\beta) = S(\alpha + \beta), && \alpha \cdot S(\beta) = \alpha \cdot \beta + \alpha, \\ &\alpha + \lambda = \sup\{\alpha + \gamma \mid \gamma < \lambda\}, && \alpha \cdot \lambda = \sup\{\alpha \cdot \gamma \mid \gamma < \lambda\}, \end{aligned}$$

где $\alpha$ — это параметр рекурсивного определения (не путать его с аргументом функции $f$). А вот как эти определения выглядели бы в формате (C1.3):

$$\alpha + \beta = \alpha \cup \sup\{S(\alpha + \gamma) \mid \gamma < \beta\}, \quad \alpha \cdot \beta = \sup\{(\alpha \cdot \gamma) + \alpha \mid \gamma < \beta\}.$$

Для того, чтобы понять, как первое определение умножения сводится ко второму, нужно во втором определении сначала вместо $\beta$ подставить $S(\gamma)$, сведя таким образом sup к вычислению в единственной максимальной точке $\gamma$, а затем подставить $\lambda$ и понять, что поскольку $(\alpha\cdot\gamma)+\alpha = \alpha\cdot S(\gamma)$ и $S(\gamma) < \lambda$ (в силу предельности $\lambda$), то $\sup\{(\alpha\cdot\gamma)+\alpha \mid \gamma < \lambda\} = \sup\{\alpha\cdot\gamma \mid \gamma < \lambda\}$, т.е. в предельном случае можно избавиться от лишнего слагаемого в свертке. Аналогичные рассуждения применяем к сложению. Кроме того, при $\beta = 0$ множество, для которого мы берем sup, пусто, и поэтому его формальный супремум равен 0, поэтому в случае сложения мы также добавляем в формулу $\alpha$.

Определение арифметических операций с помощью рекурсивного определения, возможно, не вполне отражает их суть, но зато очень удобно для вычислений и отсылает нас к арифметике Пеано, где сложение и умножение задаются таким же рекурсивным способом. Отсюда, кстати, вытекает, что сложение и умножение ординалов на $\omega$ есть в точности сложение и умножение натуральных чисел. Тем самым мы уже практически доказали, что арифметика Пеано моделируется на ординале $\omega$.

Перечислим некоторые свойства арифметики ординалов.

1° $S(\alpha) = \alpha + 1$, $0 + \alpha = \alpha$, $0\cdot\alpha = 0$, $\alpha\cdot 1 = \alpha = 1\cdot\alpha$.

2° Некоммутативность: $\omega + 2 \neq 2 + \omega$, $\omega\cdot 2 \neq 2\cdot\omega$.

3° Правая дистрибутивность нарушается: $(1+1)\cdot\omega = 2\cdot\omega = \omega$. Но $(1\cdot\omega)+(1\cdot\omega) = \omega+\omega$.

4° Ассоциативность: $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$, $(\alpha\cdot\beta)\cdot\gamma = \alpha\cdot(\beta\cdot\gamma)$.

5° Левая дистрибутивность: $\alpha\cdot(\beta+\gamma) = (\alpha\cdot\beta)+(\alpha\cdot\gamma)$.

6° Правая строгая монотонность сложения: $\beta < \gamma \Leftrightarrow \alpha+\beta < \alpha+\gamma$.

7° Правая строгая монотонность умножения: если $\alpha > 0$, то $\beta < \gamma \Leftrightarrow \alpha\cdot\beta < \alpha\cdot\gamma$.

8° Левая нестрогая монотонность: если $\alpha < \beta$, то $\alpha+\gamma \leqslant \beta+\gamma$ и $\alpha\cdot\gamma \leqslant \beta\cdot\gamma$.

9° Отсутствие делителей нуля: если $\alpha\cdot\beta = 0$, то $\alpha = 0$ или $\beta = 0$.

10° Единственность вычитания: если $\beta \leqslant \alpha$, то существует единственный ординал $\gamma$ такой, что $\beta+\gamma = \alpha$.

11° Возможность деления с остатком: для любых $\alpha$ и $\beta > 0$ существует единственная пара ординалов $\gamma, \delta$ таких, что $\alpha = \beta\cdot\gamma+\delta$, где $\delta < \beta$.

Вернемся к заявленной теме об определении ранга множества. Пользуясь рекурсивными определениями, мы можем построить иерархию универсумов $V_\alpha$ фон Неймана по следующим правилам:

$$V_0 = \varnothing, \quad V_{S(\beta)} = \mathscr{P}(V_\beta), \quad V_\lambda = \bigcup\{V_\alpha \mid \alpha < \lambda\}, \tag{C1.4}$$

или, в рамках исходного определения (C1.3) они задаются так:

$$V_\alpha = \bigcup\{\mathscr{P}(V_\beta) \mid \beta < \alpha\}.$$

Далее, несложно показать, что если $\beta < \alpha$, то $V_\beta \subsetneq V_\alpha$, т.е. построенная нами последовательность универсумов строго монотонна по вложению множеств. Действительно, пусть $\beta < \alpha$. Причем можно сразу считать, что $0 < \beta$, т.к. при $\beta = 0$ получаем

$V_0 = \varnothing \subseteq V_\alpha$. При $\beta \neq 0$ множество $V_\beta$ не пусто. Пусть $x \in V_\beta$. Тогда, следуя определению (C1.4), найдется такой $\gamma < \beta$, что $x \in \mathscr{P}(V_\gamma)$. Но тогда, поскольку $\gamma < \alpha$, $x \in V_\alpha$. Это означает, что $V_\beta \subseteq V_\alpha$. Кроме того, так как $\beta < \alpha$, то $\mathscr{P}(V_\beta) \subseteq V_\alpha$ в силу определения (C1.4), откуда следует, что $V_\beta \in V_\alpha$. Откуда, уже в силу аксиомы регулярности получаем, что $V_\beta \neq V_\alpha$.[11]

Попутно мы также доказали свойство универсумов, аналогичное свойству ординалов: $V_\beta \in V_\alpha \leftrightarrow V_\beta \subsetneq V_\alpha$. Действуя в рамках универсальной алгебры, мы бы сказали, что класс ординалов и класс универсумов порядково изоморфны, причем под порядком в обоих случаях подразумевается отношение принадлежности. А заодно мы получили еще одну разновидность транзитивных множеств — универсумы $V_\alpha$ (правда, их элементы уже не всегда транзитивны, так что универсумы, кроме $V_0, V_1$, не являются ординалами).

Ранее мы уже отмечали и теперь повторим, что универсум $V_\omega$ является моделью теории HF наследственно конечных множеств. Именно все его элементы, и только они, представляются конечными скобочными записями. Также стоит отметить, что универсум $V_{\omega+\omega}$ является моделью для теории Цермело Z, причем теория Цермело не способная доказать существование этого универсума так же, как HF не способна доказать существование универсума $V_\omega$. Это обстоятельство подчеркивает, что аксиома подстановки является фундаментально более сильным принципом, чем выделение. Выделение по своей природе «ограничено» — оно создает лишь подмножества уже существующих множеств. Подстановка же позволяет создавать потенциально «новые» множества, элементы которых могут не иметь простой связи (через принадлежность или ранг) с элементами исходного множества.

**Теорема C1.4.** *Всякое множество является элементом и, следовательно, подмножеством некоторого универсума иерархии фон Неймана.*

Доказательство этой теоремы использует понятие транзитивного замыкания множества и носит скорее технический, чем учебный характер, поэтому мы оставим его для Части 2 (см. теорему D4.7).

Для нас эта теорема означает возможность дать следующее определение: **рангом множества** $x$ называется наименьший ординал $\alpha$ такой, что $x \subseteq V_\alpha$.[12] Обозначение: $\operatorname{rank}(x)$.

Ранг множества обладает следующими свойствами.

1° если $a \in b$, то $\operatorname{rank}(a) < \operatorname{rank}(b)$;

2° $\operatorname{rank}(\varnothing) = 0$, $\operatorname{rank}(n) = n$, где $n \in \omega$, $\operatorname{rank}(\omega) = \omega$, и вообще $\operatorname{rank}(\alpha) = \alpha$;

3° $(\operatorname{rank}(A) < \alpha) \leftrightarrow (A \in V_\alpha)$;

4° $\operatorname{rank}(\mathscr{P}(A)) = S(\operatorname{rank}(A))$;

5° если $A \neq \varnothing$, то $\operatorname{rank}(\bigcup A) \leqslant \operatorname{rank}(A)$;

6° $\operatorname{rank}(\{a_1, \ldots, a_n\}) = \max\{\operatorname{rank}(a_1), \ldots, \operatorname{rank}(a_n)\} + 1$.

[11] Последнее можно получить и без аксиомы регулярности, используя теорему Кантора и теорему Кантора-Бернштейна-Шрёдера: действительно, если $\mathscr{P}(V_\beta) \subseteq V_\alpha$, то при предположении $V_\beta = V_\alpha$ мы бы получили по теореме Кантора-Бернштейна-Шрёдера биекцию между $\mathscr{P}(V_\alpha)$ и $V_\alpha$, что невозможно по теореме Кантора.

[12] Мы не используем здесь $x \in V_\alpha$, чтобы рангом пустого множества оказался ноль, а не единица.

Эти свойства делают ранг мощным инструментом для анализа структуры множеств и всей вселенной фон Неймана.

Возвращаясь к представлению множества в виде древовидной развертки отношения принадлежности, о которой мы говорили в разделе B2.2, мы теперь можем указать точное соответствие ранга множества и числовой характеристики такого дерева, именуемой высотой дерева. Действительно, последнее свойство позволяет рекуррентно вычислить ранг наследственно конечного множества, выбирая всякий раз элемент с наибольшим рангом и прибавляя единицу. Стало быть, ранг равен максимальной длине корневого пути в дереве-развертке отношения принадлежности!

Более того, если мы представим ординал $\omega$ в виде такого дерева, то там у каждого элемента $n \in \omega$ высота будет равна $n$, а значит, чтобы вычислить ранг $\omega$, нужно взять супремум $\{n + 1 \mid n \in \omega\}$, который равен $\omega$, что мы и ожидаем от бесконечного дерева. Наконец, если мы перейдем к множеству $\{\omega\}$, то по формуле для вычисления ранга окажется, что $\operatorname{rank}(\{\omega\}) = \omega + 1$, а этот ординал строго больше, чем $\omega$. Тем самым мы закрыли проблемный вопрос о том, как нам перепрыгивать через предельные случаи — когда к дереву $\omega$ прирастает сверху дополнительный хвостик в виде перехода к $\{\omega\}$. Оказывается, нужно действовать поэтапно, по уровням: сначала вычислить ранги элементов множества, а потом переходить к рангу самого множества. Финитная же интуиция подсказывала нам иную схему: считать длины всех корневых путей сразу, невзирая на степень ветвления. И это, как уже отмечалось, приводит к тому, что ранги бесконечных множеств трудно было бы отличить от $\omega$.

Древовидная развертка подсказывает нам также концепцию транзитивного множества: в древовидной развертке транзитивного множества имеются прямые ребра из корня во все без исключения вершины этого дерева. Пользуясь транспортной семантикой, можно было бы сказать, что транзитивность транспортной сети некоторого города означает, что во все пригороды можно добраться прямыми шатлами. Это свойство делает дерево транзитивного множества «плоским» или «стянутым», в теории графов мы бы сказали, что в графе имеется универсальная вершина и что в качестве одного из остовных деревьев нашего графа-множества можно взять граф-звезду.

Отсюда легко понять, как строится транзитивное замыкание множества: нужно все корневые пути продублировать прямыми ребрами (ввести в транспортную сеть шатлы). То, что получится, будет графом транзитивного замыкания.

Кстати, из этой же концепции легко видеть, что в транзитивном множестве $\in$-минимальным элементом всегда будет $\varnothing$ (в рамках аксиомы регулярности, т.е. в теории ZF). Впрочем, это ясно и без графов, ведь если $X$ транзитивно, а $a \in X$ таково, что $X \cap a = \varnothing$, то в силу транзитивности имеем $\varnothing = X \cap a = a$.

С этой точки зрения нельзя по новому не взглянуть и на ординалы. Напомним, что ординал — это транзитивное множество, каждый элемент которого транзитивен. Это значит в нашей транспортной системе есть шатлы не только из центра в пригороды, но также из всех более близких пунктов в более далекие, т.е. в направлении от центра. Иначе говоря, если в дереве-развертке ординала есть путь из вершины $u$ в вершину $v$, то обязательно там есть и ребро $uv$. Граф такого множества называется транзитивно замкнутым. Это значит, что там имеются все такие пути, которые начинаются в корне, заканчиваются в нуле и проходят через любое множество промежуточных по рангу вершин, что позволяет определить количество листьев такого дерева. Так, в дереве-развертке ординала $n$ есть столько листьев, сколько элементов в множестве $\mathscr{P}(\{1, \dots, n-1\})$, т.е. $2^n$. И здесь мы снова замечаем глубокую связь между ординалами и универсумами фон Неймана.

Наличие иерархии фон Неймана с указанными свойствами является ключевым для понимания структуры универсума множеств в аксиоматике ZF. Она показывает, как с помощью ординалов можно ввести строгую меру сложности множеств (ранг) и как весь универсум можно представить в виде иерархии $V_\alpha$, построенной с использованием операций взятия множества подмножеств и объединения на предельных шагах. Концепции трансфинитной индукции и рекурсии, основанные на ординалах, являются важнейшими инструментами для работы в теории множеств. Представление универсума множеств как предела иерархии фон Неймана тесно связано с аксиомой регулярности (фундирования), которая гарантирует, что у каждого непустого множества есть $\in$-минимальный элемент и исключает бесконечные нисходящие цепочки принадлежности, обеспечивая «слоистое» строение универсума.

Концепция ранга, таким образом, не просто технический инструмент, а фундаментальный аспект современного понимания теории множеств. Она отражает идею о том, что универсум множеств строится итеративно и упорядоченно, что позволяет избежать многих парадоксов и обеспечивает прочную основу для математики.

# C1.4. Конструкции

## C1.4.1 Структуры

Коль скоро мы ввели понятие произвольного прямого произведения множеств и произвольного упорядоченного набора, мы можем обобщить понятие отношения. Скажем, что всякое подмножество $R \subseteq A_1 \times \dots \times A_n$ является *$n$-арным отношением*. При этом, если $n = 1$, то $R$ есть просто подмножество $A_1$ (*унарное* отношение), при $n = 2$ $R$ есть *бинарное* отношение, совпадающее с тем, что мы определяли ранее (подмножество $A_1 \times A_2$), а случай $n = 0$ исключаем.

Аналогично, если задана функция $f : A_1 \times \dots \times A_n \to B$, то мы называем ее *$n$-арной функцией* и вместо $f(\langle a_1, \dots, a_n\rangle)$ пишем проще: $f(a_1, \dots, a_n)$. Случай $n = 0$ мы также исключаем для единообразия с отношениями, хотя часто принято считать 0-арные функции константами.

Функция вида $f : A^n \to A$ называется $n$-арной *операцией* на множестве $A$.

Заметим, что $n$-арные отношения, функции и операции существуют независимо от аксиомы выбора, поскольку функция выбора с конечным носителем существует вне зависимости от принятия или отвержения аксиомы выбора: конечный выбор можно осуществить всегда, просто написав формулу с соответствующим количеством кванторов существования. Суть аксиомы выбора именно в том, что она позволяет сделать одномоментный бесконечный выбор, который не может гарантироваться финитными средствами логики предикатов. Не следует противопоставлять аксиому выбора *определяемому* выбору, т.е. такому, когда выбираемые элементы явным образом можно вычислить. Нет, даже в конечном случае предоставляемый логикой предикатов выбор не обязан быть конкретным. Аксиома выбора — это что-то вроде способа заявить бесконечно много кванторов существования подряд, не прибегая к формулам бесконечной длины.

Наконец, мы походим к центральному месту понятийного аппарата математики. Упорядоченный набор $\mathscr{M} = \langle M, \mathscr{R}, \mathscr{F}, \mathscr{C}\rangle$, где $M$ — произвольное *непустое* множество, $\mathscr{R}$ — множество отношений (произвольной арности) на $M$, $\mathscr{F}$ — множество операций

(произвольной арности) на $M$, $\mathscr{C}$ — подмножество $M$, именуемое множеством констант, называется **структурой**, при этом множество $M$ называется **носителем** этой структуры.

Стоит отметить, что в литературе имеются расхождения в терминологии структур. Если мы находимся в основаниях математики, логике или теории моделей, то как правило такую структуру $\mathscr{M}$ называют **моделью**, при этом она может вовсе не содержать операций (структура без операций называется *реляционной структурой*). Однако в учебниках по алгебре и другим дисциплинам термин «алгебраическая структура» применяется лишь к структурам с непустым множеством операций и единственным отношением — равенством. Хотя часто (например, в универсальной алгебре) алгебраические структуры дополняются отношением порядка, и в таком случае называются упорядоченными алгебраическими структурами. Мы будем использовать лаконичный термин *структура* в общем случае, иногда (при отсутствии в ней отношений, кроме равенства, или при наличии одного отношения порядка) называя их алгебраическими.

**Замечание**: любую операцию $f : A^n \to A$ можно рассматривать как $n+1$-арное отношение, поскольку между упорядоченными наборами $\langle\langle a_1, \dots, a_n\rangle, b\rangle$ и $\langle a_1, \dots, a_n, b\rangle$ имеется естественное соответствие, да и в целом любая функция по определению есть отношение. Так что можно сказать, что на самом деле все структуры реляционные. Однако явное выделение в множестве отношений, операций и констант помогает лучше понять устройство структуры, а также моделировать термы формального языка, что является критически важным фактором для концептуальной ясности и удобства построения и интерпретации формальных теорий. Ирония сведения операций к отношениям состоит в том, что сами отношения есть по определению множества функций (выбора), что лишний раз подчеркивает отсутствие статуса первичности у этих понятий.

В основаниях математики структуры используются для того, чтобы построить модель формальной математической теории, сведя тем самым ее непротиворечивость к непротиворечивости ZF, в которую мы безоговорочно верим, поскольку интуитивная ясность и конструктивность как теории HF, так и ее скобочной модели дают уверенность в самом теоретико-множественном подходе, который обобщается в ZF. В теории ZF мы можем легко построить модели HF и теории Цермело (без аксиомы подстановки), пользуясь универсумами $V_\omega$ и $V_{\omega+\omega}$, но такое обоснование непротиворечивости теорий больше похоже на уловку, поскольку ссылается на непротиворечивость более сильной обобщающей их теории.

Поэтому мы будем считать наши рассуждения со скобочными записями множеств достаточно убедительными для того, чтобы считать теорию наследственно конечных множеств непротиворечивой. Более того, и скобочная модель наследственно конечных множеств, и все рассмотренные нами грамматики формальных языков в конечном алфавите представляют собой регулярно устроенные *бесконечные* множества *конечных* строк, сами по себе являющиеся свидетелями возможной выполнимости аксиомы бесконечности. Что дает нам право с чисто философской позиции считать аксиоматику ZF надежным способом формализации общематематической теории множеств, подразумевающейся повсюду в математике как данность.

Таким образом мы выстраиваем фундамент математики из двух опор: формальная теория множеств и логика предикатов. Каждая из этих теорий опирается на вторую, позволяя удерживаться «в вакууме» всей системе математических построений примерно так же, как Земля и Луна удерживаются в пространстве вместе. Логика дает язык и правила вывода для формулировки и доказательства теорем в теории множеств, а теория множеств дает семантику (модели) для интерпретации логических формул.

Чтобы не повторяться, мы не будем здесь воспроизводить упоминавшиеся ранее в

разделе B1.2.6 примеры моделей различных теорий, оставляя это в качестве упражнения читателю. Отличие ранее построенных моделей от «настоящих» теоретико-множественных структур состоит лишь в том, что в качестве базового множества мы теперь должны выбирать конкретные определяемые в ZF множества (а не коробки с карандашами).

Вместо этого мы дадим некий общий методологический подход к построению различных структур в рамках ZF (ZFC) и построим несколько конкретных примеров моделей числовых структур.

## C1.4.2 Принципы структуростроения

Итак, для начала заметим, что любой мало-мальски значимый объект в математике имеет признаки структуры, т.е. этот объект строится на каком-то базовом множестве путем определения на нем отношений и операций. Часто это строительство (как и вообще любое строительство) выходит, так сказать, за рамки бюджета — начинает использовать элементы не только исходного множества-носителя, но и некоторые дополнительные конструкции. Конечно же, есть методы, позволяющие довольно-таки хитрым образом превратить внеструктурные построения в структурные, некоторым образом расширив базовое множество, и такие, достаточно яркие примеры мы вскоре увидим. Однако в целом вся идеология вертится вокруг правильно подобранного носителя и заданных на нем отношений и операций.

Какими способами мы умеем строить множества? У нас для этого не такой уж большой арсенал средств, которые можно разделить на два класса: повышающие ранг и не повышающие ранг. В таблице C1.2 мы привели несколько элементарных операций с разбивкой их по этим двум классам.

Таблица C1.2. Операции и их отношение к рангам множеств

| Повышение ранга | неповышение ранга |
|---|---|
| $\{a\}, \{a, b\}, \ldots$ | $\cup, \cap, \setminus, \triangle$ |
| $\langle a, b\rangle, A \times B$ | выбор |
| $\mathscr{P}(A)$ | $\bigcup A$ |
| подстановка | выделение |

Заметим, что такие операции, как образование пары, упорядоченной пары (по Куратовскому), прямое произведение множеств, хоть и повышают ранг, но незначительно — на 1–2 шага. И только аксиома подстановки позволяет стремительно увеличить ранг, поскольку позволяет перейти от множества с небольшим рангом к множеству с каким угодно рангом. Как уже отмечалось, например, построение отображения $n \mapsto \omega + n$ уже пробрасывает нас из области конечных рангов в бесконечные. Но определяемые отображения, использованные в качестве генератора трансфинитной рекурсии позволяют прыгать очень высоко по ординальной шкале. Например, нумерация алефов $\aleph_\alpha$ — это нумерация бесконечных мощностей (кардиналов) с помощью ординалов. Так, $\aleph_0$ — это первый бесконечный кардинал, т.е. $\omega$, а $\aleph_1$ — это первый несчетный кардинал. Существует также нумерация $\beth_\alpha$, которая на каждом шаге переходит от мощности $\beth_\alpha$

к мощности множества $\mathscr{P}(\beth_\alpha)$. Последовательность $\beth$ растет быстрее, чем $\aleph$, если мы отвергаем обобщенную континуум-гипотезу. Существуют и другие, куда более быстрые трансфинитные последовательности.

С другой стороны, понижение ранга у нас обычно не столь стремительно. Стандартные операции либо вовсе не меняют ранг (как объединение множеств), либо могут снижать его (как пересечение множеств), но лишь до рангов тех множеств, которые уже являлись элементами изначальных. Впрочем, аксиома регулярности, например, умеет уронить ранг сразу до нуля, выбрав правильный элемент для пересечения. Аксиома выделения очевидным образом тоже не повышает ранг, действуя по аналогии с пересечением множеств. Справедливости ради нужно отметить, что аксиома подстановки может снижать ранг как угодно, так что ее можно рассматривать как «мага вне категорий» или шахматного ферзя, который ходит как угодно.

Под выбором мы здесь понимаем прямое использование аксиомы выбора, которая из исходного множества $A$ создает некоторое специальное подмножество в $\bigcup A$, область значений функции выбора. Конечно, можно сказать, что тут речь идет о функции, а значит, о повышении ранга, но на аксиому выбора можно еще смотреть как на способ выбрать так называемое *сечение* семейства множеств.

Если имеется семейство непустых множеств $\{A_i \mid i \in I\}$, то сечением этого семейства называется такое множество $\{s_i \mid i \in I\}$, что $s_i \in A_i$ для всех $i \in I$. Строго говоря, у нас была одна функция $A(i)$, определенная на $I$, а стала другая функция $s(i)$, определенная на $I$, и если сравнивать ранги этих функций, то у второй ранг будет не выше, а может даже и ниже, чем у первой.

Зная элементарные, т.е. заданные аксиомами инструменты построения множеств, мы можем использовать их комбинации для создания уже довольно сложных структур.

Предположим, у нас уже как-то определено базовое множество $M$. Чтобы задать на нем какое-то отношение $R \subseteq M^n$, мы сначала идем на повышение ранга, создавая прямое произведение $M^n$ (либо как комбинацию бинарных прямых произведений, либо через функции выбора), а затем вырезаем из полученного множества некоторое подмножество, не увеличивая ранг. Происходит двухтактовый цикл: повысить–понизить. Причем если отношение $R$ не будет тотальным, а будет охватывать лишь часть множества $M$, то ранг $R$ может провалиться ниже ранга $M$.

Аналогичное действо у нас происходит и при определении операций, которые, как уже отмечалось, по сути есть тоже отношения на $M$. Правда, операции всегда тотально определены, поэтому их ранг ниже, чем $\mathrm{rank}(M) + 2$ не свалится (двойка — за счет конструкции упорядоченной пары).

Кроме того, в структуре может быть потребность в унарных отношениях, т.е. подмножествах $M$. Здесь можно говорить либо о прямом применении аксиомы выделения (не повышаем ранг), либо мы можем сначала создать булеан $\mathscr{P}(M)$, повысив ранг, а затем вырезать из булеана некоторую часть, не повышая его ранг. Так обычно задаются топология,[13] алгебра множеств, фильтр,[14] фактор-множество и другие системы подмножеств множества $M$.

Почему для логика важно следить за описанным блужданием по шкале рангов при строительстве тех или иных структур? Дело в том, что это позволяет нам отследить,

[13] Общее понятие топологического пространства было введено Феликсом Хаусдорфом в его книге «Основы теории множеств» (1914), что позволило унифицировать изучение непрерывности и предельных переходов в самых разных математических контекстах.

[14] Понятие фильтра было введено Анри Картаном в 1937 году как обобщение понятия предела последовательности, что оказалось очень плодотворным в общей топологии и других областях анализа.

насколько мощные универсумы фон Неймана требуются при строительстве этих структур, а значит, и косвенно оценить сложность модели теории множеств, в которой мы эти структуры определяем. Сложность модели, в свою очередь, указывает на тот аксиоматический аппарат, который может потребоваться для реализации соответствующих структур.

Отметим, что пока мы хорошо вписываемся в данное выше определение структуры, поскольку не уходим далеко от исходного множества $M$.

Но давайте теперь посмотрим, что нам может дать применение аксиомы подстановки. На самом деле большинство математических структур без нее создать крайне сложно! И вот первый пример — метрическое пространство. Как известно, это — множество с заданной на нем метрикой. Но метрика есть функция $d : M^2 \to \mathbb{R}$, т.е. ее область значений находится за пределами любых степеней множества $M$ и, вообще говоря, никак с ним не связана. Иначе говоря, метрика не является операцией на $M$.

Как же быть? Во-первых, аксиома подстановки позволяет создать такую функцию, если есть правило сопоставления пары элементов $M$ действительному числу. Во-вторых, можно применить читерский прием, позволяющий запихнуть метрику в определение структуры, а именно: нужно в качестве носителя структуры рассмотреть множество $M \cup \mathbb{R}$, и тогда метрика будет законной операцией в такой структуре (правда ее придется хитрым образом доопределить на все это множество, но это уже техника).

Второй, еще более изощренный способ вписаться в каноническое определение структуры — это добавить огромное количество отдельных симметричных отношений $R_\alpha$ на $M$, состоящих из всех пар элементов $M$, расстояние между которыми равно $\alpha$, где $\alpha \in \mathbb{R}$. Нам ведь никто не запрещал в определении структуры индексировать отношения и операции какими-то внешними множествами. Таким образом, для каждого возможного расстояния между точками $M$ у нас будет определено свое собственное бинарное отношение на $M$, и формально мы впишемся в определение структуры.

Примерно такой же прием можно использовать, когда мы хотим вписать в определение структуры понятие «модуль над кольцом». Напомним, что модуль над кольцом — это по сути две структуры, связанные некоторым тесным образом. Первая — это алгебраическое кольцо $R$ (скаляры), вторая — множество $M$ (векторов), которое само по себе является абелевой группой (т.е. задана коммутативная операция сложения векторов, взятия противоположного вектора и константа 0). А между этими структурами работает операция умножения вектора на скаляр (или скаляра на вектор, если это левый модуль) $P : M \times R \to M$. И снова мы видим, что операция выпадает сразу из обеих порождающих структур. Поэтому, считая каждый скаляр параметром, можно вместо одной операции $P$ рассмотреть множество операций $P_\lambda : M \to M$, тем самым вписав исходную операцию в определение структуры.

Конечно, такие приемы не делают чести теории множеств, они лишь подчеркивают, что при желании под термином «структура» можно подразумевать достаточно простую вещь — что-то, что порождено базовым множеством с привлечением каких-то внешних параметризующих множеств или переменных. Это позволяет упрощать формально-логический анализ математики, избегая того действительно огромного разнообразия математических объектов, которые присутствуют во всей математике.

Поэтому, хотя Гильберт и уверял нас, что теория множеств — это рай, созданный Кантором, откуда нас никто не выгонит, но этот рай имеет кучу темных подвалов в виде сложностей, связанных с простотой языка и, как следствие, огромной сложностью формул, выражающих довольно простые математические факты, а также с тем, что мно-

гие интуитивно тождественные вещи в рамках ZF оказываются совершенно по-разному устроенными, подчас даже слишком изобретательно.

Но с другой стороны, цель формальной теории множеств скорее в том, чтобы обосновать математику, привести все ее теории к общему логическому базису, «приземлить» на логику первого порядка, а не в том, чтобы все великое разнообразие математических наук погрузить в единый формальный язык. Здесь прослеживается аналогия с языками программирования: в мире их существует огромное количество, адаптированных под разные нужды пользователей — от внутренних языков микросхем до универсальных языков высокого уровня вроде Pythonили Rust, но всех их можно приземлить на Ассемблер или непосредственно в машинный код.

Поэтому математика — это скорее множество формальных теорий, чем множество структур в рамках одной теории ZF. Но умение строить модели для этих теорий в рамках теории множеств является категорически необходимым умением для каждого математика.

Итак, как видим, аксиома подстановки позволяет нам уходить довольно далеко от носителя структуры $M$, привлекая разные вспомогательные множества типа $\mathbb{R}$ или абстрактных колец. Поэтому и модели теории множеств с аксиомой подстановки — это огромные с точки зрения иерархии фон Неймана модели, их ранг измеряется специальными кардинальными числами, превосходящими все разумные конструктивные ординалы.

С другой стороны, если мы заранее знаем, как устроена та или иная вспомогательная структура, то у нас нет нужды в использовании аксиомы подстановки на полную ее мощность: достаточно пользоваться ее следствием — аксиомой выделения, поскольку функцию вида $P : M \times R \to M$ можно определить как часть множества $(M \times R) \times M$, и повышение ранга здесь будет вполне предсказуемым и небольшим. Это значит, что когда мы строим сложные математические структуры поэтапно, отправляясь от, например, вещественных чисел, то мы в принципе можем вполне обходиться теорией Цермело Z, которая полностью моделируется на универсуме $V_{\omega+\omega}$, который уже не представляется нам чем-то архисложным и невообразимым. Вопрос лишь в том, как туда «приземлить» базовые математические структуры, такие как поле вещественных чисел.

### C1.4.3 Конкретный разговор о моделях

Наконец, чтобы закрепить описанное выше умение строить различные структуры, построим несколько конкретных примеров.

Для начала заметим, что структура $\mathbb{N} = \langle \omega, \varnothing, +, \cdot, S \rangle$, т.е. первый бесконечный ординал $\omega$ в качестве носителя и ординальные операции сложения и умножения, а также операция $S$ и константа $\varnothing$, является моделью арифметики Пеано, которую мы рассматривали в разделе B2.1.

Здесь в плане строительства самой структуры нет ничего экстраординарного, все бремя сложности построения перенесено на определение ординалов и операций на них.

Далее стоит отметить упоминавшуюся ранее модель $V_\omega$ наследственно конечных множеств. По сути в этой модели есть только предикаты принадлежности и равенства, причем они играют роль самих себя. Несложно проверить, что все аксиомы HF здесь выполняются, если переменные теории ограничить универсумом $V_\omega$.

Универсум $V_{\omega+\omega}$ представляет собой модель теории Z. Как мы помним, он должна включать аксиому бесконечности, т.е. содержать ординал $\omega$, откуда следует, что модель

также должна включать все множества, которые получаются из $\omega$ разрешенными аксиоматикой операциями, а это — все операции из таблицы C1.2, кроме той, что реализует аксиома подстановки, т.к. ее нет в системе Z. Но все такие операции дают лишь конечное повышение ранга, а значит, все множества будут иметь ранг либо $n$, либо $\omega + n$, где $n \in \omega$.

*Модель Куайна* представляет собой особый случай модели. Это — рефлексивное отношение на синглетоне. Возьмем произвольное множество $s$ и положим $M = \{s\}$, а затем зададим на нем отношение $\varepsilon = \{\langle s, s\rangle\}$. Такая структура $\langle M, \varepsilon\rangle$ является моделью очень специального куска теории множеств без аксиом регулярности, бесконечности, пустого множества и выделения (см. таб. C1.1), где отношение-петля $\varepsilon$ моделирует нефундированное отношение принадлежности: $(s\,\varepsilon\,s)$. В такой модели равенство интерпретируется как равенство, выполняется конгруэнтность и экстенсиональность в виду того, что там есть только один элемент, работает аксиома пары, т.к. там можно построить единственную пару $\{s, s\}$, которая равна $s$, работает аксиома степени ($\mathscr{P}(s) = \{s\} = s$), объединения ($\bigcup s = s$), работает аксиома подстановки, поскольку любое определяемое отображение будет задавать соответствие $s \mapsto s$, а также аксиома выбора, т.к. тут нечего выбирать, кроме $s$.

Модель Куайна иллюстрирует, что аксиома выделения без аксиомы пустого множества не может быть выведена из аксиомы подстановки.

Рассмотрим теперь модель $V_\omega \setminus \{\varnothing\}$, в которой принадлежность и равенство моделируют сами себя. Такая модель будет удовлетворять только следующим аксиомам: конгруэнтность, экстенсиональность, пара, степень, объединение, регулярность, подстановка, выбора, а также отрицание аксиомы бесконечности. Здесь мы снова видим отсутствие пустого множества и, как следствие, аксиомы выделения. Но при наличии аксиомы регулярности.

Выстраивая таким или похожим способом достаточно простые модели разных наборов аксиом теории множеств, мы можем показывать их независимость друг от друга или, наоборот, подчеркивать некоторые (частичные) зависимости.

Построим теперь модель вещественных чисел. Точнее, мы построим модель теории RCF вещественно замкнутых (упорядоченных) полей, которая окажется одновременно и моделью второпорядковой теории действительных чисел. RCF задается в сигнатуре $\langle =, \leqslant, +, \cdot, 0, 1\rangle$ и имеет следующую аксиоматику:

RCF1 аксиомы линейного порядка для $\leqslant$;

RCF2 стандартные аксиомы поля;

RCF3 согласованность порядка с операциями:

$$(a \leqslant b) \to (a + c \leqslant b + c), \quad (0 \leqslant a) \wedge (0 \leqslant b) \to (0 \leqslant ab);$$

RCF4 $\forall y\ (0 \leqslant y) \to \exists x\ (x \cdot x = y)$;

RCF5 $\forall q_1, \ldots, q_n\ \exists x\ (x^n + q_1 \cdot x^{n-1} + \cdots + q_n = 0)$, где $x^n$ записывается как $(n-1)$-кратная композиция умножения, а число $n$ — нечетное.

Последняя аксиома — это схема аксиом, поскольку для каждого $n$ нам нужно написать свою отдельную формулу с $n$ переменными. Аксиома RCF4 утверждает, что любое положительное число есть квадрат какого-то числа.

Про теорию RCF известно, что она полна (любое предложение языка RCF либо доказуемо, либо опровержимо в рамках перечисленных аксиом) и разрешима (существует

алгоритм, определяющий истинность любого утверждения). Это знаменитый результат А. Тарского. Поле вещественных чисел является стандартной, но не единственной моделью данной теории.

Для того, чтобы построить модель RCF, сначала мы построим стандартную модель целых чисел $\mathbb{Z}$. Здесь существует несколько подходов, мы выберем наиболее экономный. Носителем $\mathbb{Z}$ мы объявим множество $Z = \omega \times \{0\} \cup \{0\} \times \omega$. Визуально это два экземпляра ординала $\omega$, склеенные общим нулем (пара $\langle 0,0\rangle$). Отрицательными числами мы будем считать пары вида $\langle n, 0\rangle$, положительными — $\langle 0, n\rangle$. Для целых чисел нужно задать порядок и операции.

Порядок: $\langle a_1, a_2\rangle \leqslant_{\mathbb{Z}} \langle b_1, b_2\rangle$, если $a_2 = b_1 = 0$ или $(a_1 = b_1 = 0) \wedge (a_2 \subseteq b_2)$ или $(a_2 = b_2 = 0) \wedge (b_1 \subseteq a_1)$, т.е. сравнение на правом экземпляре $\omega$ производится стандартным образом, а на левом — противоположным.

Сложение:

$$\langle a_1, a_2\rangle +_{\mathbb{Z}} \langle b_1, b_2\rangle = \begin{cases} \langle a_1 +_\omega b_1, a_2 +_\omega b_2\rangle, & (a_1 = b_1 = 0) \vee (a_2 = b_2 = 0), \\ \langle a_1 \dot{-} b_2, 0\rangle & (a_2 = b_1 = 0) \wedge (b_2 \subseteq a_1), \\ \langle 0, b_2 \dot{-} a_1\rangle & (a_2 = b_1 = 0) \wedge (a_1 \subseteq b_2), \\ \langle b_1 \dot{-} a_2, 0\rangle & (a_1 = b_2 = 0) \wedge (a_2 \subseteq b_1), \\ \langle 0, a_2 \dot{-} b_1\rangle & (a_1 = b_2 = 0) \wedge (b_1 \subseteq a_2). \end{cases}$$

Здесь смысл в том, чтобы понять, разные ли это по знаку числа (если нет, то мы просто их покоординатно складываем) и как быть в случае разных знаков, потому что при сложении чисел с разными знаками нужно понять, какое из них больше по модулю, найти разность и поставить правильный знак этой разности. Кстати, операция вычитания на натуральных числах (*монус*) определяется так: $a \dot{-} b$ равно их разности, если $a \geqslant b$, и 0 в противном случае (см. раздел D3.3).

Умножение:

$$\langle a_1, a_2\rangle \cdot_{\mathbb{Z}} \langle b_1, b_2\rangle = \begin{cases} \langle 0, (a_1 +_\omega a_2) \cdot_\omega (b_1 +_\omega b_2)\rangle, & (a_1 = b_1 = 0) \vee (a_2 = b_2 = 0), \\ \langle (a_1 +_\omega a_2) \cdot_\omega (b_1 +_\omega b_2), 0\rangle, & \text{иначе.} \end{cases}$$

Здесь проще, т.к. в случае одинакового знака при умножении получается неотрицательное число, а в случае разных знаков — неположительное.

Нулем в $Z$ будет $0_{\mathbb{Z}} = \langle 0,0\rangle$, единицей: $1_{\mathbb{Z}} = \langle 0,1\rangle$.

Можно проверить, что определенные таким образом отношение $\leqslant_{\mathbb{Z}}$, операции $+_{\mathbb{Z}}, \cdot_{\mathbb{Z}}$ и константы $0_{\mathbb{Z}}, 1_{\mathbb{Z}}$ удовлетворяют аксиомам упорядоченного дискретного коммутативного кольца с единицей, моделью которого и является структура $\mathbb{Z} \overset{\text{def}}{\rightleftharpoons} \langle Z, =, \leqslant_{\mathbb{Z}}, +_{\mathbb{Z}}, \cdot_{\mathbb{Z}}, 0_{\mathbb{Z}}, 1_{\mathbb{Z}}\rangle$.

Далее можно идти разными путями. Например, мы можем вспомнить, что действительное число есть сумма целого числа и дробной части, которую можно выразить счетной двоичной последовательностью. Носитель такой модели легко строится, но в ней очень сложно определить операции сложения и умножения. Поэтому мы пойдем другим путем, более классическим, определив сначала множество рациональных чисел как классы эквивалентных дробей.

Пусть $Q = \{\langle p, q\rangle \mid (p, q \in Z) \wedge (q > 0)\}$. На элементах $Q$ введем отношение эквивалентности:

$$\langle p_1, q_1\rangle \sim \langle p_2, q_2\rangle \overset{\text{def}}{\leftrightarrow} p_1 \cdot_{\mathbb{Z}} q_2 = p_2 \cdot_{\mathbb{Z}} q_1.$$

Неформально: $\frac{p_1}{q_1} \sim \frac{p_2}{q_2}$, если и только если $p_1 q_2 = p_2 q_1$. Нетрудно проверить, что $\sim$ действительно есть отношение эквивалентности на $Q$. Это значит, что $Q$ можно разбить на непересекающиеся классы эквивалентности вида

$$[\langle p, q\rangle]_\sim = \{\langle x, y\rangle \mid \langle p, q\rangle \sim \langle x, y\rangle\}.$$

Теперь мы факторизуем множество $Q$ по отношению $\sim$, т.е. рассмотрим фактор-множество $Q' = Q/_\sim = \{[x]_\sim \mid x \in Q\}$. Факторизация — еще один пример повышения ранга множеств, который комбинирует в себе два элементарных шага: взятие булеана и выделение из него подмножества.[15]

Каждый класс эквивалентности теперь представляет собой то, что в школе мы называли дробью или рациональным числом. Мы могли бы отказаться о классов эквивалентности и работать только с несократимыми парами чисел $\langle p, q\rangle$, т.е. в определение $Q$ сразу зашить ограничительный предикат, выражающий взаимную простоту чисел $p$ и $q$. Но такой путь ведет к усложнению определения операций.

Далее мы будем опускать тильду в обозначении классов эквивалентности. Разобравшись с носителем, определим теперь отношение порядка, константы и операции на элементах $Q'$.

Порядок: $[\langle p, q\rangle] \leqslant_\mathbb{Q} [\langle p', q'\rangle]$, если $p \cdot_\mathbb{Z} q' \leqslant_\mathbb{Z} p' \cdot_\mathbb{Z} q$ (обычное правило сравнения дробей). Правда, здесь есть тонкий момент: мы определяем предикат на классах эквивалентности через их представителей, но будет ли то же самое верно для других представителей этих классов (корректность определения)? Это нужно всегда проверять, и в данном случае это несложно сделать. Пусть $\langle p, q\rangle \sim \langle a, b\rangle$ и $\langle p', q'\rangle \sim \langle a', b'\rangle$, будет ли тогда верно условие $a \cdot_\mathbb{Z} b' \leqslant_\mathbb{Z} a' \cdot_\mathbb{Z} b$?

Умножим неравенство $p \cdot_\mathbb{Z} q' \leqslant_\mathbb{Z} p' \cdot_\mathbb{Z} q$ на $b \cdot_\mathbb{Z} b'$ (знак не изменится, т.к. это положительные знаменатели): $p \cdot_\mathbb{Z} q' \cdot_\mathbb{Z} b \cdot_\mathbb{Z} b' \leqslant_\mathbb{Z} p' \cdot_\mathbb{Z} q \cdot_\mathbb{Z} b \cdot_\mathbb{Z} b'$. Из определения эквивалентности пар извлекаем, что $p \cdot_\mathbb{Z} b = a \cdot_\mathbb{Z} q$ и $p' \cdot_\mathbb{Z} b' = a' \cdot_\mathbb{Z} q'$, откуда, пользуясь конгруэнтностью равенства, приходим к $a \cdot_\mathbb{Z} q \cdot_\mathbb{Z} q' \cdot_\mathbb{Z} b' \leqslant_\mathbb{Z} a' \cdot_\mathbb{Z} q' \cdot_\mathbb{Z} q \cdot_\mathbb{Z} b$, после чего сокращением на положительное $q \cdot_\mathbb{Z} q'$ получаем требуемое неравенство. Безусловно нам здесь помогает весь алгебраический арсенал коммутативного кольца $\mathbb{Z}$.

Сложение: $[\langle p, q\rangle] +_\mathbb{Q} [\langle p', q'\rangle] = [\langle p \cdot_Z q' +_\mathbb{Z} p' \cdot_\mathbb{Z} q, q \cdot_\mathbb{Z} q'\rangle]$. Здесь использование классов эквивалентности облегчает определение, т.к. нам не нужно заботиться о несократимости дроби. Но корректность определения, разумеется, тоже следует проверить.

Умножение: $[\langle p, q\rangle] \cdot_\mathbb{Q} [\langle p', q'\rangle] = [\langle p \cdot_Z p', q \cdot_\mathbb{Z} q'\rangle]$.

Константы: $0_\mathbb{Q} = [\langle 0_\mathbb{Z}, 1_\mathbb{Z}\rangle]$, $1_\mathbb{Q} = [\langle 1_\mathbb{Z}, 1_\mathbb{Z}\rangle]$.

Таким образом у нас определена структура $\mathbb{Q} \overset{\text{def}}{=\!=} \langle Q', =, \leqslant_\mathbb{Q}, +_\mathbb{Q}, \cdot_\mathbb{Q}, 0_\mathbb{Q}, 1_\mathbb{Q}\rangle$, которая представляет собой стандартную модель поля рациональных чисел или, как сказал бы алгебраист, упорядоченное поле частных кольца $\mathbb{Z}$.

Наконец, можем перейти к построению структуры $\mathbb{R}$, которая будет моделью поля действительных чисел. Здесь также есть несколько эквивалентных подходов, но мы выберем самый простой с точки зрения определения операций. Рассмотрим множество $(Q')^\omega$ всех функций из $\omega$ в $Q'$. Это — последовательности рациональных чисел, которые мы по традиции будем записывать как $\langle x_n\rangle$. Скажем, что последовательность $\langle x_n\rangle$

[15] Построение фактор-структур (фактор-групп, фактор-колец) через классы эквивалентности — мощный метод абстрактной алгебры, во многом обязанный работам Эмми Нётер и её школы в 1920-х годах, которые систематизировали и обобщили эти конструкции.

**фундаментальная**,[16] если

$$\forall \varepsilon >_{\mathbb{Q}} 0_{\mathbb{Q}} : \exists N \in \omega : \forall n, m > N : |x_n - x_m| <_{\mathbb{Q}} \varepsilon.$$

Здесь мы уже выходим на привычный нам с детства язык математического анализа. Приведенная формула означает, что для достаточно больших номеров члены последовательности становятся сколь угодно близкими (число $\varepsilon$ берется из $Q'$, т.к. ничего другого у нас нет). Мы не приводим определение функций разности и модуля рациональных чисел, считая это упражнение тривиальным.

Далее мы определим множество

$$F \overset{\text{def}}{\rightleftharpoons} \{x \mid x \in (Q')^\omega \wedge x \text{ фундаментальна}\}$$

всех фундаментальных последовательностей. Наконец, на этом множестве введем отношение эквивалентности:

$$\langle x_n \rangle \approx \langle y_n \rangle \overset{\text{def}}{\leftrightarrow} \forall \varepsilon >_{\mathbb{Q}} 0_{\mathbb{Q}} : \exists N \in \omega : \forall n > N : |x_n - y_n| <_{\mathbb{Q}} \varepsilon,$$

т.е. мы отождествляем последовательности, разность между которыми стремится к нулю. Класс эквивалентности $[\langle x_n \rangle]_\approx$ по данному отношению и будет моделью вещественного числа. Положим

$$R \overset{\text{def}}{\rightleftharpoons} F/_\approx.$$

Осталось задать константы, порядок и операции.

$$0_{\mathbb{R}} \overset{\text{def}}{\rightleftharpoons} [\langle x_n = 0_{\mathbb{Q}} \rangle], \quad 1_{\mathbb{R}} \overset{\text{def}}{\rightleftharpoons} [\langle x_n = 1_{\mathbb{Q}} \rangle],$$

где $\langle x_n = r \rangle$ означает функцию-константу со значением $r \in Q'$. На самом деле все рациональные числа таким способом отображаются в $R$. Для иррациональных чисел уже потребуются более хитрые последовательности. Например, если мы хотим определить $\sqrt{2}$, то возьмем рекурсивно определяемую последовательность $\langle x_n \rangle$ такую, что

$$x_0 = 1, \quad x_{n+1} = \frac{1}{2}\left(x_n +_{\mathbb{Q}} \frac{2}{x_n}\right),$$

где деление — из построенного поля $\mathbb{Q}$. Это так называемая «вавилонская» последовательность, имеющая пределом число $\sqrt{2}$.

Далее, как и в случае с рациональными числами, порядок и операции на классах эквивалентности задаются через их представителей (с доказательством корректности определения).

Порядок:

$$[\langle x_n \rangle] <_{\mathbb{R}} [\langle y_n \rangle] \overset{\text{def}}{\leftrightarrow} \exists \delta >_{\mathbb{Q}} 0_{\mathbb{Q}} : \exists N \in \omega : \forall n > N : x_n +_{\mathbb{Q}} \delta \leqslant_{\mathbb{Q}} y_n,$$

т.е. первая последовательность строго меньше второй, если они через конечное число шагов расходятся на расстояние не меньше $\delta$ с тем же знаком неравенства.

[16] Такие последовательности называют также последовательностями Коши — в честь французского математика Огюстена Луи Коши, заложившего строгие основания анализа.

Сложение и умножение:

$$[\langle x_n\rangle] +_{\mathbb{R}} [\langle y_n\rangle] \stackrel{\text{def}}{\rightleftharpoons} [\langle x_n +_{\mathbb{Q}} y_n\rangle], \quad [\langle x_n\rangle] \cdot_{\mathbb{R}} [\langle y_n\rangle] \stackrel{\text{def}}{\rightleftharpoons} [\langle x_n \cdot_{\mathbb{Q}} y_n\rangle].$$

Как видим, определения не сложные, и доказательство их корректности тоже. Таким образом у нас полностью определена структура $\mathbb{R} \stackrel{\text{def}}{\rightleftharpoons} \langle =, <_{\mathbb{R}}, +_{\mathbb{R}}, \cdot_{\mathbb{R}}, 0_{\mathbb{R}}, 1_{\mathbb{R}}\rangle$. Если смотреть на наши построения с точки зрения рангов множеств, то мы недалеко ушли от ранга $\omega$ (если точнее, то $\mathrm{rank}(Z) = \omega$, $\mathrm{rank}(Q/_{\sim}) = \omega + 1$, $\mathrm{rank}(R) = \omega + 5$). В случае использования дедекиндовых сечений ранг был бы чуть меньше.[17]

Мы не будем здесь (и даже в Части II) приводить доказательство истинности аксиом RCF в данной модели вещественных чисел, т.к. это стандартная процедура, показанная во многих учебниках по математическому анализу (см., напр., [19]). Для нас важно другое: имея очень простой язык ZF, мы сумели построить конкретные теоретико-множественные структуры, являющиеся моделями натуральных, целых, рациональных и вещественных чисел. При желании мы можем продолжить строительство, перейдя к структуре $\mathbb{R}^n$ с нужной сигнатурой, получая тем самым комплексные числа и эвклидово пространство, а затем еще добавить бесконечномерное пространство $\mathbb{R}^\omega$ и т.д. В смысле шкалы рангов мы не сильно уйдем от $\omega$ (на конечное число шагов).

Наличие таких моделей в первую очередь говорит о том, что все эти числовые системы непротиворечивы постольку, поскольку непротиворечива теория множеств Цермело-Френкеля.

В-вторых, это построение является классическим учебным приемом построения моделей каких-либо формальных математических языков и теорий.

В-третьих, мы можем заметить, что все наши модели очень сильно завязаны на конкретные множества, прежде всего ординал $\omega$. Но это вовсе не означает, что они являются единственно возможными моделями. Можно менять как саму методику построения носителей этих структур (скажем, выбирать дедекиндовы сечения для построения $\mathbb{R}$ или специального вида матрицы для построения $\mathbb{Z}$), так и стартовые множества. Дело в том, что в конечном счете нас интересуют только алгебраические свойства вновь созданных моделей, выразимые в языке сигнатуры, а никак не их внутреннее устройство и место в иерархии фон Неймана. Больше того, знания об устройстве конкретной модели нельзя использовать для получения теорем той теории, которую мы в ней моделируем, потому что теория — это прежде всего подмножество языка. И если в языке теории (как, например, в языке RCF) нет предиката принадлежности, то использовать факты из модели, содержащие такой предикат, для работы с теорией нельзя.

Конечно, есть ситуации, когда теоретико-множественный факт из модели может быть переведен на язык структуры, т.е. выражен в языке, полученном из сигнатуры данной структуры, в таком случае у нас получается модель, выполняющая некоторое предложение из языка теории. И если ни это предложение, ни его отрицание не выводятся из аксиом теории, то модель подтверждает его независимость от этих аксиом.

В случае же теории RCF мы знаем, что эта теория полна, т.е. любое предложение в ее языке либо доказуемо, либо опровержимо, а значит, во всех ее моделях верны те и только те предложения, которые выводимы из аксиом. Все остальное — от лукавого. Точнее, любые другие факты из модели не могут быть записаны (выражены) на языке теории RCF.

Хорошим примером такого «лукавого» факта является архимедовость стандартной модели $\mathbb{R}$. Поле, которое мы построили выше, обладает свойством Архимеда, т.е. для

[17] Построение $\mathbb{R}$ с помощью дедекиндовых сечений см. в [4].

любых вещественных чисел $a, b > 0$ найдется такое натуральное число $n$, что $an > b$. Это свойство нельзя выразить в языке сигнатуры $\langle 0, 1, \leqslant, +, \cdot \rangle$, поскольку мы не можем производить в нем квантование по произвольным натуральным числам. Да, мы можем выразить каждое конкретное натуральное число нумералом вида $1 + \cdots + 1$ (похожим образом мы вводили нумералы в PA), но мы не можем написать $\forall n$ или $\exists n$ и не можем написать в этом языке формулу, областью истинности которой будут только натуральные числа, инкапсулированные в модель $\mathbb{R}$.

Поскольку свойство архимедовости невыразимо на языке RCF, оно тем более не может быть ни доказано, ни опровергнуто в рамках аксиом RCF, так что существуют модели вещественно замкнутых полей как обладающие таким свойством, так и не обладающие им.

Другим примером такого невыразимого факта является полнота множества вещественных чисел. Свойство полноты состоит в том, что любое непустое ограниченное сверху множество вещественных чисел имеет точную верхнюю грань. Модель, которую мы построили, обладает таким свойством, но в языке RCF это утверждение также невыразимо, поскольку для него требуется привлечение средств теории второго порядка (с кванторами по множествам действительных чисел).

Приведенные примеры подчеркивают тот факт, что для одной и той же теории в заданном языке может существовать большое разнообразие моделей, причем в этих моделях могут быть факты, невыразимые и/или недоказуемые в данной теории.

Даже с самой теорией множеств не все так гладко, как хотелось когда-то Гильберту. Да, этот язык обладает колоссальной выразительной способностью, но даже для него мы можем изобретать очень непохожие друг на друга модели, если, конечно, чуть-чуть ослабим аксиоматику (вспомним модели Куайна и $V_\omega \setminus \{\varnothing\}$). Впрочем, при одной и той же аксиоматике ZF мы также имеем различные модели, построенные Гёделем и Коэном, подтверждающие независимость аксиомы выбора и обобщенной континуум-гипотезы.

Тем не менее, чтобы не привязываться всякий раз к какой-то конкретной модели, предлагается рассматривать класс изоморфных моделей, обладающих нужными нам свойствами. Изоморфизм моделей — это биекция между их носителями, сохраняющая отношения, операции и константы.[18] Изоморфизм является отношением эквивалентности на классе всех структур с заданной сигнатурой, и с точки зрения абстрактной алгебры или общей топологии изоморфные структуры считаются тождественными. Например, группа, состоящая из единственного элемента, считается единственной во всей вселенной, несмотря на то, что в теории множеств у нее существует целый собственный класс изоморфных моделей.

В то же время, замечая, что структуры, являющиеся моделями какой-то конкретной теории, могут обладать теми или иными полезными свойствами (например, архимедовостью и полнотой), невыразимыми в этой теории, мы можем выделить особый подкласс изоморфных моделей, обладающих именно такими свойствами, и объявить этот подкласс, скажем, стандартной моделью теории. Больше того, специально для этого подкласса моделей мы можем сделать язык теории более выразительным (ввести для него переменные по множествам, например), чтобы эти «хорошие» с нашей точки зрения свойства моделей можно было выразить в данном языке. После чего мы можем изучать так называемую *элементарную теорию* этой модели (точнее, подкласса

[18] Понятие изоморфизма кристаллизовалось в XIX веке в работах по абстрактной алгебре (например, у Артура Кэли, который ввел понятие абстрактной группы).

изоморфных моделей), которая по определению будет полной, поскольку включает все истинные в модели предложения.

К таким теориям обычно относят $\mathrm{Th}(\mathbb{N})$ — полная теория стандартной модели арифметики, $\mathrm{Th}(\mathbb{Z})$ — полная теория стандартной модели кольца целых чисел, $\mathrm{Th}(\mathbb{Q})$ — полная теория стандартной модели поля рациональных чисел. Все три теории задаются в первопорядковом языке сигнатуры $\langle =, <, +, \cdot, 0, 1\rangle$,[19] они полны по определению, но множество их теорем неперечислимо. Тем интереснее, что полная первопорядковая теория вещественных чисел $\mathrm{Th}(\mathbb{R})$ *в той же самой сигнатуре* совпадает с теорией RCF, т.е. является перечислимой.

Может показаться на первый взгляд, что здесь есть некое противоречие: вроде бы с каждым разом числовая структура становится более сильной в алгебраическом смысле, и того же хочется ожидать от ее теории, но теории наоборот становятся проще в каком-то смысле, по крайней мере, это можно сказать про теорию $\mathrm{Th}(\mathbb{R})$. Почему так?

Дело в том, что все четыре теории, будучи полными, выхватывают различные подмножества замкнутых формул из общего для них языка. Иначе говоря, каждая из них содержит такие предложения, которые не доказуемы в других теориях. У их множеств истинных предложений нет никакой преемственности, они не следуют вложению множеств $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$. Вот примеры уникальных для каждой теории предложений:

- $\forall y \geqslant 0 : \exists x\ (y = x^2)$ (из любого неотрицательного числа можно извлечь квадратный корень) — истинно в $\mathrm{Th}(\mathbb{R})$ (аксиома RCF), но ложно в $\mathrm{Th}(\mathbb{N})$, $\mathrm{Th}(\mathbb{Z})$, $\mathrm{Th}(\mathbb{Q})$;
- утверждение о существовании числа $x$ такого, что $0 < x < 1$ и $x$ не есть квадрат какого-то $y$, истинно в $\mathrm{Th}(\mathbb{Q})$, но ложно в $\mathrm{Th}(\mathbb{N})$, $\mathrm{Th}(\mathbb{Z})$, $\mathrm{Th}(\mathbb{R})$;
- утверждение о существовании отрицательного простого числа истинно в $\mathrm{Th}(\mathbb{Z})$, но ложно в $\mathrm{Th}(\mathbb{N})$, $\mathrm{Th}(\mathbb{Q})$ и $\mathrm{Th}(\mathbb{R})$;
- $\forall x\ (x \geqslant 0)$ истинно в $\mathrm{Th}(\mathbb{N})$, но ложно в $\mathrm{Th}(\mathbb{Z})$, $\mathrm{Th}(\mathbb{Q})$ и $\mathrm{Th}(\mathbb{R})$.

Чуть более сложная вещь — полная теория $\mathrm{Th}^2(\mathbb{R})$ вещественных чисел второго порядка со свойствами полноты и архимедовости. Ее выразительные способности гораздо сильнее, чем у первопорядковых теорий, и все теории $\mathrm{Th}(M)$, где $M \in \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$ естественным образом интерпретируются в $\mathrm{Th}^2(\mathbb{R})$.

Теория RCF, являясь полной теорией,[20] является одновременно теорией *всех* своих моделей, класс которых значительно шире, чем класс вещественно замкнутых архимедовых полных полей, который и принимается в качестве *стандартной модели вещественных чисел*.[21]

## C1.5. Итоги и вопросы для самоконтроля

На этом мы завершаем наше путешествие в мир формальных теорий и их моделей. Мы увидели, как из довольно скромного набора аксиом теории множеств, подобно строительным блокам, можно возводить сложные и разнообразные математические

[19] В случае $\mathbb{N}$ сигнатура немного отличается (нет 1, но есть последователь), однако ее легко переписать в этой же сигнатуре, заменив $S(x)$ на $x + 1$.

[20] Она не является геделевой уже по причине того, что не умеет интерпретировать арифметику

[21] Имеется в виду модель Хенкина теории RCF, а также модель гипердействительных чисел с бесконечно малыми числами (инфинитезималями). В обоих моделях не выполняется ни аксиома Архимеда, ни принцип полноты.

структуры, служащие интерпретациями для других, более специфических теорий — от арифметики до анализа. Построение моделей не только демонстрирует относительную непротиворечивость этих теорий (в предположении непротиворечивости самой теории множеств), но и позволяет глубже понять их природу, выявляя свойства, которые могут быть истинными в одних моделях и ложными в других, или вовсе невыразимыми на языке исходной теории.

Идея сопоставления формальной теории и конкретной математической структуры, в которой эта теория «живет», имеет богатую историю. Хотя интуитивное понятие модели использовалось в математике задолго до формализации (например, в геометрии Эвклида или при построении моделей неевклидовых геометрий Бельтрами, Клейном и Пуанкаре в XIX веке), явное формулирование связи между синтаксисом (аксиомами и правилами вывода) и семантикой (интерпретациями, моделями) стало возможным лишь на рубеже XIX–XX веков с развитием математической логики.

Работы Леопольда Лёвенгейма (1915) и Туральфа Скулема (1920-е гг.), кульминацией которых стала теорема Лёвенгейма-Скулема, показали, что если теория первого порядка имеет бесконечную модель, то она имеет модели любой бесконечной мощности. Это привело к пониманию, что аксиомы первого порядка не могут однозначно охарактеризовать такие структуры, как натуральные или вещественные числа, породив концепцию «нестандартных моделей».

Ключевым моментом стало доказательство Куртом Гёделем теоремы о полноте для логики первого порядка (1929), утверждающей, что любая непротиворечивая теория первого порядка имеет модель. Это фундаментально связало доказуемость (синтаксическое понятие) с истинностью во всех моделях (семантическое понятие). Его же теоремы о неполноте (1931) для достаточно богатых теорий, таких как арифметика Пеано, продемонстрировали существование истинных, но недоказуемых утверждений, что также стимулировало изучение нестандартных моделей арифметики.

Альфред Тарский в 1930-50-е годы заложил основы современной теории моделей как самостоятельной дисциплины, введя строгое определение истины в модели и разработав методы исследования элементарных теорий. Результат Тарского-Зайденберга о полноте и разрешимости теории вещественно замкнутых полей, упомянутый нами, является одним из классических достижений этой эпохи.

*Альфред Тарский*

Наконец, революционным прорывом в теории множеств стало развитие метода форсинга Полом Коэном в 1960-х годах, позволившего строить модели теории множеств, в которых независимы такие утверждения, как аксиома выбора или континуум-гипотеза. Это продемонстрировало невероятную гибкость и богатство универсума фон Неймана и его возможных «альтернативных версий».

Таким образом, понятие модели прошло путь от интуитивного инструмента до центрального объекта изучения в математической логике. Оно позволяет не только строить и классифицировать математические структуры, но и глубже понимать пределы и возможности формальных систем, а также природу математической истины. Надеемся, что знакомство с этим подходом, представленное в данной книге, послужит для читателя стимулом к дальнейшему изучению этих увлекательных и фундаментальных вопросов математики и логики.

Как обычно, в завершение очередного «лингвистического» уровня предлагаем несколько вопросов для самоконтроля.

**Q1** Чем отличаются различные аксиоматики теории множеств (ZF, ZFC, Z)? [стр. 147]

**Q2** Объясните концептуальное значение иерархии универсумов фон Неймана (C1.4) и понятия ранга множества. Как эта иерархия помогает структурировать универсум множеств и понимать природу бесконечных множеств? [стр. 167]

**Q3** Обсудите концептуальное влияние аксиомы выбора на математику. В чем ее положительные и отрицательные стороны? [стр. 153]

**Q4** Приведите примеры утверждений, равносильных AC.

**Q5** Приведите примеры утверждений, которые слабее AC.

**Q6** Приведите примеры утверждений, которые сильнее AC или являются альтернативами для AC.

## C1.6. Упражнения

**Ex1.** Переведите следующие утверждения в формулы языка ZF, используя предикат принадлежности $\in$ и логические связки:

1. Множество $A$ является подмножеством множества $B$.
2. Множества $A$ и $B$ не имеют общих элементов (не пересекаются).
3. Множество $A$ содержит ровно два элемента.
4. Множество $P$ является множеством всех подмножеств (булеаном) $A$ (т.е. $P = \mathscr{P}(A)$).

**Ex2.** Сформулируйте следующие понятия и теоремы в виде одиночных формул на языке теории множеств (используя вспомогательные предикаты, если необходимо):

- Теорема Кантора: не существует сюръекции из $A$ в $\mathscr{P}(A)$.
- Аксиома счетного выбора ($\mathrm{AC}_\omega$).
- Определение фильтра: Семейство $\mathscr{F} \subseteq \mathscr{P}(S)$ является фильтром на $S$, если:
  1. $S \in \mathscr{F}$ и $\varnothing \notin \mathscr{F}$;
  2. $\mathscr{F}$ замкнуто относительно пересечения (если $A \in \mathscr{F}$ и $B \in \mathscr{F}$, то $A \cap B \in \mathscr{F}$);
  3. $\mathscr{F}$ замкнуто относительно надмножеств (если $A \in \mathscr{F}$ и $A \subseteq B \subseteq S$, то $B \in \mathscr{F}$).
- Принцип максимума Хаусдорфа: в любом частично упорядоченном множестве любая цепь содержится в максимальной цепи.

**Ex3.** Пусть $S$ — бесконечное множество. Рассмотрим совокупность $\mathscr{F}$ всех подмножеств $X \subseteq S$, таких что $S \setminus X$ конечно. Докажите, что $\mathscr{F}$ является фильтром.

**Ex4.** Пусть $A = \{a, b, c\}$. Определите, какие из следующих отношений на $A$ являются рефлексивными, симметричными, антисимметричными или транзитивными:

1. $R_1 = \{\langle a, a\rangle, \langle b, b\rangle, \langle c, c\rangle\}$.
2. $R_2 = \{\langle a, b\rangle, \langle b, a\rangle, \langle a, a\rangle\}$.
3. $R_3 = \{\langle a, b\rangle, \langle b, c\rangle, \langle a, c\rangle\}$.

**Ex5.** Пусть функция $J : \omega \times \omega \to \omega$ задана формулой:

$$J(a, b) = 2^a(2b + 1) - 1.$$

Докажите, что $J$ является биекцией.

**Ex6.** Используя Аксиому выбора, докажите, что для любой сюръективной функции $f : A \to B$ существует функция $g : B \to A$ (называемая правым обратным или сечением), такая что $f(g(y)) = y$ для всех $y \in B$.

**Ex7.** Пусть $A$ — конечное непустое множество с частичным порядком $\leqslant$. Пусть $n = |A|$. Опишите рекурсивный алгоритм, который строит биекцию $f : A \to \{0, 1, \ldots, n - 1\}$, такую что:

$$x < y \implies f(x) < f(y).$$

Покажите, что порядок, заданный условием $x \preccurlyeq y \iff f(x) \leqslant f(y)$, является линейным порядком на $A$, который продолжает $\leqslant$.

**Ex8.** Определите, являются ли следующие множества ординалами (согласно определению: транзитивное множество, вполне упорядоченное отношением $\in$):

1. $A = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$.
2. $B = \{\varnothing, \{\{\varnothing\}\}\}$.
3. $C = \omega \cup \{\omega\}$.

**Ex9.** Вычислите ранг (rank) следующих множеств:

1. $\varnothing$.
2. $\{\varnothing\}$.
3. $\{\{\varnothing\}\}$.
4. $\{\varnothing, \{\varnothing\}\}$.

**Ex10.** 1. Используя определение пары Куратовского $\langle a, b\rangle = \{\{a\}, \{a, b\}\}$, выразите $\operatorname{rank}(\langle a, b\rangle)$ через $\alpha = \operatorname{rank}(a)$ и $\beta = \operatorname{rank}(b)$.

2. Определите ранг множества целых чисел $\mathbb{Z}$, если целые числа определены как классы эквивалентности пар натуральных чисел.

**Ex11.** Определите, к какому универсуму $V_\alpha$ следующие множества принадлежат впервые (найдите наименьшее $\alpha$, такое что $x \in V_\alpha$):

1. $x = \varnothing$.
2. $x = \omega$.
3. $x = \mathscr{P}(\omega)$.

**Ex12.** Пусть функция $F : \mathrm{Ord} \to \mathrm{Ord}$ задана условием $F(\alpha) = \sup(\{F(\beta) + 1 \mid \beta < \alpha\})$. Чему равно $F(\alpha)$?

**Ex13.** Мы хотим определить последовательность Фибоначчи $F$ на натуральных числах $\omega$ (рассматриваемых как конечные ординалы) так, что $F(0) = 0, F(1) = 1, F(n) = F(n - 1) + F(n - 2)$. Явно опишите порождающую функцию $\Phi(g)$, которая принимает функцию предыстории $g$ (определенную на некотором ординале $\alpha < \omega$) и возвращает следующее значение.

**Ex14.** Постройте явную биекцию между множеством вещественных чисел $\mathbb{R}$ и замкнутым единичным интервалом $[0;1]$.

**Ex15.** Покажите, что множество точек в открытом интервале $(0,1)$ равномощно множеству точек в объединении интервалов $(0,1) \cup (2,3)$.

**Ex16.** Пусть $A = B = \omega$ (множество натуральных чисел) со стандартным порядком $\leqslant$. Рассмотрим произведение $P = A \times B$. Сравните пары $x = \langle 2, 100\rangle$ и $y = \langle 3, 1\rangle$, используя следующие отношения. Для каждого отношения определите, является ли оно линейным порядком и является ли оно вполне упорядочением на $P$:

1. Покомпонентный порядок $\leqslant_{prod}$: $\langle a,b\rangle \leqslant_{prod} \langle c,d\rangle \overset{\text{def}}{\leftrightarrow} a \leqslant c \wedge b \leqslant d$.
2. Лексикографический порядок $\leqslant_{lex}$: $\langle a,b\rangle \leqslant_{lex} \langle c,d\rangle \overset{\text{def}}{\leftrightarrow} a < c \vee (a = c \wedge b \leqslant d)$.

**Ex17.** Покажите, что аксиома регулярности запрещает существование множества $x$, такого что $x = \{x\}$.

**Ex18.** Вычислите следующие суммы и произведения ординалов (напоминаем, что операции некоммутативны):

1. $1 + \omega$.
2. $\omega + 1$.
3. $2 \cdot \omega$.
4. $\omega \cdot 2$.

**Ex19.** Проверьте закон правой дистрибутивности $(\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma$ для $\alpha = 1, \beta = 1, \gamma = \omega$.

**Ex20.** Найдите все ординалы $x$, удовлетворяющие уравнению:

$$\omega + x = \omega \cdot 2.$$

**Ex21.** Сравните ординалы $\alpha = \omega^2 + \omega \cdot 3 + 1$ и $\beta = \omega^2 + \omega \cdot 2 + 5$. Какой из них меньше?

**Ex22.** Рассмотрим множество $P = \omega \times \omega$ (пары натуральных чисел), снабженное лексикографическим порядком $\leqslant_{lex}$ из упражнения 16. Определите порядковый тип структуры $\langle P, \leqslant_{lex}\rangle$. Выразите результат, используя умножение ординалов. *Подсказка: Визуализируйте порядок как последовательность «строк» $R_n = \{\langle n, m\rangle \mid m \in \omega\}$, упорядоченных по индексу $n$.*

**Ex23.** Почему в ZFC нельзя говорить о «множестве всех множеств»? Какая аксиома была бы нарушена, если бы такое множество существовало?

**Ex24.** Предположим, что поле вещественных чисел $\mathbb{R}$ построено. Определите множество комплексных чисел $\mathbb{C}$ как декартово произведение $\mathbb{R} \times \mathbb{R}$. Определите операции $+_{\mathbb{C}}$ и $\cdot_{\mathbb{C}}$ формально как подмножества $(\mathbb{C} \times \mathbb{C}) \times \mathbb{C}$. Проверьте, что для элемента $i = \langle 0, 1\rangle$ выполняется условие $i \cdot_{\mathbb{C}} i = \langle -1, 0\rangle$.

**Ex25.** Пусть $\langle A, \leqslant\rangle$ — частично упорядоченное множество. Мы говорим, что отношение $\preccurlyeq$ является продолжением $\leqslant$, если $\leqslant \subseteq \preccurlyeq$. Используйте Лемму Цорна, чтобы доказать, что существует линейный порядок на $A$, который продолжает частичный порядок $\leqslant$ (теорема Шпильрайна о продолжении). *Подсказка: Рассмотрите множество всех частичных порядков на $A$, продолжающих $\leqslant$, упорядоченное по включению $\subseteq$.*

# Часть II

# Доказательная база

# ГЛАВА D1

# Язык

*Вы должны воспринимать не то, что я говорю или пишу, а то, что я думаю.*

— Николай А. Вавилов

## D1.1. Элементарные частицы языка

Поскольку наш язык $\mathfrak{Math}$ чисто письменный, мы будем смотреть на его возможные реализации как на тексты или, более общо, тексты с дополнительными графическими материалами, начисто забыв о том, как эти тексты могли бы озвучиваться в каком-либо разговорном языке. И тексты, и дополнительная графика к ним складываются из **элементарных графем**, т.е. некоторых неделимых графических изображений, масштаб и незначительные вариации начертания которых не играют существенной роли для языка $\mathfrak{Math}$ (за редкими исключениями). При этом графемы из разных шрифтов (начертаний), а также графемы разного регистра (строчные и прописные) мы будем считать различными, чтобы не вводить еще и понятие *аллографа*.

Понятие неделимого графического изображения — довольно-таки условное понятие, но в целом его можно определить как композицию графических элементов, которая в любой реализации языка $\mathfrak{Math}$ не разделяется и не перекрывается другими элементами (иначе говоря, неделимую графему нельзя разделить на две части так, чтобы обе части имели какой-то смысл в математике, кроме особого случая — жестких графем, принудительно отнесенных в класс элементарных).

С другой стороны, элементарная графема может быть достаточно сложной и содержать в себе как часть более простую элементарную графему. Поэтому элементарные графемы необходимо структурировать, выделив в них классы и виды так, чтобы получить некоторую «алгебру» построения элементарных графем.

Прежде всего, выделим **алфавит**, или список **осно́вных графем**.

Прежде всего, список осно́вных графем включает *латинские буквы* от $A, a$ до $Z, z$. Некоторые строчные и прописные буквы латинского алфавита трудно различить, не зная их размер, однако в рамках достаточно длинного текста всегда можно понять средний размер строчных букв и тем самым выявить, какой вариант латинской буквы используется.

Далее, безусловно к осно́вным графемам относятся греческие буквы от $\alpha$ до $\omega$, а также их прописные варианты, которые отличаются по начертанию от латинских аналогов, например, $\Lambda$, $\Sigma$, $\Omega$.

Кроме того, с меньшей частотой язык $\mathfrak{Math}$ использует буквы других алфавитов, прежде всего, еврейского, например, $\aleph$ или $\beth$, а также различные модификации букв с помощью существенного изменения шрифта: например, буквы $F$, $\mathbb{F}$, $\mathrm{F}$ и $\mathscr{F}$ мы считаем разными осно́вными графемами.

Следующий вид основ́ных графем нашего алфавита — это цифры $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$, которые также могут подвергаться шрифтовым модификациям, порождая новые элементарные графемы (но это крайне редкое явление).

Буквенно-цифровые основ́ные графемы мы объединим в один класс — *самостоятельные основ́ные графемы*. Обычно это такие символы, из которых складываются собственные названия и обозначения объектов и переменных в языке $\mathfrak{Math}$. Класс самостоятельных графем можно также расширить небольшим набором спецсимволов вроде $\infty$ или %, если очень нужно использовать их в названиях объектов.

К алфавиту языка $\mathfrak{Math}$ мы также отнесем различные небуквенные неделимые графемы, которые условно можно разделить на три вида: а) группирующие; б) разделяющие; в) операторные. Эти три вида элементарных графем мы объединим в класс *несамостоятельных* графем. Они как правило служат для обозначения функций и отношений, а значит, употребляются в сочетании с самостоятельными графемами.

*Группирующие графемы* (или *группира́торы*) — это чаще всего парные символы, предназначенные для обособления группы графем. Это такой мягкий способ собрать новую лексическую единицу из более простых. Мягким я его называю потому, что создаваемая группа не представляет собой какой-то новый единый объект языка и может быть разобрана при контекстном анализе на составляющие ее части.

Примеры группираторов: круглые скобки ( ), квадратные скобки [ ], фигурные скобки { }, угловые скобки $\langle\ \rangle$, кавычки (одинарные, двойные), а также прямые скобки | | и двойные прямые скобки || ||. Иногда символы группиратора могут быть несимметричными, например, обозначения бра- и кет-векторов: $\langle$ | и | $\rangle$.

*Разделяющие графемы* (или *разделители*) — это по сути знаки препинания языка $\mathfrak{Math}$, которые призваны отделить одну часть сложной лексемы от другой. К ним можно отнести: запятую (,), двоеточие (:), точку с запятой (;), штрих (|) и т.п. (здесь скобки использованы для обособления определяемого символа и не входят в его состав).

Наиболее богатый арсенал средств языка $\mathfrak{Math}$ представляют собой операторные графемы, которые используются для обозначений всевозможных действий (операций) и связей (отношений). По сути, операторные графемы — это глаголы языка $\mathfrak{Math}$, а точнее, лишь базовая часть глаголов, поскольку из них мы можем составлять более сложные операторные лексемы, которые можно считать аналогом более сложных глаголов (тут уместно вспомнить словообразование немецкого языка в качестве аналога).

*Операторные графемы*, или *опера́торы*, представляют собой «иероглифическую» составляющую языка $\mathfrak{Math}$. В качестве широко известных примеров операторных графем приведем такие: $+$, $\int$, $<$, $\Rightarrow$, $\cup$, $\square$, $\vdash$. Количество операторных графем, используемых в математике, на порядки превышает количество используемых букв. Более того, встречаются такие операторные графемы, которые получены из букв с помощью переворачивания, например, $\forall$, $\exists$, $\nabla$ (иногда это позволяет объяснить смысл выбранного обозначения).

Кроме того, некоторые операторные графемы внешне могут напоминать какие-то другие символы алфавита, например, символ объединения множеств $\cup$ похож на латинскую букву $U$ (поскольку происходит от слова *unite*), символ суммирования $\sum$ прямо происходит от греческой буквы $\Sigma$, а отношение делимости | неотличимо от разделяющего символа штриха и группирующей прямой скобки. Тонкие различия этих символов для нас на самом деле не столь существенны (хотя можно, например, сказать, что операторная графема $\sum$ никогда не встречается без операндов, а знак делимости имеет вокруг себя половинные пробелы в отличие от прямой скобки), поскольку при желании

мы можем считать, что один и тот же базовый символ участвует в образовании более сложных лексем в разных ипостасях, а его значение определяется контекстом.

Многие операторные графемы получаются из других операторных графем отражением или поворотом. Например, мы можем взять одну стрелку $\rightarrow$ и из нее сделать несколько новых символов: $\leftarrow$, $\uparrow$, $\nearrow$. Другой пример: взаимно обратные отношения $\in$ и $\ni$, $\subset$ и $\supset$, $<$ и $>$. Синтаксически это разные графемы (они и читаются по-разному, и иногда даже применяются для разных целей[1] ), хотя и продуцируются из одного базового графического элемента.

На этом заканчивается описание множества основ́ных графем (алфавита) языка Math.

Таблица D1.1. Элементарные графемы

| Класс графем | Вид графем | Примеры |
|---|---|---|
| | *Основ́ные графемы (алфавит)* | |
| Самостоятельные | Буквы | $A \ldots z$, $\alpha \ldots \omega$, $\aleph$, $\beth$ |
| | Цифры | $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ |
| | Спецсимволы | $\infty$, $\varnothing$, $\top$, $\bot$, $\hbar$ |
| Несамостоятельные | Группираторы | $()$, $[]$, $\lvert\,\rvert$, $\langle\rangle$, $\{\}$, $\langle\,\rvert$, $\lvert\,\rangle$ |
| | Разделители | $,$ $:$ $;$ $.$ $!$ $\lvert$ |
| | Операторы | $+$, $\int$, $<$, $\Rightarrow$, $\cup$, $\square$, $\vdash$, $\uparrow$ |
| Вспомогательные графемы | | $\tilde{}$ $'$ $\acute{}$ $\grave{}$ $\hat{}$ $\ddot{}$ $\bar{}$ $*$ $\vec{}$ |
| | *Производные графемы* | |
| Самостоятельные | Буквы | $A' \ldots \hat{\hat{z}}$, $\tilde{\alpha} \ldots \omega^*$, $\overline{\overline{\aleph}}$, $\overline{\beth}$ |
| | Цифры | $\overline{0}, \overline{1}', 2'', 3''', 4'''', 5, 6^*, 7^{**}, \vec{8}, \tilde{9}$ |
| | Спецсимволы | $\overline{\infty}$ |
| Несамостоятельные | Операторы | $+'$, $<''$, $\square'$ |

Следующий блок элементарных графем — это **вспомогательные графемы**. Это — такие символы, которые, как правило, не используются в качестве основ́ных графем, но служат для образования потенциально бесконечного ряда элементарных графем.

К вспомогательным графемам относятся, например, следующие: тильда ($\tilde{o}$), апостроф ($o'$), акют ($\acute{o}$), гравис ($\grave{o}$), циркумфлекс ($\hat{o}$), умляут ($\ddot{o}$), горизонтальный штрих ($\bar{o}$), где буква *o* подставлена для наглядности и не является частью перечисленных вспомогательных графем. Как правило, это диакритические знаки из разговорных языков, но встречаются и другие варианты вспомогательных графем, как, например, звездочка ($*$), которая может выступать и в роли акцента для обозначения переменной, и в роли операторного символа для обозначения сопряженного оператора или умножения.

[1] Например, символ $\supset$ иногда используется для обозначения импликации вместо $\rightarrow$.

Вспомогательные графемы сами по себе не являются именами объектов или переменных (кроме тех, которые графически совпадают с операторами).

Наконец, последняя часть элементарных графем — **производные графемы**. Это такие графемы, которые получаются соединением одной основной графемы и одной или нескольких вспомогательных графем. Производные элементарные графемы наследуют от основных деление на классы и виды, и их названия: самостоятельные (буквенные, цифровые, специальные) и несамостоятельные (в основном это операторы).

Таким образом, **элементарные графемы** — это основные графемы (алфавитные) либо сами по себе, либо соединенные со вспомогательными графемами, т.е. производные графемы.

В таблице D1.1 собраны перечисленные выше классы и виды элементарных графем языка Math с примерами.

## D1.2. Лексемы

Разобравшись со стартовым набором символов, мы теперь переходим к правилам «текстостроения». Иначе говоря, мы укажем ряд нехитрых принципов, пользуясь которыми в нашем языке Math можно что-либо в принципе собирать в какой-то текст. Это не значит, что все полученные таким способом лексемы применяются на практике, т.е. являются хоть в какой-то мере распространенными, но мы совершенно точно можем сказать, что весь «корректный» текст языка Math может быть построен только так и никак иначе.

Напомним, что и в разговорном языке есть определенные правила словостроения (по одному из них как раз построено это слово), но это не значит, что мы реально пользуемся всеми теми словами, которые можно таким способом построить. Есть регулярные слова, есть редкие, есть вульгарные, а есть несуществующие — среди тех, которые можно построить по правилам.

Мы выделим два основных метода «текстостроения». Все фрагменты текста языка Math, получаемые этими методами, мы будем называть *лексемами*. Любой текст, составленный из элементарных графем, не являющийся правильно построенной лексемой, считается некорректным. Точное определение лексемы будет приведено ниже.

Во-первых, мы можем конкатенировать любые самостоятельные элементарные графемы, а также их производные графемы в любом количестве и в любом порядке. Иначе говоря, последовательность букв и цифр (а также, может быть, спецсимволов), некоторые из которых могут быть наделены вспомогательными символами (в любом количестве) является правильно построенной графемой Math.

Таким способом, например, появляются многобуквенные наименования функций вроде sin и cos, а также записи чисел вроде 123 (десятичная запись), 1EF0 (шестнадцатеричная запись), MMXXII (римские цифры).

Графемы, полученные указанным способом, назовем *жесткими графемами* в том смысле, что они представляют собой синтаксически неделимые наименования объектов и переменных (например, сочетание sin никто в здравом уме не станет читать как произведение трех переменных). Причем, если чисто цифровых (десятичных или шестнадцатеричных) графем существует бесконечно много (для каждого натурального числа есть своя графема), то буквенно-цифровых — лишь конечный набор, поскольку на практике мы пользуемся ограниченным количеством названий функций и отношений.

К жестким графемам мы также отнесем графемы, которые получаются из уже построенных жестких графем добавлением вспомогательных символов. Например, пусть мы сначала построили жесткую графему lim, а затем решили снабдить ее акцентом в виде горизонтального штриха, и в результате получили графему $\overline{\lim}$. Такая графема тоже относится к жестким.

Иногда можно встретить использование вспомогательных символов в качестве обозначения оператора, например, комплексное сопряжение или производная, и в таком случае этот вспомогательный символ может относиться к сколь угодно длинному фрагменту текста (лексеме). Но, как уже отмечалось выше, это значит лишь то, что графически вспомогательный символ очень похож на операторный, хотя по сути это два символа разного назначения (поэтому $\overline{\lim}$ — это не комплексное сопряжение предела, а целостная операторная графема производного вида).

Как нетрудно видеть, все самостоятельные элементарные графемы являются жесткими графемами. Тем самым мы построили расширение класса самостоятельных элементарных графем до жестких. Поэтому уместно также жесткие графемы называть самостоятельными. Заметим, что операторные элементарные графемы и спецсимволы (как осно́вные, так и производные) мы не относим к жестким (самостоятельным) графемам.

Если проводить параллели с разговорным языком, то жесткие графемы можно, по-видимому, сравнить со словами, причем многобуквенные и цифровые жесткие графемы — это имена собственные, однобуквенные — это имена нарицательные (обычно это переменные). Операторные графемы больше напоминают глаголы, т.к. символизируют действие.

Второй путь построения лексем в языке Math — это *подстановочные шаблоны* или просто *шаблоны*. По сути это некоторый сложный графический символ, составленный из жестких графем, несамостоятельных графем и их производных (речь идет об акцентированных значках операторов), а также из спецсимвола пробела, который в данном случае называется *подстановочным местом*.

Если говорить точнее, то сначала определим **простой шаблон**, который образуется не более чем из одной пары группираторов (скобок) и некоторого (возможно, нулевого) количества разделителей и пробелов, находящихся между группираторами (если таковые есть). Важно заметить, что шаблон, вообще говоря, является двумерной фигурой,[2] а его подстановочные места могут располагаться как угодно друг относительно друга, запрещается лишь перекрытие подстановочных мест. Шаблон требуется именно для того, чтобы некоторым способом сгруппировать и разместить в определенном порядке жесткие графемы и операторы.

Типичный простой подстановочный шаблон имеет линейный вид:

$$\sqcup(\sqcup, \sqcup, \ldots, \sqcup),$$

т.е. одно подстановочное место, следом за которым внутри скобок располагается некоторое (ненулевое) количество пробелов, разделенных запятыми. Такой префиксный способ записи оператора и его аргументов называется *польской нотацией* Лукасевича (Jan Łukasiewicz) и по большому счету даже не требует круглых скобок для перечисления аргументов, поскольку порядок действий определяется однозначно.[3]

[2] На самом деле есть даже трехмерные шаблоны, примером которых является символ Леви-Чивиты в тензорном исчислении.

[3] Существует также *обратная польская запись*, при которой знак оператора ставится после перечис-

Отметим, что в данном случае многоточие — это не символ языка Math, а всего лишь указание на то, что пробелов и запятых внутри скобок может быть любое количество, т.е. указанная выше запись на самом деле охватывает бесконечную серию простых шаблонов. Этот способ предъявления серии однотипных объектов называется *схемой*. Понятие схемы часто используется для записи списка аксиом формальной теории.

Более сложный пример — матрица, образованная парой скобок и некоторым количеством пробелов, расположенных в столбцах и строках:

$$\begin{pmatrix} ␣ & ␣ & ␣ \\ ␣ & ␣ & ␣ \end{pmatrix}.$$

Для того, чтобы двигаться дальше, нам потребуется понятие **рекурсивного определения**. Такие определения чрезвычайно полезны и потому распространены в математике. Они обычно состоят из двух шагов: базового и производного (или продуктивного). Базовый шаг рекурсивного определения задает стартовый набор объектов, относящихся к данному определению, а производный шаг дает алгоритм генерации новых объектов из уже построенных или базовых. Тем самым, многократно применяя производный шаг рекурсивного определения, мы можем строить все более и более сложные объекты, отправляясь от базового набора. Понятие «Рекурсивное определение» или, проще говоря, *рекурсия* получает более точное определение в конкретных областях математики. Так, в арифметике мы имеем дело с *рекурсивными функциями*, а в теории множеств — с *трансфинитной рекурсией*.

Приведем простейший пример рекурсивного определения. Пусть у нас имеется набор букв $a, b, c$. Скажем, что каждая из букв $a, b, c$ является словом, а кроме того, всякое слово есть конкатенация двух слов. Здесь базовым шагом рекурсивного определения понятия «слово» является отнесение букв $a, b, c$ к словам, а производным шагом — получение новых слов путем конкатенирования уже имеющихся. Таким образом данное определение говорит нам, что словами являются любые конечные последовательности букв из списка $a, b, c$.

Итак, дадим рекурсивное определение понятия **подстановочного шаблона** (или, короче, **шаблона**). Во-первых, скажем, что всякий простой шаблон является (подстановочным) шаблоном. Во-вторых, если шаблоны подставить в подстановочные места шаблона, то в результате тоже получается шаблон. Таким образом шаблон — это все, что получается из простых шаблонов путем подстановок шаблонов в шаблоны. Получается этакая «матрешка» из простых шаблонов.

Пример шаблона, соответствующего приведенному определению:

$$\left[\begin{pmatrix} (␣,\ ␣) & ␣ & ␣ \\ ␣ & ␣ & \langle ␣; ␣ \rangle \end{pmatrix} \mid \{␣ \mid ␣\}\right].$$

Но на самом деле нам этого мало, поскольку мы хотели бы иметь более содержательные шаблоны, в которых заранее заданы некоторые операторные графемы, позволяющие понять, как именно применяется данный шаблон в конкретной реализации

ления аргументов. Такой способ записи операций использовался раньше на программируемых калькуляторах.

языка Math. Поэтому мы дополним данное выше определение шаблонов понятием **производного шаблона**. К производным шаблонам относятся все те конструкции, которые можно получить из шаблонов путем подстановки на их подстановочные места произвольных жестких графем, пробелов и операторных символов.

Условно говоря, если мы возьмем матрешку и в самую маленькую ее часть положим конфету, то у нас получится производный шаблон. Однако, как известно, любая аналогия ложна, вот и в нашем примере с матрешкой мы имеем лишь линейную конструкцию с единственным подстановочным местом, в которое мы положили конфету. На деле же шаблоны имеют обычно разветвленную структуру, так что конфет в них можно спрятать несколько. К сожалению, я не встречал матрешек, в которых было бы несколько камер для размещения в них более мелких матрешек с несколькими же камерами.

Но вернемся к языку Math. Например, взяв шаблон ␣(␣) и подставив вместо первого пробела графему sin, мы получим производный шаблон с одним подстановочным местом sin(␣), служащий для записи функции синуса. Если же мы возьмем исходный шаблон вида

$$\begin{matrix}\sqcup\\ \sqcup\\ \sqcup\end{matrix}\ \sqcup\ \sqcup\ \sqcup,$$

то, подставив в него операторный символ $\int$ и букву $d$, получим производный шаблон для обозначения определенного интеграла:

$$\int\limits_{\sqcup}^{\sqcup}\ \sqcup\, d\, \sqcup\,.$$

Производные шаблоны являются основой для синтаксического определения всех математических операций, отношений и функций. Здесь мы можем привести такие примеры:

$$\sqcup+\sqcup,\quad -\sqcup,\quad \frac{\sqcup}{\sqcup},\quad \sqrt{\sqcup},\quad \sqcup^{\sqcup},\quad \sqcup=\sqcup,\quad \cos(\sqcup),\quad \ldots$$

В качестве еще одного примера можно привести шаблон ␣.␣, который позволяет записывать числа с точкой, отделяющей целую часть. Этот шаблон можно расширить, сделав из него шаблон для обозначения чисел с плавающей точкой в экспоненциальной форме ␣.␣E␣.

На примере определения производных шаблонов мы можем продемонстрировать очень важную особенность математических определений, а именно: максимальное покрытие крайних случаев одним определением. Так, в определении производного шаблона мы разрешили на подстановочные места шаблонов ставить пробелы. По сути это означает, что мы можем ничего не делать, и поэтому *всякий подстановочный шаблон является производным шаблоном* в силу определения. Иначе говоря, понятие производного шаблона расширяет понятие подстановочного шаблона.

Далее, поскольку в определении производного шаблона мы умолчали о том, могут ли при его построении быть заполнены все подстановочные места или какие-то должны остаться пустыми, мы можем рассмотреть другой крайний случай — когда пробелы полностью устранены, т.е. в полученном производном шаблоне не осталось подстановочных мест. В связи с этим дадим следующее определение. **Лексемой** языка Math называется производный шаблон без подстановочных мест.

Таким образом производные шаблоны включают в себя лексемы как частный случай. То есть наша матрешка, в которой все пустоты заполнены конфетами, — это лексе-

ма. Соответственно, лексемами будут такие графические конструкции, как, например,

$$a+\hat{b},\quad -x^*,\quad \frac{32.33}{127.87},\quad \sqrt{5},\quad e^{\pi},\quad A=\tilde{B},\quad \cos(x),\quad \int\limits_0^{\infty} u dt.$$

Здесь можно провести прямую аналогию с формулами и предложениями. В формулах, как и в производных шаблонах, имеются неопределенные подстановочные места — свободные переменные, а предложения — это замкнутые формулы, в которых все свободные переменные так или иначе устранены (заменены замкнутыми термами или замкнуты кванторами). Так что лексемы — это в каком-то смысле замкнутые производные шаблоны.

Кстати, если мы воспользуемся шаблоном ⊔ (состоящим только из единственного подстановочного места, что не запрещается определением), то тем самым к лексемам причислим и все жесткие графемы (а значит, и все самостоятельные графемы с акцентами и без таковых) и операторные символы. Например, буква $x$ является лексемой, буквосочетание cos — тоже лексема, знак интеграла — тоже лексема, и т.д. Но в дальнейшем мы условимся в виде исключения из правил (хотя математики не любят исключений!) чисто из эстетических соображений не считать лексемами несамостоятельные элементарные графемы.

Наконец, отметим еще один замечательный факт: если в производный шаблон вместо пробелов подставить производные же шаблоны, то мы получим производный шаблон. Оформим это дедуктивное соображение как теорему.

**Теорема D1.1.** *Производные шаблоны образуют множество графем, замкнутое относительно операции подстановки.*

Проверить это свойство довольно просто, сведя замкнутость операции подстановки на производных шаблонах к аналогичной операции на подстановочных шаблонах. А для последних замкнутость гарантирована определением.

Продемонстрируем эту теорему на примере. Пусть у нас имелся шаблон ⊔(⊔), затем мы получили из него производный шаблон sin(⊔), а затем в этот производный шаблон подставили его же самого, и получили в результате конструкцию: sin(sin(⊔)). Почему такая конструкция является производным шаблоном?

Для ответа на этот вопрос мы переходим от подстановки производного шаблона в производный к подстановке шаблона в шаблон. Именно, подставим ⊔(⊔) в самого себя на второе подстановочное место, в результате получим новый шаблон ⊔(⊔(⊔)). Из этого шаблона путем подстановки жесткой графемы sin на первые два места получим требуемый производный шаблон.

Иначе говоря, мы можем как угодно подставлять друг в друга шаблоны и производные шаблоны, не выходя за рамки разрешенных конструкций!

Отсюда, в частности, следует, что в производный шаблон мы можем подставлять какие угодно лексемы, и в результате получим производный шаблон, а если при этом не останется свободных подстановочных мест, то мы получим новую лексему. В частности, пользуясь производным шаблоном sin(⊔) и лексемой $i\sqrt{\pi}$, которая получается из шаблона операции умножения ⊔ ⊔ и шаблона квадратного корня $\sqrt{⊔}$, мы можем получить новую лексему $\sin(i\sqrt{\pi})$.

Таким вот хитрым путем, с применением рекурсивного определения, мы достигли главного описательного определения языка Math — понятия *лексемы*. Весь текст, на-

писанный на языке Math — это и есть последовательность корректно построенных лексем!

На рис. D1.1 приведена краткая схема образования лексем из алфвита с помощью описанных нами методов.

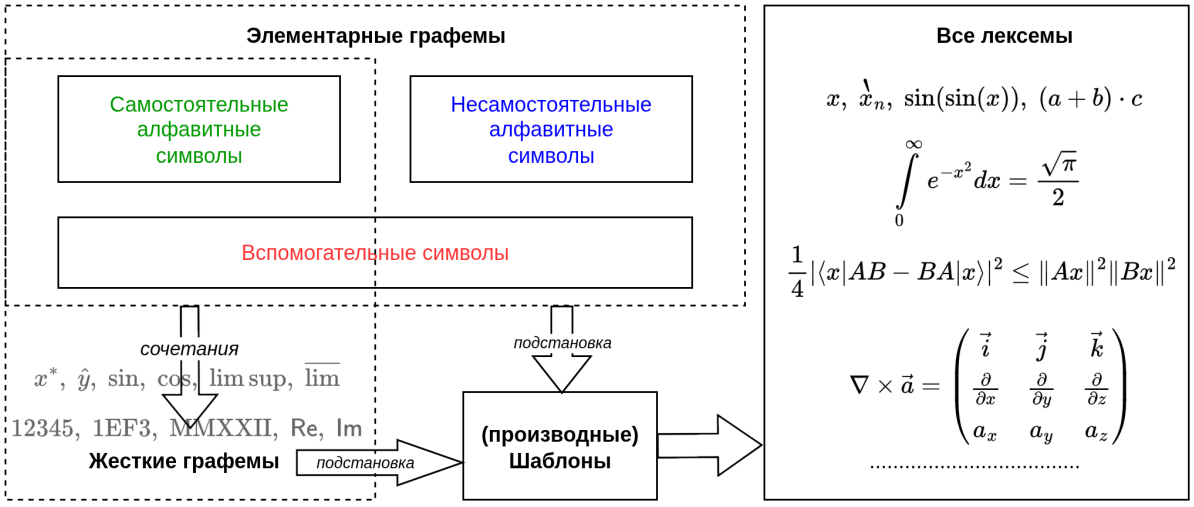



Рис. D1.1. Схема построения лексем.

## D1.3. Синтаксический разбор

Подстановочные шаблоны — это, пожалуй, главный и самый удобный инструмент «текстостроения» в языке Math. Во-первых, он прекрасен тем, что его очень просто описать и использовать — бери и комбинируй шаблоны по принципу матрешки. Во-вторых, любую лексему, построенную с помощью подстановочных шаблонов, можно представить в виде так называемого **дерева разбора**, из которого видно, как именно строилась данная лексема. Правда, одной лексеме может соответствовать несколько вариантов дерева разбора, и чтобы это исключить, в формальных языках правила построения текстов становятся более жесткими, чем в нашем общем варианте языка Math.

Именно эта жесткость делает формальные языки доступными для машинной обработки. В лингвистике и информатике существует так называемая иерархия Хомского, которая классифицирует формальные языки по сложности их грамматики. Простейшие из них, регулярные языки, описывают простые шаблоны, в то время как более сложные, контекстно-свободные языки, способны описывать вложенные структуры, подобные тем, что мы видим в арифметических выражениях со скобками или в языках программирования. Дерево разбора является ключевым инструментом именно для анализа контекстно-свободных грамматик, на которых основано большинство языков, «понятных» компьютеру.

Пример дерева разбора одной известной формулы показан на рис. D1.2.

Для удобства конечный результат, т.е. сама разбиремая лексема, помещена в корень дерева. Как видим, в основном мы используем здесь производные шаблоны с двумя или одним подстановочными местами (оператор равенства, дробь, степень, корень, оператор отрицания), но есть также один более сложный производный шаблон для создания интегрального выражения с четырьмя подстановочными местами. Дерево разбора, как

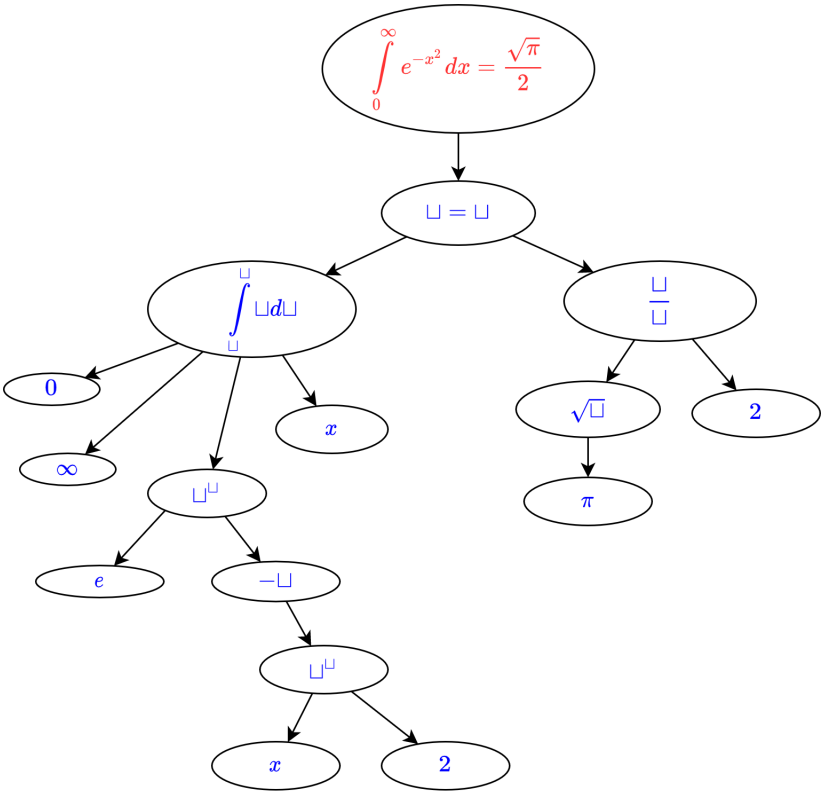



Рис. D1.2. Дерево разбора для формулы Пуассона.

и положено, заканчивается листьями (узлами без потомков), в которых стоят жесткие графемы, представленные основными графемами (цифры 0 и 2, буквы $e$, $x$, $\pi$ и спецсимвол $\infty$).

Отметим, что данное дерево можно еще больше детализировать, если не использовать в нем никакие шаблоны, кроме простых подстановочных шаблонов. В этом случае у дерева появятся листья, содержащие операторные символы (в нашем случае это интеграл, равенство, дробь и квадратный корень). Однако такое дерево будет очень плохо читаемым, т.к. шаблоны с операторными символами (например, интеграл и корень) позволяют с первого взгляда понять их семантику. Кроме того, производные шаблоны с операторами соответствуют конкретным математическим понятиям, что также делает их более привлекательными для использования в синтаксическом разборе лексемы.

Понимание внутренней структуры формулы через дерево разбора — не просто упражнение в визуализации. Это фундаментальный принцип, используемый компьютерными системами для обработки математических языков и языков программирования. Компиляторы строят такие деревья (абстрактные синтаксические деревья, AST), чтобы переводить читаемый человеком код в машинные инструкции; системы компьютерной алгебры (CAS) опираются на них при символьных преобразованиях вроде интегрирования или упрощения; а современные модели искусственного интеллекта используют аналогичные структурные представления, чтобы «понимать» и порождать корректные математические тексты.

В приведенном примере мы обошлись без символов-группираторов, т.е. без скобок, поэтому в качестве самостоятельного упражнения читателю предлагается построить

дерево разбора для неравенства Робертсона–Шрёдингера:

$$\frac{1}{4}|\langle x|AB-BA|x\rangle|^2 \leqslant \|Ax\|^2\|Bx\|^2,$$

используя производные шаблоны с операторными символами.

## D1.4. Упрощения

Выше мы описали построение лексем языка $\mathfrak{Math}$ в том виде, как это принято в математике. Однако мы можем заметить, что этот язык можно существенно упростить, если в качестве простых шаблонов рассматривать только линейные шаблоны вида

$$\sqcup(\sqcup,\dots,\sqcup).$$

Действительно, каким бы сложным и многомерным ни был шаблон, он представляет собой некоторое количество подстановочных мест, связанных определенной «геометрией». Сколько бы ни было таких шаблонов, их всех можно пронумеровать специально придуманными для такого дела жесткими графемами вида Sch1, Sch2, Sch3 и т.д. Кроме того, в каждом из них можно определить некоторый порядок заполнения подстановочных мест, например, в шаблоне для интеграла мы скажем, что сначала пишется знак интеграла, затем — нижний предел, затем — верхний, затем — подынтегральная функция, затем буква $d$, и в конце — переменная интегрирования.

Это значит, что вместо того огромного зоопарка шаблонов, которые мы обрисовали ранее, мы можем оставить лишь линейные шаблоны вида:

$$\mathrm{Sch1}(\sqcup,\dots,\sqcup),\quad \mathrm{Sch2}(\sqcup,\dots,\sqcup),\quad \mathrm{Sch3}(\sqcup,\dots,\sqcup),\quad \dots$$

Более того, мы можем проделать такую операцию с большинством производных шаблонов (кроме лексем), так что весь язык у нас будет состоять исключительно из лексем, которые получаются путем подстановки жестких графем в шаблоны указанного вида. По сути мы получим язык, где всякая лексема — это польская запись функции с аргументами, например,

$$\mathrm{Sch1}(a,b,c),\quad \mathrm{Sch2}(\textstyle\int,0,\infty,\mathrm{Sch4}(\sin,x),d,x),\quad \mathrm{Sch3}(\sqrt{\ },\mathrm{Sch5}(+,i,\lambda).$$

Наконец, мы можем упростить и эти шаблоны, договорившись о том, что у нас в алфавите есть только одна буква $x$, одна цифра 0, один спецсивол $\lambda$, одна пара группираторов (круглые скобки), один разделитель (запятая), один вспомогательный символ (штрих) и бесконечный набор названий шаблонов Sch11, Sch11, Sch111 и т.д. При этом самостоятельные производные графемы мы будем получать путем неограниченного добавление штриха к букве $x$ и к цифре 0, все производные операторы — путем неограниченного добавления штриха к символу $\lambda$, а также договоримся о том, что в шаблоне мы всегда сначала подставляем буквенные графемы, затем цифровые, затем операторные. Тогда лексемы нашего ужасно упрощенного языка примут следующий вид

$$\mathrm{Sch1...1}(x,x'',x'''',\dots,0'',0''',\dots,\lambda''',\lambda'''',\dots).$$

Мы получим очень простой, эквивалентный нашему языку Math, но жутко нечитабельный язык, который удобен для анализа языка, как предмета исследований, но неудобен для практического применения.

Такой метод упрощения (редукции) языка часто используется именно для анализа выразительных возможностей языка, для доказательства некоторых общих синтаксических свойств. Например, имея дело с таким упрощенным вариантом языка Math, нам было бы гораздо легче доказывать теорему D1.1 о замкнутости производных шаблонов относительно операции подстановки. Честно говоря, мы примерно так и поступили, «доказав» эту теорему на примере простейшего шаблона $\sin(\sqcup)$.

## D1.5. Графика

В начале разговора о языке Math мы отмечали, что помимо текстов язык допускает дополнительные графические изображения. Сразу же заметим, что любые графические материалы в математике — это лишь иллюстрация понятий, отношений, идей и т.д. Никакое рассуждение в математике не будет принято за доказательство, если оно опирается только на «графику».

Конечно, бывают исключительные случаи, когда объяснить доказательство «на пальцах» сильно легче, чем записать его формальный текст, но в таких случаях предполагается, что любой адресат такого доказательства однозначно и полностью сможет восстановить формальные рассуждения, спрятанные под иллюстрацией. С такой ситуацией мы часто сталкиваемся в простых геометрических задачах, где какое-нибудь дополнительное построение или вращение фигур подсказывает идею доказательства и выводит нас на ранее доказанные теоремы геометрии.

Тем не менее, любой иллюстративный материал в математике следует считать не более чем вспомогательным.

Какого же рода графический материал мы можем отметить? Дадим такую классификацию:

- геометрические построения в планиметрии и стереометрии;
- конечные или счетные графы;
- диаграммы Венна–Эйлера;
- коммутативные диаграммы;
- графики;
- таблицы и диаграммы.

Типы вспомогательных графических материалов расположены в порядке убывания их значимости для доказательной базы рассуждений в математике (по мнению автора).

Возникает вопрос: если графические элементы мы все-таки считаем частью языка Math, то как же они вписываются во все предыдущие построения? Ведь очевидно, что никакой лексемой их не задать.

Да, с одной стороны так и есть, и содержательно передать структуру, например, графика функции с асимптотами с помощью производных шаблонов и жестких графем вряд ли возможно. Однако если подойти к делу чисто синтаксически, то придумывается как минимум два подхода.

Первый подход состоит в том, что всякий график, будучи отрисован компьютерным способом, является конечной матрицей, в ячейках которой стоят нули или единицы (ноль — ячейка белая, единица — черная). Иначе говоря, всякий рисунок можно считать пиксельной матрицей, и тогда мы можем задать его простейшим матричным шаблоном, заполняя его подстановочные места только там, где должны быть черные точки нашего рисунка. Проблема в том, что такой подход является чересчур общим, ведь таким способом можно изобразить не только график функции с асимптотами, но также портрет Моны Лизы и любую формулу языка Math. При этом напрочь потеряется синтаксическая структура текста, ведь в дереве разбора будет присутствовать только один шаблон (матрица) и листья-единички, которые проставлены в некоторых ячейках этой матрицы. Ясно, что потерять структуру нам бы совсем не хотелось. Поэтому такой путь мы будем считать тупиковым.

Второй подход заключается в том, что мы можем разрешить добавлять к любым шаблонам любые графические подложки (фоновые изображения). Тогда у нас получится некий гибрид шаблонов и графики, причем шаблон будет отвечать за то, в какие места на картинке можно вставлять лексемы, чтобы заполнить график необходимыми текстовыми вставками. Правда, при этом следует принять правило, что шаблоны с разными фонами следует считать разными, даже если количество и взаимное расположение в нем подстановочных мест, скобок и разделителей одинаковое.

Однако и во втором подходе есть ряд неудобных проблем. Например, никто не мешает нам взять график параболы в фоновом изображении, а в подписях при помощи шаблона вписать тот же синус, в результате чего такая графическая лексема получится противоречивой. Увязать же чисто текстовые лексемы с графической подложкой без специальных программных средств уже не получится. А это означает, в свою очередь, что внутри языка Math нам потребуется построить некоторое специальное подмножество лексем, которые будут представлять собой некоторый язык программирования, позволяющий строить графики функций, и только после этого можно будет определить специальный вид шаблонов (вычисляющие, рисующие шаблоны), которые будут «понимать» вписанный в определенную ячейку текст как программный код и с его помощью строить фоновое изображение в виде графика функции или чего-либо еще, что можно задать аналитически на эвклидовой координатной плоскости.

Короче говоря, это путь непростой, но продуктивный. И все же мы в рамках книги будем придерживаться той парадигмы, которую мы обозначили выше, а именно, что *весь иллюстративный материал мы считаем чисто вспомогательным и не считаем его частью языка* Math. Хотя, повторимся, определенные возможности для реализации графики у нашего языка имеются.

Кстати говоря, таблицы, которые оказались у нас на последнем месте по значимости для математики, реализовать с помощью шаблонов намного проще, чем все остальные графические материалы, поскольку таблица — это по сути матричный шаблон, причем вполне осмысленный в отличие от пиксельной матрицы, которую мы упоминали выше. Но таблицы в математике если чему и помогают, то, разве что, красиво подать или суммировать некоторую уже доказанную классификацию каких-либо объектов и понятий. Придти же к этой классификации или доказать о ней некоторые факты таблицы не позволяют.

## D1.6. Определение переменных

Ранее мы упоминали некоторые аналогии языка $\mathfrak{Math}$ с разговорными языками. В частности, операторные графемы можно считать аналогами глаголов, поскольку они как правило обозначают действия, а буквенно-цифровые жесткие графемы — аналогами имен существительных, причем однобуквенные — нарицательных, многобуквенные — собственных.

На самом деле, конечно, все не так однозначно, поскольку операторы могут обозначаться далеко не только операторными графемами, а точнее, они всегда производятся при помощи производных шаблонов, содержащих операторные графемы. Например, уже знакомый нам шаблон для определенного интеграла собирается из операторного символа интеграла и резервирует свободные места для пределов интегрирования, подынтегральной функции и переменной интегрирования. Кроме того, к операторным шаблонам можно отнести и ряд таких шаблонов, в которых используются жесткие графемы в качестве обозначения оператора. Например, sin — это жесткая графема (аналог существительного), а $\sin(\sqcup)$ — операторный шаблон для записи функции синуса.

Не проще дело обстоит с корректным сопоставлением имен собственных и нарицательных с лексемами языка $\mathfrak{Math}$. Во-первых, не только жесткие графемы, но и некоторые лексемы могут быть именами собственными. Прежде всего, такие лексемы–имена собираются из жестких графем и цифровых индексов. Например, стандартное обозначение первого бесконечного кардинала $\aleph_0$ есть лексема, полученная из буквы и цифрового индекса с помощью шаблона $\sqcup_{\sqcup}$. С точки зрения обычного языка $\aleph_0$ — это имя собственное, поскольку за этим обозначением закрепляется единственный на всю математику объект. Можно было бы сказать, что имена собственные — это обозначения констант, но и тут аналогия будет неполной, поскольку мы в математике очень часто используем временные обозначения для констант.

Наконец, нарицательные имена у нас также могут быть не только жесткими графемами, но и лексемами, поскольку очень часто мы используем нумерованные имена переменных.

Рассмотрим подробнее случай лексем, которые служат для обозначения **переменных**, т.е. аналогов имен нарицательных разговорного языка. В большинстве случаев (в математике — практически в 100% случаев) имена переменных задаются следующими способами:

V1 однобуквенная основ́ная графема, т.е. попросту буква, чаще латинского или греческого алфавита;

V2 однобуквенная производная графема, т.е. буква с одной или несколькими вспомогательными графемами;

V3 лексема, полученная подстановкой в шаблон $\sqcup_{\sqcup}$ на первое место — однобуквенной графемы, на второе место — цифровой графемы.

Примеры переменных: $x, y, z, \hat{x}, y_1, z''_{100}$. Конечно, не все такие лексемы используются как переменные, среди них есть и собственные имена, но они как правило выделяются особым начертанием. К таковым можно отнести обозначения числовых множеств $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, символа вероятности $\mathrm{P}$, ординала $\omega$ и некоторые другие.

В формальных языках (в частности, языках программирования) очень часто приходится разделять переменные по типам. Во-первых, как мы уже отмечали в первой части

книги, переменные можно разделить на связанные и свободные. Связанные переменные служат для определения сверток, т.е. таких лексем, которые несут в себе некое итеративное описание объекта, например, множество $\{x \mid \mathscr{A}(x)\}$ или формула $\forall x\ \mathscr{A}(x)$. Свободные переменные — это параметры, они служат для описания одной лексемой целого класса объектов, каждый из которых получается заменой всех параметров на какие-то константы.

Во-вторых, все переменные (как свободные, так и связанные) можно разделить на несколько типов, запрещая тем самым при построении лексем подставлять что угодно куда угодно. Например, у нас могут быть строковые и числовые переменные (язык программирования), либо же переменные для натуральных чисел и множеств натуральных чисел (арифметика второго порядка). Такая типизация ограничивает свободу лексемостроения в языке Math под нужды конкретного формализма.

Свободные переменные можно рассматривать как поименованные подстановочные места в шаблонах. В этом смысле шаблон можно воспринимать как частный случай лексемы. При этом переменные имеют преимущество перед пустыми подстановочными местами, поскольку позволяют некоторые из этих мест отождествить. Действительно, глядя на шаблон $\langle \sqcup, \sqcup, \sqcup \rangle$, мы лишь видим возможность собрать лексему из трех произвольных обозначений, не акцентируя внимания на том, что при этом получится и насколько оно соответствует нашим целям. Если же мы напишем лексему $\langle x, x, y \rangle$, то мы уже понимаем, что на первые два места можно подставить только что-то одно, поскольку вместо одинаковых переменных нужно подставлять одинаковые лексемы. Более того, если переменным присвоен тип, то мы сразу же понимаем какого типа объекты можно подставлять вместо них в данную лексему.

Обычно саму процедуру подстановки лексемы вместо переменной принято записывать так: $[x/a]$ (заменить $x$ на $a$). Это не что иное как обозначение *синтаксического оператора подстановки*, который сообщает нам в тексте, что в лексеме, предшествующей данному оператору, переменную $x$ следует всюду заменить на лексему $a$. В логике и математических теориях (см. дальше) мы будем использовать его в более конкретном понимании лексем и переменных.[4]

Наличие типов у переменных одновременно обязывает и все лексемы распределить по этим же типам, иначе мы просто не сможем лексемы подставлять вместо переменных. Поэтому при описании любого формализма наряду с конкретными правилами построения лексем через шаблоны нужно также указывать тип получаемых лексем. Обычно в математике все лексемы делятся на формулы и термы. **Формулы** — это лексемы логического типа (значение бывает либо истинным, либо ложным), а **термы** — это лексемы объектного типа, предназначенные для обозначения исследуемых объектов. Термы, в свою очередь, могут делиться на типы, те самые числа и строки, числа и множества и т.д.

Учитывая все вышесказанное, отметим, что хоть шаблоны с подстановочными местами и являются базовыми единицами построения лексем, в определении каждого конкретного формализма используется более продвинутая технология, а именно: *типизованные лексемы*. Они представляют собой лексемы со свободными переменными, причем как для этих переменных, так и для самой лексемы задан определенный тип. Набор этих типов называется *сигнатурой* типизованной лексемы. Например, лексема $a + b$ в арифметике сопровождается следующей сигнатурой: $a, b$ — натуральные числа,

[4] В некоторых источниках используется симметричная нотация оператора замены: $[a/x]$ ($a$ вместо $x$).

Таблица D1.2. Переменные и константы

| | Переменные | Собственные названия |
|---|---|---|
| Определение | общее обозначение для элементов класса | обозначение конкретного объекта |
| Структура | однобуквенные жесткие графемы [+ цифровые индексы] | многобуквенные (редко — однобуквенные) жесткие графемы [+ цифровые индексы] |
| Для чего | свертки и параметры | обозначения функций, операторов, множеств, классов |
| Разговорный язык | имена нарицательные, местоимения | имена собственные |
| Примеры | $x$, $y$, $\hat{z}$, $t_1$, $w'_2$ | sin, P, $\aleph_0$, $\mathbb{Z}$, Ord |

результат $a + b$ — тоже натуральное число. В языке Python явное указание сигнатуры при определении функции вводится следующим способом:

```
def Func(x: int, y:str)->bool:
```

Здесь **int**, **str**, **bool** составляют сигнатуру функции Func.

В завершение приведем сравнительную таблицу переменных и констант (собственных названий объектов) — см. таблицу D1.2.

## D1.7. Упражнения

**Ex1.** Классифицируйте следующие элементарные графемы по типу (самостоятельные/несамостоятельные, осно́вные/производные): a) $\pi$; b) $\subseteq$; c) $\hat{y}$; d) $\nabla$; e) $\{\}$.

**Ex2.** Определите тип следующих элементарных графем (осно́вная/производная, самостоятельная/несамостоятельная, оператор/разделитель и т.д.): a) $\Sigma$ (заглавная греческая сигма); b) $\sum$ (символ суммирования); c) $\overline{z}$ (переменная с баром); d) ; (точка с запятой); e) $\to$ (стрелка).

**Ex3.** Какие из следующих графем считаются жесткими (синтаксически неделимыми именами)? a) arctan; b) $x_1$; c) $a + b$; d) const.

**Ex4.** Найдите подстановочные места в следующих шаблонах. Сколько аргументов принимает каждый шаблон?

1. $\lim_{\sqcup\to\sqcup}\sqcup$;
2. $\log_{\sqcup}\sqcup$;
3. $|\sqcup|$;
4. $\frac{\partial\sqcup}{\partial\sqcup}$.

**Ex5.** Постройте дерево разбора для формулы логистической функции (сигмоиды):

$$\sigma(x) = \frac{1}{1 + e^{-x}},$$

используя производные шаблоны для деления, сложения, возведения в степень и отрицания.

**Ex6.** Преобразуйте следующие двумерные шаблоны в линейный формат (например, польскую запись или вызовы функций вида ‘Template(arg1, arg2...)’).

1. $\frac{a}{b}$;
2. $a^b$;
3. $\sqrt[n]{x}$.

**Ex7.** Переведите стандартное арифметическое выражение $(a + b) \cdot (c - d)$ в:

1. Префиксную нотацию (польскую запись);
2. Постфиксную нотацию (обратную польскую запись).

**Ex8.** Выполните операцию синтаксической подстановки $[x/T]$ для следующих лексем:

1. $(a + x) \cdot y$, где $T \stackrel{\text{def}}{\rightleftharpoons} \sin(\omega t)$;
2. $\int_0^x f(t)dt$, где $T \stackrel{\text{def}}{\rightleftharpoons} x^2$ (примечание: различайте свободные и связанные переменные в контексте типичной математической записи, хотя формально в шаблоне это просто знакоместа);
3. $P(x, y) \to Q(x)$, где $T \stackrel{\text{def}}{\rightleftharpoons} g(z)$.

**Ex9.** Пусть $T \stackrel{\text{def}}{\rightleftharpoons} f(u)$. Выполните синтаксическую подстановку $[x/T]$ в следующих лексемах. Убедитесь, что скобки добавлены там, где это необходимо для сохранения приоритета операций.

1. $x^2$;
2. $\sin(2 \cdot x)$;
3. $D_x$ (оператор производной, действующий по $x$).

**Ex10.** Мы утверждали, что «подстановка лексемы в производный шаблон порождает лексему». Продемонстрируйте это, подставив лексему $2k + 1$ в производный шаблон $\sum_{k=0}^{\infty} \sqcup$.

**Ex11.** Определите сигнатуру (типы переменных и результата) для следующих типизированных лексем:

1. $\vec{a} \cdot \vec{b}$ (скалярное произведение);
2. $\|\vec{x}\|$ (норма);
3. $A \subset B$.

**Ex12.** Определите сигнатуру для следующих операторов в контексте стандартной векторной алгебры (где $S$ — скаляр, $V$ — вектор):

1. Оператор $\cdot$ (скалярное произведение);
2. Оператор $\times$ (векторное произведение);
3. Оператор $\cdot$ (умножение на число, например, $\alpha\vec{v}$);
4. Оператор $|\sqcup|$ (модуль/длина).

**Ex13.** Рассмотрим лексему $\sin x + y$.

1. Нарисуйте дерево разбора, соответствующее интерпретации $(\sin x) + y$.
2. Нарисуйте дерево разбора, соответствующее интерпретации $\sin(x + y)$.
3. Какой вариант является стандартным соглашением?

**Ex14.** Пусть определение «Списка» таково:

1. () — это Список.
2. Если $L$ — Список, а $a$ — атом, то $(a, L)$ — это Список.

Сконструируйте список, содержащий атомы $1, 2, 3$, используя это определение.

**Ex15.** Сконструируйте три различные производные графемы на основе буквы $x$, используя разные вспомогательные символы (акценты, индексы).

**Ex16.** В логической формуле $\forall x(P(x) \to Q)$, определите типы лексем:

1. $x$;
2. $P(x)$;
3. $\to$;
4. $\forall x(\dots)$.

(Варианты: свертка, переменная, формула, логическая связка).

**Ex17.** Дана логическая лексема $\neg\mathscr{A} \wedge \mathscr{B} \to \mathscr{C}$. Расставьте скобки, чтобы отразить стандартный порядок операций в логике (Отрицание > Конъюнкция > Импликация).

**Ex18.** В лексеме $\int_a^b x^2 dx$ замените связанную переменную $x$ на $t$. Изменится ли смысл лексемы? А если заменить $x$ на $a$?

**Ex19.** Декомпозируйте (разберите) лексему $\sum_{i=1}^{n} x_i^2$ на составляющие её элементарные графемы и простые шаблоны.

## Рекомендуемая литература

Поскольку центральной темой нашей книги является взгляд на математику как на язык, обзор литературы стоит построить вокруг двух его ипостасей: математического языка как строгого формального исчисления и как феномена, тесно связанного с естественными языками и человеческим мышлением.

Историческим столпом, на котором зиждется современное представление о формализации, является монументальный двухтомник Гильберта и Бернайса «Основания математики» [24]. Эта работа, выросшая из знаменитой программы Гильберта, представляет собой исчерпывающе детальную попытку построить здание математики на прочном синтаксическом фундаменте. Хотя сегодня ее стиль может показаться громоздким, это первоисточник, к которому так или иначе восходят все современные изложения.

Педагогически выверенное и каноническое развитие этих идей можно найти в фундаментальном труде Стивена Клини «Введение в метаматематику» [28]. Именно здесь с непревзойденной тщательностью проводится различие между языком-объектом и метаязыком, что напрямую перекликается с нашим «принципом матрешки» и рекурсивным определением лексем. Книга Клини на десятилетия стала золотым стандартом в преподавании основ математической логики.

Совершенно иную перспективу, связывающую математику и лингвистику, предлагает сборник статей и эссе выдающегося математика Владимира Успенского «Предисловие к математике» [14]. В нем в доступной и увлекательной форме раскрываются многие философские и структурные аспекты математического языка. Для понимания же истоков формального подхода к синтаксису, повлиявшего и на логику, и на информатику, необходимо обратиться к революционной работе лингвиста Ноама Хомского «Синтаксические структуры» [65], где были введены понятия порождающей грамматики и иерархии формальных языков, которые напрямую перекликаются с введенным в этой главе методом построения лексем из графем при помощи шаблонов и стали сегодня неотъемлемой частью Computer Science.

# ГЛАВА D2
# Логика

*Wir müssen wissen — wir werden wissen.*
*(Мы должны знать — мы будем знать.)*

— Давид Гильберт

## D2.1. Логика высказываний

Логика высказываний (или исчисление высказываний) — один из самых простых формализмов. Его задача — максимально абстрактно описать логические связки между аргументами, не предполагая какую-либо, кроме истинностной, зависимость этих аргументов. Поэтому алфавит системы состоит из так называемых пропозициональных переменных $\mathscr{A}, \mathscr{B}, \mathscr{C}, \ldots$, которые могут снабжаться индексами (чтобы количество переменных было потенциально бесконечным для реализации сколь угодно длинных формул), символов логических связок $\wedge, \vee, \neg, \to, \leftrightarrow, \uparrow$ и скобок. Мы сразу добавили в язык еще две связки ($\leftrightarrow$ и $\uparrow$), чтобы включать их в формулы без дополнительных соглашений.

Формулами данной теории является минимальное множество текстов в данном алфавите, замкнутое относительно композиции связок и формул. Подробно сам язык и правила редукции скобок мы обсуждали в разделе B1.1.2.

У логики высказываний существует несколько разновидностей моделей, одна из которых (стандартная) — это булевы функции вида $f : \{0,1\}^n \to \{0,1\}$. Оценивая пропозициональные переменные числами 0 или 1 и вычисляя значение логических связок по таблице истинности D2.1, мы получаем оценку числом 0 или 1 для любой формулы. Таким образом каждой формуле сопоставляется булева функция (единственная с точностью до нумерации ее переменных).

Таблица D2.1. Таблица истинности для логических связок

| $\mathscr{A}$ | $\mathscr{B}$ | $\neg\mathscr{A}$ | $\mathscr{A}\wedge\mathscr{B}$ | $\mathscr{A}\vee\mathscr{B}$ | $\mathscr{A}\to\mathscr{B}$ | $\mathscr{A}\leftrightarrow\mathscr{B}$ | $\mathscr{A}\uparrow\mathscr{B}$ |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 |
| 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 |

Формулы, которые при любой оценке переменных дают в результате 1, называются *тавтологиями*. Например, формулы $\mathscr{A}\vee\neg\mathscr{A}$ и $\mathscr{A}\to\mathscr{A}$ являются тавтологиями. Тавтология $\mathscr{A}\vee\neg\mathscr{A}$ часто заменятеся символом $\top$ (*истина*), а тождественно ложная формула $\mathscr{A}\wedge\neg\mathscr{A}$ заменяется символом $\bot$ (*ложь*), они используются как символы-константы в

языке логики высказываний. Формулы называются *равносильными*, если они оцениваются одинаковыми булевыми функциями. Для записи равносильности формул мы используем метауровневый предикат $\equiv$. Таким образом тавтологии — это все формулы, равносильные $\top$. Вот несколько примеров равносильностей:

- закон двойного отрицания: $\neg\neg\mathscr{A} \equiv \mathscr{A}$;
- ассоциативность конъюнкции и дизъюнкции:

$$((\mathscr{A} \wedge \mathscr{B}) \wedge \mathscr{C}) \equiv (\mathscr{A} \wedge (\mathscr{B} \wedge \mathscr{C})), \quad ((\mathscr{A} \vee \mathscr{B}) \vee \mathscr{C}) \equiv (\mathscr{A} \vee (\mathscr{B} \vee \mathscr{C})); \tag{D2.1}$$

- коммутативность конъюнкции и дизъюнкции:

$$(\mathscr{A} \wedge \mathscr{B}) \equiv (\mathscr{B} \wedge \mathscr{A}), \quad (\mathscr{A} \vee \mathscr{B}) \equiv (\mathscr{B} \vee \mathscr{A}); \tag{D2.2}$$

- дистрибутивность конъюнкции и дизъюнкции:

$$(\mathscr{A} \wedge (\mathscr{B} \vee \mathscr{C})) \equiv ((\mathscr{A} \wedge \mathscr{B}) \vee (\mathscr{A} \wedge \mathscr{C})), \quad (\mathscr{A} \vee (\mathscr{B} \wedge \mathscr{C})) \equiv ((\mathscr{A} \vee \mathscr{B}) \wedge (\mathscr{A} \vee \mathscr{C})); \tag{D2.3}$$

- равносильности с константами:

$$\mathscr{A} \wedge \top \equiv \mathscr{A}, \quad \mathscr{A} \vee \top \equiv \top, \quad \mathscr{A} \vee \bot \equiv \mathscr{A}, \quad \mathscr{A} \wedge \bot \equiv \bot \tag{D2.4}$$

- идемпотентность[1] конъюнкции и дизъюнкции:

$$(\mathscr{A} \wedge \mathscr{A}) \equiv \mathscr{A}, \quad (\mathscr{A} \vee \mathscr{A}) \equiv \mathscr{A};$$

- законы поглощения:

$$\mathscr{A} \vee (\mathscr{A} \wedge \mathscr{B}) \equiv \mathscr{A}, \quad \mathscr{A} \wedge (\mathscr{A} \vee \mathscr{B}) \equiv \mathscr{A};$$

- другие равносильности:

$$(\mathscr{A} \to \mathscr{B}) \equiv (\neg\mathscr{A} \vee \mathscr{B}), \quad (\mathscr{A} \leftrightarrow \mathscr{B}) \equiv ((\mathscr{A} \to \mathscr{B}) \wedge (\mathscr{B} \to \mathscr{A})), \tag{D2.5}$$

$$\neg(\mathscr{A} \wedge \mathscr{B}) \equiv \neg\mathscr{A} \vee \neg\mathscr{B}, \quad \neg(\mathscr{A} \vee \mathscr{B}) \equiv \neg\mathscr{A} \wedge \neg\mathscr{B}, \quad (\mathscr{A} \to \mathscr{B}) \equiv (\neg\mathscr{B} \to \neg\mathscr{A}),$$

$$\mathscr{A} \uparrow \mathscr{B} \equiv \neg(\mathscr{A} \wedge \mathscr{B}), \quad \neg\mathscr{A} \equiv \mathscr{A} \uparrow \mathscr{A},$$

$$\mathscr{A} \vee \mathscr{B} \equiv (\mathscr{A} \uparrow \mathscr{A}) \uparrow (\mathscr{B} \uparrow \mathscr{B}), \quad \mathscr{A} \wedge \mathscr{B} \equiv (\mathscr{A} \uparrow \mathscr{B}) \uparrow (\mathscr{A} \uparrow \mathscr{B}).$$

Кроме того, верно следующее утверждение: $\varphi \leftrightarrow \psi$ является тавтологией тогда и только тогда, когда $\varphi \equiv \psi$ (или так: $(\varphi \leftrightarrow \psi) \equiv \top \Leftrightarrow \varphi \equiv \psi$). А также верен принцип замены подформулы на равносильную: если $\psi_1 \equiv \psi_2$, то $\varphi[\mathscr{A}/\psi_1] \equiv \varphi[\mathscr{A}/\psi_2]$.[2]

Из приведенных равносильностей, в частности, видно, что все булевы связки можно выразить через пару связок $\neg, \wedge$ или $\neg, \vee$ или $\neg, \to$, либо же через одну связку $\uparrow$, которая называется *штрих Шеффера*.

[1] Слово означает равносильность (*лат. idem potens*) всех степеней операции.

[2] Это достаточно просто установить, пользуясь индукцией по построению формул.

**Теорема D2.1** (о функциональной полноте)**.**
*Всякой булевой функции* $f : \{0,1\}^n \to \{0,1\}$ *соответствует формула с* $n$ *переменными, оценка которой совпадает с этой функцией.*

*Доказательство.* Пусть задана функция $f : \{0,1\}^n \to \{0,1\}$ и пропозициональные переменные $\mathscr{A}_1, \dots, \mathscr{A}_n$. Необходимо построить такую формулу $\varphi$ от этих переменных, что для любой оценки $\varepsilon$ выполнялось бы тождество $f \circ \varepsilon = \varepsilon(\varphi)$.

Если $f$ тождественно равна 0, то возьмем формулы $\mathscr{A}_k \wedge \neg\mathscr{A}_k$, $k = 1, \dots, n$, и соединим их, например, дизъюнкцией.

Пусть $f$ принимает значение 1 на непустом множестве $X$ наборов $\vec{x}$. Определим степень переменной (или, как говорят, *литерал*):

$$\mathscr{A}^x = \begin{cases} \mathscr{A}, & x = 1, \\ \neg\mathscr{A}, & x = 0. \end{cases}$$

После чего рассмотрим формулу

$$\varphi \overset{\text{def}}{\leftrightarrow} \bigvee_{\vec{x} \in X} (\mathscr{A}_1^{x_1} \wedge \dots \wedge \mathscr{A}_n^{x_n}). \tag{D2.6}$$

Проверим, что оценки этой формулой совпадают с функцией $f$. Пусть $\varepsilon(\mathscr{A}_k) = x_k$. Если $\vec{x} \in X$, т.е. $f(\vec{x}) = 1$, то оценка конъюнкции, соответствующей $\vec{x}$, равна

$$\varepsilon(\mathscr{A}_1^{x_1} \wedge \dots \wedge \mathscr{A}_n^{x_n}) = x_1^{x_1} \wedge \dots \wedge x_n^{x_n} = 1,$$

откуда вся дизъюнкция в определении $\varphi$ также оценивается 1.

Если же $\vec{x} \notin X$, т.е. $f(\vec{x}) = 0$, то для каждого $\vec{y} \in X$ существует такой $k$, что $x_k \neq y_k$, откуда $x_k^{y_k} = 0$, откуда $x_1^{y_1} \wedge \dots \wedge x_n^{y_n} = 0$. А значит, все конъюнкции в определении $\varphi$ оцениваются нулем.

Таким образом при любой оценке $\varepsilon$ оценка формулы $\varphi$ совпадает с значением $f$ при сопоставлении переменной $\mathscr{A}_k$ с $k$-ым аргументом $f$. □

Представление формулы в виде (D2.6) называется дизъюнктивной нормальной формой (ДНФ). Из теоремы следует, что любая формула логики высказываний имеет представление в виде ДНФ.

Все тавтологии логики высказываний можно получить из аксиом, используя два правила вывода: подстановку (B1.6) и Modus Ponens (B1.7). Напомним, что правило подстановки применяется только к тавтологиям, в то время как MP можно применять к любым гипотезам.

Следующий список есть классическая аксиоматика логики высказываний:

A1 введение импликации: $\mathscr{A} \to (\mathscr{B} \to \mathscr{A})$;

A2 аксиома Фреге: $(\mathscr{A} \to (\mathscr{B} \to \mathscr{C})) \to ((\mathscr{A} \to \mathscr{B}) \to (\mathscr{A} \to \mathscr{C}))$;

A3 удаление конъюнкции: $(\mathscr{A} \wedge \mathscr{B}) \to \mathscr{A}$, $(\mathscr{A} \wedge \mathscr{B}) \to \mathscr{B}$;

A4 введение конъюнкции: $\mathscr{A} \to (\mathscr{B} \to (\mathscr{A} \wedge \mathscr{B}))$;

A5 введение дизъюнкции: $\mathscr{A} \to (\mathscr{A} \vee \mathscr{B})$, $\mathscr{B} \to (\mathscr{A} \vee \mathscr{B})$;

A6 конструктивная дилемма: $(\mathscr{A} \to \mathscr{C}) \to ((\mathscr{B} \to \mathscr{C}) \to ((\mathscr{A} \vee \mathscr{B}) \to \mathscr{C}))$;

A7 закон Дунса Скота: $\neg\mathscr{A} \to (\mathscr{A} \to \mathscr{B})$;

A8 введение отрицания: $(\mathscr{A} \to \mathscr{B}) \to ((\mathscr{A} \to \neg\mathscr{B}) \to \neg\mathscr{A})$;

A9 закон исключенного третьего: $\mathscr{A} \vee \neg\mathscr{A}$.

Соответственно, теоремами логики высказываний являются все такие формулы, которые можно вывести из этих аксиом по правилам вывода. Тот факт, что формула $\varphi$ является теоремой, обозначают так: $\vdash \varphi$.

В современных учебниках правило подстановки вовсе не используется, вместо этого перечисленные выше аксиомы подаются не в виде конкретных формул, а в виде схем, где вместо переменных $\mathscr{A}, \mathscr{B}, \mathscr{C}$ стоят нетерминальные переменные, которые можно заменять произвольными формулами языка логики высказываний. По сути это и есть реализация правила подстановки, просто все результаты подстановок причисляются к списку аксиом.

Стоит отметить, что представленный здесь аксиоматический подход, часто называемый гильбертовским, не единственный. Существует и другой, более интуитивный способ формализации логических рассуждений — **исчисление естественного вывода**, предложенное Г. Генценом. В нем, как правило, нет логических аксиом, а вместо этого для каждой логической связки имеется пара правил: правило *введения* этой связки в формулу и правило ее *удаления*. Например, для конъюнкции правило введения выглядит как $\frac{\mathscr{A}, \mathscr{B}}{\mathscr{A} \wedge \mathscr{B}}$, а правило удаления — $\frac{\mathscr{A} \wedge \mathscr{B}}{\mathscr{A}}$ и $\frac{\mathscr{A} \wedge \mathscr{B}}{\mathscr{B}}$ (ср. с аксиомами A3 и A4). Такой подход гораздо ближе к тому, как математики строят доказательства неформально, оперируя гипотезами и выводами из них. Хотя оба подхода (гильбертовский и генценовский) для классической логики эквивалентны, второй часто оказывается более удобным для анализа самой структуры доказательств.

Отметим также, что если не все логические связки считать базовыми, а оставить, например, только $\neg$ и $\to$, то число аксиом можно резко сократить, оставив аксиомы только для этих связок, а все остальные связки ввести как сокращения, полагая по определению, что $\mathscr{A} \vee \mathscr{B} = \neg\mathscr{A} \to \mathscr{B}$, $\mathscr{A} \wedge \mathscr{B} = \neg(\mathscr{A} \to \neg\mathscr{B})$. Правда, при таком подходе мы чисто синтаксически навязываем этим логическим связкам классическое поведение.

**Теорема D2.2** (корректность и полнота вывода)**.**
*Формула $\varphi$ языка логики высказываний выводима из аксиом тогда и только тогда, когда она является тавтологией.*

*Доказательство.* Необходимость ($\Rightarrow$) проверить несложно. Для начала заметим, что все аксиомы являются тавтологиями. Чтобы в этом убедиться, достаточно выполнить проверку по таблице истинности. Например, рассмотрим аксиому $\mathscr{A} \to (\mathscr{B} \to \mathscr{A})$: поскольку она имеет вид импликации, она может быть ложной только в одном случае, когда $\mathscr{A} = 1$ и $(\mathscr{B} \to \mathscr{A}) = 0$, т.е. когда $(\mathscr{B} \to 1) = 0$, но последнее равенство ложно при любой оценке $\mathscr{B}$, так что данная аксиома есть тавтология.

Далее нужно показать, что правила вывода сохраняют тавтологичность (от тавтологий переходят к тавтологиям):

$$\frac{\varphi}{\varphi[\mathscr{A}/\psi]}, \qquad \frac{\varphi, \quad \varphi \to \psi}{\psi}.$$

Действительно, пусть $\varphi(\mathscr{A}, \mathscr{B}, \dots)$ — тавтология. Что будет, если вместо переменной $\mathscr{A}$ подставить формулу $\psi$ (про тавтологичность которой нам ничего не известно)? Для этого достаточно заметить, что если формуле $\varphi(\mathscr{A}, \mathscr{B}, \dots)$ соответствует булева функция

$f(a, b, \dots)$ (мы оцениваем пропозициональные переменные одноименными строчными латинскими переменными, пробегающими множество $\{0, 1\}$), а формуле $\psi(a, b, \dots)$ — функция $g(a, b, \dots)$, то согласно определению оценки формул оценкой формулы $\varphi[\mathscr{A}/\psi]$ будет композиция функций $f(g(a, b, \dots), b, \dots)$ (при выбранных оценках переменных $a, b, \dots$). Но так как $f$ есть тождественная единица, то и композиция будет таковой. Следовательно, $\varphi[\mathscr{A}/\psi]$ является тавтологией.

Правило MP: предполагая, что $\varphi$ и $\varphi \to \psi$ тавтологии, следуя таблице истинности для импликации, замечаем, что $\psi$ тоже тавтология, поскольку уравнение $(1 \to x) = 1$ решается единственным способом $x = 1$.

Таким образом, получая на вход тавтологии, правила вывода всегда дают на выходе тавтологии, что и доказывает корректность «штопора».

Достаточность ($\Leftarrow$). Здесь ситуация сильно сложнее, поэтому мы не будем приводить классические доказательство полноты, сославшись на книгу [42], где оно подробно рассмотрено.

Вместо этого мы приведем альтернативный способ доказательства полноты, воспользовавшись некоторыми алгебраическими построениями. Мы изложим его схематично, пропуская детали, но оставляя суть рассуждений.

Предположим, что формула $\varphi_0$ невыводима в логике высказываний. Наша задача — построить этом случае такую оценку $\varepsilon$ пропозициональных переменных, при которой $\varepsilon[\varphi_0] = 0$. Это будет означать, что $\varphi_0$ не является тавтологией. Таким образом, если формула является тавтологией, то она выводима.

Теперь для логики высказываний построим алгебру Линденбаума, элементами которой являются классы доказуемо эквивалентных формул. Мы говорим, что формула $\varphi$ *доказуемо эквивалентна* формуле $\psi$, если в логике высказываний выводима эквиваленция $\varphi \leftrightarrow \psi$. Тогда полагаем $[\varphi] = \{\psi \mid \vdash \varphi \leftrightarrow \psi\}$. Для этих классов операции и константы вводятся естественным образом: $\neg_L[\varphi] = [\neg\varphi]$, $[\varphi] \wedge_L [\psi] = [\varphi \wedge \psi]$, $[\varphi] \vee_L [\psi] = [\varphi \vee \psi]$, $\top_L = [\varphi \vee \neg\varphi]$, $\bot_L = [\varphi \wedge \neg\varphi]$.

Фактор-множество формул $L = \mathbb{L}/_{\leftrightarrow}$ с операциями $\neg_L, \wedge_L, \vee_L$ и константами $\top_L, \bot_L$ является счетной булевой алгеброй.[3]

Поскольку формула $\varphi_0$ не выводима, ее класс $[\varphi_0] \neq \top_L$, а значит, $[\neg\varphi_0] \neq \bot_L$.

Далее мы строим ультрафильтр на алгебре Линденбаума, содержащий $[\neg\varphi_0]$. В универсальной алгебре для факта существования такого ультрафильтра мы бы воспользовались теоремой Тарского об ультрафильтре (той самой, которая является ослаблением аксиомы выбора из списка на стр. 157), но поскольку у нас множество формул счетно (и более того, множество доказуемых формул перечислимо), такой ультрафильтр можно построить счетной рекурсией в рамках ZF, не прибегая к более сильным принципам. Обозначим этот ультрафильтр за $U$.[4]

---

[3] **Булева алгебра** — это множество $B$, на котором определены две бинарные операции $\vee_B$ (дизъюнкция, объединение, join, ИЛИ), $\wedge_B$ (конъюнкция, пересечение, meet, И), одна унарная операция $\neg_B$ (отрицание, дополнение, complement, НЕ), и выделены два различных специальных элемента $\bot_B$ (ноль, ложь, bottom, 0) и $\top_B$ (единица, истина, top, 1), аксиомами для которых являются тождества (D2.1)–(D2.4), в которых знак $\equiv$ нужно заменить на $=$, а также определение логических констант $\top_B = a \vee_B \neg_B a$, $\bot_B = a \wedge_B \neg_B a$. На булевой алгебре также вводится неравенство по правилу: $a \leqslant b \overset{\text{def}}{\rightleftharpoons} a \wedge_B b = a$.

[4] **Ультрафильтром** на булевой алгебре $B$ называется такое подмножество $U \subseteq B$, что $\bot_B \notin U$, $\forall x, y \in U : x \wedge_B y \in U$, $\forall x, y \in B : (x \in U) \wedge (x \leqslant_B y) \to (y \in U)$, $\forall x \in B : (x \in U) \vee (\neg_B x \in U)$.

Теперь мы можем задать функцию оценки для формул следующим способом:

$$\varepsilon(\mathscr{A}) = \begin{cases} 1, & [\mathscr{A}] \in U, \\ 0, & [\mathscr{A}] \notin U, \end{cases}$$

для пропозициональных переменных. Далее мы расширяем оценку на все формулы, следуя обычной схеме. Заметим, что эта же оценка задает функцию $h : L \to \{0, 1\}$ по правилу $h([\varphi]) = \varepsilon(\varphi)$, причем $h$ является гомоморфизмом булевых алгебр $L$ и $\mathbf{2}$.[5] На самом деле можно было пойти в обратную сторону: сначала выбрать гомоморфизм $h$, определив его как $h([\varphi]) = 1 \Leftrightarrow [\varphi] \in U$. А затем из него извлечь оценку пропозициональных переменных.

*Гомоморфизм* алгебр — это отображение, сохраняющее операции, и наше $h$ таковым является (здесь ключевую роль играет тот факт, что мы его определили как характеристическую функцию ультрафильтра). При этом, поскольку $h([\neg\varphi_0]) = 1$ и $h$ — гомоморфизм, получаем, что $h([\varphi_0]) = 0$, а значит, и оценка $\varepsilon(\varphi_0) = 0$. То есть, $\varphi_0$ не является тавтологией. □

Из доказательства второй части теоремы может показаться, что мы никак не используем аксиоматику логики высказываний и правила вывода. Но на самом деле мы используем их существенным образом. Во-первых, без закона исключенного третьего алгебра Линденбаума перестала бы быть булевой алгеброй, т.к. в булевой алгебре этот закон выполняется, а значит, мы бы не смогли построить гомоморфизм, «решающий», как оценивать элементы этой алгебры с помощью алгебры $\mathbf{2}$, а кроме того, наше рассуждение о том, что если $[\varphi_0] \neq \top_L$, то $[\neg\varphi_0] \neq \bot_L$, было бы неверным. Остальные аксиомы логики напрямую связаны с аксиоматикой булевой алгебры. Во-вторых, определение классов эквивалентности (и тот факт, что они вообще являются классами эквивалентности) напрямую основано на выводимости, т.е. на правиле MP. Если это правило ослабить, то, действительно, либо само по себе доказательство будет некорректным, либо мы докажем, что в этом случае выводимость не будет полной.

Оба доказательства (классическое и через гомоморфизм алгебр) весьма нетривиальны. В одном случае (классическом) оно требует разбора многочисленных случаев и индукции по сложности формул, в другом (как выше) — привлечения аппарата булевых алгебр и нетривиального построения ультрафильтра. Поэтому теорема о полноте логики высказываний — это весьма значимый и глубокий математический факт.

Алгебра Линденбаума является имманентным примером булевой алгебры как модели исчисления высказываний. Однако оказывается, что вообще весь класс булевых алгебр — это в точности класс моделей классической логики высказываний.

**Теорема D2.3** (об алгебраической полноте)**.**
*Формула $\varphi$ выводима в логике высказываний тогда и только тогда, когда она истинна в любой булевой алгебре (общезначима).*

*Доказательство.* Здесь корректность ($\Rightarrow$) доказывается также, как выше: нужно показать, что аксиомы эквивалентны $\top$, а правила вывода $\top$ всегда переводят в $\top$.

Полнота ($\Leftarrow$) доказывается по правилу контрапозиции. Предположим, что формула $\varphi$ не выводима. Тогда построим пример булевой алгебры, где она не будет истинной (не равна $\top$). Таким примером является как раз алгебра Линденбаума.

[5] Здесь $\mathbf{2}$ — это двухэлементная булева алгебра.

Действительно, если формула $\varphi$ не является теоремой ($\nvdash \varphi$), то ее класс эквивалентности $[\varphi]$ не равен верхнему элементу $\top_L$ в алгебре Линденбаума по определению.

Мы можем определить интерпретацию переменных в этой алгебре так: пропозициональной переменной $\mathscr{A}$ сопоставляется её собственный класс эквивалентности $[\mathscr{A}]$. Тогда значение формулы $\varphi$ при такой интерпретации будет равно $[\varphi]$. Поскольку $[\varphi] \neq \top_L$ в этой алгебре, мы нашли булеву алгебру, в которой $\varphi$ не истинна, а значит, $\varphi$ не общезначима. □

В продолжение темы использования булевых алгебр нельзя не задаться вопросом, как в булевой алгебре можно выразить отношение выводимости. Пусть $\Gamma \vdash \varphi$, где $\Gamma$ — произвольное множество формул. Ввиду компактности вывода на самом деле имеет место $\Gamma' \vdash \varphi$, где $\Gamma'$ — конечное подмножество $\Gamma$. Более того, это равносильно $\bigwedge \Gamma' \vdash \varphi$, где $\bigwedge \Gamma'$ — это конъюнкция всех формул из $\Gamma'$. Иначе говоря, выводимость сводится к бинарному отношению между формулами, а значит, и в алгебре будет интерпретироваться как бинарное отношение между элементами.

Положим для $a, b \in B$, где $B$ — булева алгебра, $a \leqslant b \overset{\text{def}}{\leftrightarrow} (a \wedge_B b) = a$, т.е. отношение $\leqslant$ определим через отношение равенства и операцию meet. Чисто алгебраически несложно показать, что $\leqslant$ является частичным (нестрогим) порядком на $B$, причем $\top_B$ — максимум, а $\bot_B$ — минимум этого отношения ($\forall x \in B : \bot_B \leqslant x \leqslant_B \top_B$).

Проверим, будет ли оно моделью отношения выводимости на формулах. Для этого необходимо удостовериться в том, что правила вывода при таком переводе являются истинными предикатами в алгебре.

Правило подстановки $\frac{\varphi}{\varphi[\mathscr{A}/\psi]}$. Пусть $\varphi$ — тавтология и $\varepsilon$ — произвольная оценка пропозициональных переменных в алгебре $B$. Требуется показать, что $\varepsilon(\varphi) \leqslant \varepsilon(\varphi[\mathscr{A}/\psi])$, т.е. что $(\varepsilon(\varphi) \wedge_B \varepsilon(\varphi[\mathscr{A}/\psi])) = \varepsilon(\varphi)$ для всех оценок $\varepsilon$. Из того, что $\varphi$ — тавтология, получаем $\varepsilon(\varphi) = \top_B$ (в силу корректности). Кроме того, $\varepsilon(\varphi[\mathscr{A}/\psi]) = \varphi(\varepsilon(\psi)) = \top_B$, следовательно, нам нужно проверить, что $\top_B \wedge_B \top_B = \top_B$, а это очевидное следствие аксиом булевой алгебры.

Правило MP: $\frac{\varphi,\quad \varphi \to \psi}{\psi}$. Необходимо показать, что при любой оценке $\varepsilon$: $\varepsilon(\varphi) \wedge_B \varepsilon(\varphi \to \psi) \leqslant \varepsilon(\psi)$. Для этого раскроем импликацию по определению: $\varepsilon(\varphi \to \psi) = \varepsilon(\neg\varphi \vee \psi) = \neg_B \varepsilon(\varphi) \vee_B \varepsilon(\psi)$. Иначе говоря, нужно проверить, что в алгебре $B$ выполняется тождество

$$a \wedge_B (\neg_B a \vee_B b) \leqslant b, \text{ где } a = \varepsilon(\varphi), b = \varepsilon(\psi).$$

Следуя аксиомам булевой алгебры, легко получаем, что

$$a \wedge_B (\neg_B a \vee_B b) = (a \wedge_B \neg_B a) \vee_B (a \wedge_B b) = \bot_B \vee_B (a \wedge_B b) = a \wedge_B b,$$

т.е. осталось проверить, что $a \wedge_B b \leqslant b$, что по определению означает $(a \wedge_B b) \wedge_B b = a \wedge_B b$, а это тоже верно по аксиомам булевой алгебры.

Таким образом применение правил вывода к формулам означает переход вверх по шкале $\leqslant$ для оценок формул. А это значит, что для всего вывода $\Gamma' \vdash \varphi$ выполняется неравенство $\varepsilon(\bigwedge \Gamma') \leqslant \varepsilon(\varphi)$ при любой оценке $\varepsilon$.

С другой стороны, если при любой оценке $\varepsilon$ имеем $\varepsilon(\bigwedge \Gamma') \leqslant \varepsilon(\varphi)$, то также верно, что $\neg_B \varepsilon(\bigwedge \Gamma') \vee_B \varepsilon(\varphi) = \top_B$, откуда в силу полноты следует, что формула $\neg \bigwedge \Gamma' \vee \varphi$ является тавтологией, т.е. выводима импликация $\bigwedge \Gamma' \to \varphi$. Тогда по правилу MP можно показать, что $\Gamma' \vdash \varphi$.

Таким образом $\Gamma' \vdash \varphi$ тогда и только тогда, когда при любой оценке в любой булевой алгебре $\varepsilon(\bigwedge \Gamma') \leqslant \varepsilon(\varphi)$.

Отсюда легко следует

**Теорема D2.4** (о дедукции)**.** $\Gamma, \varphi \vdash \psi$ *тогда и только тогда, когда* $\Gamma \vdash (\varphi \to \psi)$.

*Доказательство.* Мы сразу можем считать, что $\Gamma$ конечно (если нет, то можно выбрать конечно подмножество вместо него). Обозначим за $\chi$ формулу $\bigwedge \Gamma$, тогда утверждение теоремы состоит в следующем:

$$\chi \wedge \varphi \vdash \psi \quad \Leftrightarrow \quad \chi \vdash (\varphi \to \psi),$$

а из предыдущих выкладок это равносильно теореме булевой алгебры

$$(a \wedge_B b \leqslant c) \leftrightarrow (a \leqslant (\neg_B b \vee_B c)),$$

которая равносильна, согласно определению неравенства:

$$(a \wedge_B b \wedge_B c = a \wedge_B b) \leftrightarrow (a \wedge_B (\neg_B b \vee_B c) = a). \tag{D2.7}$$

Здесь есть два пути доказательства: 1) честно проверить это утверждение по аксиомам булевой алгебры, 2) воспользоваться «читерским» приемом, который заключается в том, что любое тождество в языке булевой алгебры верно или не верно одновременно во всех булевых алгебрах. Этот результат есть следствие того факта, что из любой булевой алгебры можно построить гомоморфизм в алгебру **2**. Поэтому если бы какое-то тождество нарушалось в какой-то булевой алгебре, то оно нарушалось бы и в **2**.[6]

Следовательно, нам остается только проверить, что (D2.7) выполняется в алгебре **2**, что можно выполнить простым перебором, подставляя вместо переменных числа 0 и 1. □

Теперь мы лучше начинаем понимать, что логика — это не просто игра в формулы, которая пытается смоделировать абстрактный мыслительный процесс, но еще и внутренний язык целого класса алгебр, где логические символы становятся настоящими операциями, а выводимость обретает конкретный смысл в виде порядка на элементах алгебры. Отсюда возникает такая математическая дисциплина, которая называется алгебраической логикой и позволяет анализировать логику чисто алгебраическими (традиционными для математики) методами.[7]

Следующие примеры булевых алгебр показывают, что даже классическое исчисление высказываний имеет весьма разнообразный класс моделей: 1) множество $\mathbf{2} = \{0, 1\}$ с одноименными булевыми функциями (стандартная модель); 2) булеан $\mathscr{P}(A)$ любого непустого множества $A$ с операциями дополнения, пересечения и объединения; 3) множество всех делителей свободного от квадратов числа $N$ с операциями $N/a$, НОД$(a, b)$, НОК$(a, b)$; 4) алгебра открыто-замкнутых подмножеств топологического пространства (с операциями дополнения, пересечения и объединения).

С другой стороны, общность этих структур проявляется в теореме о том, что каждая булева алгебра изоморфна алгебре, являющейся некоторым (декартовым) произведением копий двухэлементной булевой алгебры **2**. Эта теорема есть следствие известной теоремы Стоуна о представлении булевых алгебр (которую мы упоминали в списке следствий аксиомы выбора на стр. 157).

[6] Этот фундаментальный факт тесно связан с теоремой Стоуна о представлении булевых алгебр, гарантирующей достаточное количество ультрафильтров/гомоморфизмов в **2**.

[7] Речь идет, конечно, не только и не столько о классической логике и булевой алгебре, сколько о большом разнообразии логик, отличающихся от классической и имеющих свои алгебраические интерпретации.

# D2.2. Логика предикатов

Ввиду того, что логика предикатов была достаточно подробно освещена в разделе B1.2, мы остановимся здесь только на некоторых ключевых конструкциях и теоремах.

Напомним аксиомы и правила вывода логики предикатов:

PC1 универсальные замыкания всех подстановок всех формул языка логики предикатов во все тавтологии логики высказываний;

PC2 аксиомы для кванторов:

$$(\forall)\quad (\forall x\ \varphi[a/x]) \to \varphi[a/T]; \qquad (\exists)\quad \varphi[a/T] \to \exists x\ \varphi[a/x],$$

где $\varphi$ не содержит связанную переменную $x$, $T$ — любой терм теории;

PC3 правила вывода:

$$(MP)\quad \frac{\varphi,\quad \varphi \to \psi}{\psi}; \qquad (R1)\quad \frac{\varphi \to \psi}{\varphi \to \forall x\ \psi[a/x]};$$

$$(R1')\quad \frac{\psi}{\forall x\ \psi[a/x]}; \qquad (R2)\quad \frac{\psi \to \varphi}{(\exists x\ \psi[a/x]) \to \varphi},$$

где для правил (R1), (R1'), (R2) переменная $a$ не входит в $\varphi$ и ни в одну из активных (непогашенных) гипотез, от которых зависит вывод формулы в посылке этих правил.

Правила $(R1)$ и $(R2)$ называются **правилами Бернайса**. Правило (R1'), называемое *правилом обобщения* является производным правилом в нашей системе вывода, т.к. его можно получить из правила (R1), подставляя в нем вместо формулы $\varphi$ тождественную истину.

Действительно, если $\psi$ доказано (посылка для (R1')), то из этого следует $\top \to \psi$ (где $\top$ — любая подстановка тавтологии или доказанная теорема, не содержащая $a$). Применяя (R1) к $\top \to \psi$, получаем $\top \to \forall x\ \psi[a/x]$. Поскольку $\top$ истинно (доказуемо), по MP получаем $\forall x\ \psi[a/x]$.

**Теорема D2.5** (о дедукции)**.** *Пусть $T$ множество формул (в заданном языке первого порядка), $\varphi, \psi$ — произвольные формулы. Тогда если существует такой вывод формулы $T, \varphi \vdash \psi$, в котором ни при каком применении правила $(R1)$ к формулам, зависящим в этом выводе от формулы $\varphi$, не связывается ни одна из свободных переменных формулы $\varphi$, то $T \vdash (\varphi \to \psi)$.*

Доказательство этой теоремы почти полностью воспроизводится со случая синтаксического доказательства теоремы о дедукции в логике высказываний с поправкой на проверку применения правил (R1) и (R2). Ограничение на свободные переменные формулы $\varphi$, о котором идет речь в теореме, требуется именно для того, чтобы корректно проверить применение правила (R1). Если же формула $\varphi$ замкнутая, то теорема приобретает такой же вид, как в случае логики высказываний. Более того, в обратную сторону утверждение в любом случае очевидно в силу правила Modus Ponens, так что для замкнутых формул мы имеем равносильность:

$$T, \varphi \vdash \psi \quad \Leftrightarrow \quad T \vdash (\varphi \to \psi).$$

**Теорема D2.6.** *Пусть $\varphi$ — произвольная формула со свободной переменной $a$ (и, возможно еще какими-то свободными переменными), $t$ — произвольный терм, тогда*

$$\vdash \varphi[a/t] \leftrightarrow \exists x\ (\varphi[a/x] \wedge (x = t)).$$

*Доказательство.* ($\Rightarrow$) Рассмотрим новую формулу $\psi(a) \overset{\text{def}}{\rightleftharpoons} \varphi(a) \wedge (a = t)$. Очевидно, что $\varphi[a/t]$ выводит $\psi[a/t]$. Кроме того, по аксиоме для квантора существования верна импликация $\psi[a/t] \to \exists x\ \psi[a/x]$. Отсюда и из предыдущего по правилу Modus Ponens получаем, что $\exists x\ \varphi[a/x] \wedge (x = t)$. И по теореме о дедукции имеем нужную импликацию.

($\Leftarrow$) Ясно, что $\psi(a) \to \varphi[a/t]$ в силу конгруэнтности равенства. При этом, поскольку $a$ не входит в формулу $\varphi[a/t]$, можно применить правило Бернайса для введения квантора существования:

$$\frac{\psi(a) \to \varphi[a/t]}{\exists x\ \psi[a/x] \to \varphi[a/t]},$$

а это в точности обратная импликация теоремы. □

Следующее утверждение мы приводили в пример как общезначимую формулу чистого исчисления предикатов в разделе B1.2.8.

**Теорема D2.7.** *Пусть $\varphi$ — произвольная формула со свободными переменными $a, b$ (и, возможно, еще какими-то свободными переменными), тогда:*

$$(\exists x \forall y\ \varphi[a/x, b/y]) \to \forall y \exists x\ \varphi[a/x, b/y].$$

*Доказательство.* Сначала докажем следующую лемму (в случае одной переменной мы не пишем явным образом замену $[a/x]$):

$$\forall x\ (\psi_1(x, \vec{p}) \to \psi_2(x, \vec{q})) \to ((\exists x\ \psi_1(x, \vec{p})) \to \exists x\ \psi_2(x, \vec{q})), \tag{D2.8}$$

где $\vec{p}, \vec{q}$ — наборы свободных переменных (параметров), которые мы дальше не будем писать в целях экономии места, т.к. на вывод они никак не влияют. Мы используем здесь одну и ту же связанную переменную под кванторами, поскольку области действия этих кванторов не пересекаются, и коллизия переменных невозможна.

Примем в качестве гипотезы формулу $\forall x\ (\psi_1(x) \to \psi_2(x))$. Тогда по аксиоме ($\forall$) получаем для свободной переменной $a$ формулу $\psi_1(a) \to \psi_2(a)$. По аксиоме введения квантора существования замечаем, что

$$\psi_2(a) \to \exists x\ \psi_2(x),$$

отсюда и из предыдущей импликации, пользуясь транзитивностью импликации, получаем, что

$$\psi_1(a) \to \exists x\ \psi_2(x),$$

теперь рассмотрим полученную формулу как формулу вида $\psi_1(a) \to \psi_3$, где переменная $a$ не входит в формулу $\psi_3$ (мы там уже заменили ее на $x$), и применим к этой импликации правило Бернайса ($R2$) для введения квантора существования, получим формулу

$$(\exists x\ \psi_1(x)) \to \exists x\ \psi_2(x).$$

По теореме о дедукции ставим нашу гипотезу в антецедент импликации:

$$\forall x\ (\psi_1(x) \to \psi_2(x)) \to ((\exists x\ \psi_1(x)) \to \exists x\ \psi_2(x)),$$

что доказывает (D2.8). Таким образом мы можем вносить в обе части импликации кванторы существования на одну и ту же свободную переменную.

На теоретико-множественном языке эта лемма утверждает, что если непустое множество $A$ является подмножеством множества $B$, то и $B$ обязано быть непустым. Воспользуемся этим для доказательства теоремы.

По аксиоме элиминации квантора всеобщности верно следующее:

$$(\forall y\ \varphi[a, b/y]) \to \varphi(a, b).$$

Теперь, рассматривая эту импликацию как $\psi_1(a) \to \psi_2(a)$, используя (D2.8) и правило MP, получаем, что:

$$(\exists x \forall y\ \varphi[a/x, b/y]) \to \exists x\ \varphi[a/x, b].$$

Полученная формула имеет вид $\varphi_1 \to \varphi_2(b)$, где $b$ не входит в формулу $\varphi_1$ (т.к. уже заменена на $y$), следовательно, можно применять правило Бернайса ($R1$) для введения квантора всеобщности:

$$(\exists x \forall y\ \varphi[a/x, b/y]) \to \forall y \exists x\ \varphi[a/x, b/y],$$

что и завершает доказательство теоремы.

Отметим, что области действия кванторов $\exists x \forall y$ и $\forall y \exists x$ здесь не пересекаются, поэтому мы можем использовать одноименные связанные переменные под кванторами. □

В качестве примера применения теоремы D2.7 заметим, что к этой формуле сводится утверждение из математического анализа «равномерно непрерывная на множестве функция непрерывна на нем».

### D2.2.1 Корректность и полнота исчисления

Теперь дадим точное определение истинности формулы логики предикатов в модели. Пусть имеется язык логики первого порядка с сигнатурой $\Sigma$, непустое множество $M$ и интерпретация $I$, сопоставляющая каждому символу из $\Sigma$ соответствующий элемент (отношение, функцию или константу) на $M$ (с учетом арности). Тогда структура $\mathcal{M} = \langle M, I[\Sigma] \rangle$ называется **моделью** языка, порожденного данной сигнатурой, а множество $M$ называется при этом *доменом* интерпретации.

*Оценка* (или *означивание*) свободных переменных — это функция $\varepsilon$ из множества свободных переменных в $M$, т.е. присвоение переменным (произвольных) значений из $M$. Определение интерпретации языка и теории строится вокруг произвольности выбора оценки.

Имея интерпретацию символов сигнатуры в модели, а также оценку свободных переменных, мы можем вычислить значения термов и истинностные значения формул языка в сигнатуре $\Sigma$ в данной модели. Для удобства записи значения термов при данной оценке переменных мы тоже будет обозначать как оценку $\varepsilon(t)$, где $t$ — произвольный терм.

Значения термов вычисляются рекурсивно:

- символы констант означиваются своей интерпретацией: $\varepsilon(c) = I(c)$;

- пусть уже вычислены значения термов $t_1, \ldots, t_n$ и $F$ есть $n$-местный функциональный символ сигнатуры, тогда $\varepsilon(F(t_1, \ldots, t_n)) = I(F)(\varepsilon(t_1), \ldots, \varepsilon(t_n))$.

Затем мы начинаем означивать формулы истинностными значениями, следуя похожей схеме, только теперь мы определяем отношение $\mathcal{M} \models$ (*истинно в модели*):

- для атомарных предикатов: $\mathcal{M} \models_\varepsilon P(t_1, \ldots, t_n)$ тогда и только тогда, когда $\langle \varepsilon(t_1), \ldots, \varepsilon(t_n) \rangle \in I(P)$;
- для логических связок: $\mathcal{M} \models_\varepsilon \neg\varphi \Leftrightarrow$ не верно, что $\mathcal{M} \models_\varepsilon \varphi$;
  $\mathcal{M} \models_\varepsilon \varphi \wedge \psi \Leftrightarrow \mathcal{M} \models_\varepsilon \varphi$ И $\mathcal{M} \models_\varepsilon \psi$;
  $\mathcal{M} \models_\varepsilon \varphi \vee \psi \Leftrightarrow \mathcal{M} \models_\varepsilon \varphi$ ИЛИ $\mathcal{M} \models_\varepsilon \psi$;
  $\mathcal{M} \models_\varepsilon \varphi \to \psi \Leftrightarrow$ не верно $\mathcal{M} \models_\varepsilon \varphi$ ИЛИ $\mathcal{M} \models_\varepsilon \psi$;
- для кванторов: $\mathcal{M} \models_\varepsilon \forall x\, \varphi(a/x, \vec{p})$ тогда и только тогда, когда $\mathcal{M} \models_{\varepsilon[a/m]} \varphi(a, \vec{p})$ для всех $m \in M$; $\mathcal{M} \models_\varepsilon \exists x\, \varphi(a/x, \vec{p})$ тогда и только тогда, когда $\mathcal{M} \models_{\varepsilon[a/m]} \varphi(a, \vec{p})$ при некотором $m \in M$, где мы использовали модифицированную оценку

$$\varepsilon[a/m](v) = \begin{cases} \varepsilon(v), & v \neq a, \\ m, & v = a, \end{cases} \qquad m \in M.$$

Если коротко, то мы логические связки и кванторы нашего языка интерпретируем логическими связками и кванторами мета-теории, т.е. теории множеств, в которой модель $\mathcal{M}$ задана.

Наконец, скажем, что $\mathcal{M} \models \varphi$ ($\varphi$ *истинна в модели* $\mathcal{M}$), если при любой оценке $\varepsilon$ верно $\mathcal{M} \models_\varepsilon \varphi$, где $\varphi$ — произвольная формула языка с сигнатурой $\Sigma$.

Формула называется **выполнимой**, если она истинна в какой-то модели, **общезначимой** — если в любой. Множество формул $T$ истинно в модели ($\mathcal{M} \models T$), если все его формулы истинны в этой модели. Соответственно определяется и выполнимость множества формул (в частности, аксиоматики или теории). Выполнимое множество формул также называется **совместным**.

Очевидно, что отношение $\mathcal{M} \models T$ монотонно по $T$, т.е. если $\mathcal{M} \models T$ и $T' \subseteq T$, то и $\mathcal{M} \models T'$.

Напомним, что теория называется **непротиворечивой**, если в ней нельзя вывести противоречие ($T \nvdash \bot$).

С наличием моделей тесно связано понятие семантического (или логического) следования. Мы говорим, что формула $\varphi$ **семантически** (логически) следует из множества формул $T$, если для любой модели $\mathcal{M}$ из $\mathcal{M} \models T$ следует $\mathcal{M} \models \varphi$. Обозначение: $T \Vdash \varphi$.[8]

Как уже отмечалось в разделе B1.2.9, несложно показать, что логика предикатов *корректна* относительно семантики, т.е.

**Теорема D2.8** (о корректности вывода)**.** *Если имеет место вывод $T \vdash \varphi$, то верно и семантическое следование $T \Vdash \varphi$.*

Это вытекает напрямую из того, что логику языка мы интерпретируем как логику мета-теории, т.е. формальный вывод будет соответствовать выводу в модели в силу определения истинности в модели.

[8] С обозначениями истинности в модели и логического следования часто возникает путаница, например, в обоих случаях используется символ $\models$ или очень похожий на него символ $\models$. Здесь мы решили использовать отдельный символ $\Vdash$ для логического следования, хотя и этот символ часто используется с другими целями.

**Следствие D2.1.** *Если теория имеет модель, то она непротиворечива.*

Действительно, предположим, что у теории есть модель, но теория противоречива, но тогда в силу корректности вывода в модели истинно противоречие.

**Следствие D2.2.**
*Если совместны множества $T, \varphi$ и $T, \neg\varphi$, то $\varphi$ не зависит от $T$.*

Напомним, что независимость формулы $\varphi$ от множества формул $T$ означает, что $T \nvdash \varphi$ и $T \nvdash \neg\varphi$. Данное следствие корректности — основной инструмент демонстрации независимости каких-либо утверждений. Например, независимость аксиомы параллельных от остальных аксиом геометрии (модель $\mathbb{R}^2$ и модель Пуанкаре), независимость аксиомы выбора и континуум-гипотезы от аксиом ZF (модели Гёделя и Коэна).

Модели, которые мы приводили в разделах B1.2.7, B1.2.10, C1.4.3, показали нам ряд примеров непротиворечивых теорий, таких, как теория линейных порядков, теория групп, теория равенства, арифметика Пеано (ее модель — ординал $\omega$), теория вещественно замкнутых полей, некоторые фрагменты теории множеств. Разумеется, все это доказывается в предположении непротиворечивости нашей мета-теории, в роли которой обычно выступает ZF, но для простых случаев (вроде равенства, линейных порядков и групп) достаточно очень примитивных конечных, почти физических моделей.

Что же касается самой ZF, то в силу второй теоремы Гёделя о неполноте она не может обосновать свою собственную непротиворечивость, и для выяснения этого вопроса понадобится еще более сильная теория (например, ZF с аксиомой строго недостижимого кардинального числа), которая требует более сильных онтологических допущений.

Тем не менее, как мы уже обсуждали в разделе ZF без аксиомы бесконечности, или HF, выглядит безусловно надежной теорией, учитывая возможность ее интерпретации в арифметике, а также скобочную модель. Поэтому в настоящее время существует консенсус среди математиков о том, что ZF непротиворечива.

**Теорема D2.9** (Гёделя о полноте логики предикатов)**.**

**(1)** *Если теория первого порядка непротиворечива, то она совместна.*

**(2)** *Эквивалентная формулировка: для любого $T$ и формулы $\varphi$, если $T \Vdash \varphi$, то $T \vdash \varphi$.*

Доказательство (1) впервые было получено Гёделем в его докторской диссертации в 1929 году. Работа была опубликована в 1930 году под названием „Die Vollständigkeit der Axiome des logischen Funktionenkalküls“ («Полнота аксиом логического исчисления функций»). Затем Хенкин (в 1949) нашел более прозрачное доказательство, основанное на использовании констант, являющихся свидетелями экзистенциальных формул. По сути, модель строится из имеющихся констант, свежих констант, извлекаемых из теорем теории вида $\exists x\ \varphi(x)$, и всех замкнутых термов, которые получаются по правилам формирования термов из этих констант.

При этом в доказательстве используется возможность расширить теорию до максимальной непротиворечивой (и, следовательно, полной) методом построения ультрафильтра в алгебре Линденбаума, что для счетных языков выполнимо в чистой теории ZF (благодаря перечислимости всех формул), а для несчетных языков требует теоремы Тарского об ультрафильтре (см. стр. 157).

Пункт (1) с помощью теоремы о корректности обобщается так: теория непротиворечива тогда и только тогда, когда она совместна (имеет модель).

Пункт (2) тоже обобщается до эквиваленции: $T \Vdash \varphi$ тогда и только тогда, когда $T \vdash \varphi$, в силу корректности логики предикатов первого порядка относительно семантики.

*Доказательство эквивалентности формулировок.* ($\Rightarrow$) Пусть выполнено (1) и $T \Vdash \varphi$, тогда, предполагая, что $T \nvdash \varphi$, получаем, что $\neg\varphi$ не противоречит $T$, следовательно, множество формул $T \cup \{\neg\varphi\}$ непротиворечиво, а значит, имеет модель в силу (1). Обозначим эту модель $\mathcal{M}$. Тогда $\mathcal{M} \models T \cup \{\neg\varphi\}$ и, в частности, $\mathcal{M} \models T$. Тогда, с одной стороны, $\mathcal{M} \models \varphi$ в силу предположения $T \Vdash \varphi$, с другой стороны, $\mathcal{M} \models \neg\varphi$ в силу выбора самой модели $\mathcal{M}$. Противоречие. Следовательно, $T \vdash \varphi$, т.е. из (1) следует (2).

($\Leftarrow$) Обратно, пусть выполнено (2) и теория $T$ непротиворечива. Допустим, что она не имеет модели, т.е. для любой структуры $\mathcal{M}$: $\mathcal{M} \not\models T$. Запишем условие (2) полностью для данной теории $T$:

$$\forall\varphi\ [\forall\mathcal{M}\ (\mathcal{M} \models T) \to (\mathcal{M} \models \varphi)] \to (T \vdash \varphi),$$

где красным отмечены кванторы и импликация мета-теории. Как видим, у нас посылка первой импликации ложная для данной теории $T$, значит, вся импликация истинная. Следовательно, из второй импликации с истинной посылкой получаем, что

$$\forall\varphi\ (T \vdash \varphi),$$

в таком случае возьмем в качестве $\varphi$ ложную формулу и получим, что $T \vdash \bot$, а это противоречит тому, что $T$ непротиворечива. Таким образом из (2) следует (1).

Используя теорему о полноте, можно иначе переписать теорему о дедукции:

$$T, \varphi \Vdash \psi \quad \Leftrightarrow \quad T \Vdash (\varphi \to \psi), \tag{D2.9}$$

и этот результат можно доказать уже семантически примерно так же, как мы его доказывали для логики высказываний. Отличие состоит в том, что вместо булевых алгебр нужно будет использовать цилиндрические или полиадические алгебры, в которых предусмотрена интерпретация кванторов.[9] Тогда утверждение (D2.9) перепишется в виде аналогичной алгебраической теоремы:

$$(g \wedge_B a) \leqslant_B b \quad \Leftrightarrow \quad g \leqslant (a \to_B b),$$

истинность которой легко следует из аксиом соответствующей алгебры.

Используя теорему о полноте, можно дать другое (семантическое) доказательство теоремы D2.7, которую теперь с учетом теоремы о дедукции можно сформулировать иначе:

$$\exists x \forall y\ \varphi[a/x, b/y] \Vdash \forall y \exists x\ \varphi[a/x, b/y].$$

Пусть дана произвольная модель $\mathcal{M}$, состоящая из непустого множества (области интерпретации) $M$ и интерпретации предикатного символа $\varphi$. Предположим, что $\mathcal{M} \models \exists x \forall y\ \varphi(x, y)$. Это означает, что в $M$ существует хотя бы один элемент, назовем его $a$, такой, что $\mathcal{M} \models \forall y\ \varphi(a, y)$. Это означает, что для любого элемента $d \in M$: $\mathcal{M} \models \varphi(a, d)$.

Покажем, что при этом предположении $\mathcal{M} \models \forall y \exists x\ \varphi(x, y)$.

Возьмем произвольный элемент $b \in M$. Из предыдущего мы знаем, что существует элемент $a \in M$ такой, что $\mathcal{M} \models \varphi(a, d)$ для всех $d \in M$. Поскольку это верно для всех $d$, это будет верно и для нашего произвольно выбранного $b$. То есть, $\mathcal{M} \models \varphi(a, b)$. Это

[9] Цилиндрические алгебры были введены Альфредом Тарским и его учениками (Леон Хенкин, Дональд Монк). Полиадические алгебры разработаны Полом Халмошем. См. [66, 71].

означает, что для нашего произвольного $b$ мы нашли такой элемент $x$ (а именно, $a$), для которого $\varphi(x, b)$ истинно.

Поскольку мы выбрали $b$ произвольно, это рассуждение верно для любого элемента $y \in M$. Следовательно, $\mathscr{M} \models \forall y \exists x \varphi(x, y)$.

Поскольку мы никак не ограничивали выбор модели, логическое следование $\exists x \forall y\ \varphi[a/x, b/y] \Vdash \forall y \exists x\ \varphi[a/x, b/y]$ доказано.

## D2.2.2 Выразимость

Далее приведем справочно еще несколько фактов о логике первого порядка (без доказательств).

Ранее мы уже вкратце говорили про изоморфизмы структур, дадим теперь точное определение. Пусть имеется две модели $\mathscr{M} = \langle M, P, F, C\rangle$ и $\mathscr{N} = \langle N, P', F', C'\rangle$, причем задано взаимно однозначное соответствие их сигнатур $I$ такое, что $I(P) = P'$ для всех $P \in \mathscr{P}$, $I(F) = F'$ для всех $F \in \mathscr{F}$ и $I(c) = c'$ для всех $c \in \mathscr{C}$, сохраняющее арность. **Гомоморфизмом** структуры $\mathscr{M}$ в структуру $\mathscr{N}$ называется функция $g : M \to N$, сохраняющая предикаты и функции, т.е.

$$\begin{aligned} F(a_1, \dots, a_n) = b \quad &\Rightarrow \quad F'(g(a_1), \dots, g(a_n)) = g(b), \\ \langle a_1, \dots, a_n\rangle \in P \quad &\Rightarrow \quad \langle g(a_1), \dots, g(a_n)\rangle \in P', \\ g(c) = c' & \end{aligned}$$

Если $g$ — биекция между $M$ и $N$ и в определении выше вместо $\Rightarrow$ можно поставить $\Leftrightarrow$, то $g$ называется **изоморфизмом** структур $\mathscr{M}$ и $\mathscr{N}$ (эквивалентное определение: существует $g^{-1} : N \to M$, тоже являющаяся гомоморфизмом). Наличие изоморфизма структур обозначается $\mathscr{M} \cong \mathscr{N}$.

Если $\mathscr{M} = \mathscr{N}$ и при этом $I = \mathrm{id}$, то изоморфизм называется **автоморфизмом** структуры $\mathscr{M}$. Легко проверить, что автоморфизмы структуры образуют группу относительно операции композиции функций, которая обозначается $\mathrm{Aut}(\mathscr{M})$.

Пусть теперь имеется язык первого порядка с сигнатурой $\Sigma$, которую мы одинаково (с точностью до сопоставления их сигнатур) интерпретируем в моделях $\mathscr{M}$ и $\mathscr{N}$.

**Теорема D2.10.** *Истинность формул сохраняется при изоморфизме моделей, т.е.*

$$\text{если } \mathscr{M} \cong \mathscr{N}, \text{ то} \qquad \mathscr{M} \models \varphi \quad \Leftrightarrow \quad \mathscr{N} \models \varphi.$$

Здесь важно подчеркнуть, что формула $\varphi$ задана в одном и том же языке, который мы одинаково интерпретируем в этих двух моделях (с учетом сопоставления $I$ между сигнатурами моделей).

Данная теорема применительно к автоморфизмам дает мощный инструмент анализа выразимости модельных предикатов в языке теории. Рассмотрим пример: теория абелевых групп без кручения с операцией $+$ интерпретируется в модели $\mathbb{Z}$ естественным образом. Однако в структуре $\mathbb{Z}$ есть отношение линейного порядка $\leqslant$. Вопрос: можно ли его выразить через операцию сложения в $\mathbb{Z}$? Если такое возможно, т.е. предикат $a \leqslant b$ можно записать формулой $\varphi(a, b)$ в языке этой абелевой группы, то этот предикат должен сохранять истинность при автоморфизмах во всех моделях, в частности в $\mathbb{Z}$. Но в структуре $\mathbb{Z}$ существует два автоморфизма, сохраняющих сигнатуру теории, т.е. операцию сложения: это $f(x) = x$ и $g(x) = -x$. Однако же автоморфизм $g$ очевидным

образом не сохраняет формулу $a \leqslant b$, т.к. он меняет отношение порядка на обратное $(-b \leqslant -a)$. Следовательно, предикат $a \leqslant b$ невыразим через $+$ в структуре $\mathbb{Z}$.

Такой аргумент не прошел бы, если бы мы рассматривали сигнатуру теории колец, поскольку в кольце $\mathbb{Z}$ с операциями сложения и умножения предикат порядка уже можно выразить:

$$(a \leqslant b) \overset{\text{def}}{\leftrightarrow} \exists x_1, x_2, x_3, x_4 : \; a + x_1 \cdot x_1 + x_2 \cdot x_2 + x_3 \cdot x_3 + x_4 \cdot x_4 = b.$$

Он не нарушается при автоморфизмах, поскольку в кольце $\mathbb{Z}$ с операциями сложения и умножения есть ровно один автоморфизм: id. При этом мы не утверждаем, что так определенный предикат будет задавать порядок во *всех* моделях теории колец. Достаточно привести пример кольца гауссовых чисел $\mathbb{Z}[i]$, где указанное определение не задаст линейный порядок (будет одновременно выполняться $-1 \leqslant 1$ и $1 \leqslant -1$).

Иначе говоря, теорема об автоморфизмах обычно бывает полезной, когда нужно опровергнуть выразимость какого-то отношения (или функции) через элементы данной сигнатуры, а не показать возможность его выразить.

Можно привести еще несколько примеров:

- В целых числах операцию $+$ и константу $0$ нельзя выразить через одно только отношение порядка.
- В языке элементарной планиметрии Тарского невыразимы:
  - никакая конкретная фигура, кроме всей плоскости;
  - единица длины, т.е. предикат «длина отрезка $AB$ равна 1»;
  - ориентация, т.е. предикат «вершины треугольника $ABC$ обходятся против часовой стрелки».
- В языке теории вещественно замкнутых полей невыразимы:
  - предикат «быть целым числом»;
  - предикат «быть рациональным числом»;
  - предикаты, выражающие элементарные функции $y = \sin(x)$, $y = e^x$ и т.д;
  - числа $\pi$ и $e$.

### D2.2.3 Категоричность

**Теорема D2.11** (Лёвенгейма-Скулема о понижении мощности)**.**
*Если теория первого порядка в счетном языке имеет бесконечную модель, то она имеет счетную модель.*

**Замечание**: можно обобщить эту теорему, говоря о несчетных языках и моделях, в таком случае нижняя планка для мощности модели будет иной, но поскольку в этой книге мы рассматриваем только счетные языки, мы опустим такие подробности.

Практически все знакомые нам по данному курсу теории удовлетворяют условиям этой теоремы. Например, теория равенства без аксиом о конечном домене, теория линейных порядков, теория групп, арифметика Пеано, теория вещественно замкнутых полей, теория множеств Цермело-Френкеля...

По поводу последних двух примеров могут возникнуть сомнения, особенно если вспомнить, что в теории множеств существует аксиома, позволяющая как угодно долго повышать мощность множества, применяя операцию $\mathscr{P}(X)$.

Однако тут надо понимать, что способности теории часто гораздо слабее как в плане доказуемости, так и в плане выразительности, чем способности мета-теории, в которой мы строим модели. Если теория говорит, что можно строить восходящую цепочку булеанов, то это еще не значит, что в ее модели эти доказуемые булеаны будут соответствовать «настоящим» булеанам. В частности, счетная модель теории множеств ZF строится на так называемом конструктивном универсуме Гёделя $L$, в котором все множества определимы, т.е. все они представляют собой только такие совокупности, которые можно определить формулами. Точнее, каждый следующий конструктивный универсум строится как множество всех *определимых* подмножеств предыдущего, а значит, на самом деле (с точки зрения мета-теории) мощности всех этих универсумов не более чем счетны.

Как же там дела обстоят с теоремой Кантора, утверждающей, что между $X$ и $\mathscr{P}(X)$ не существует биекции? А очень просто, поскольку эта биекция тоже должна быть конструктивным множеством. И когда теория доказывает нам, что биекции не существует, она говорит нам только лишь про биекции, которые являются множествами внутри этой модели, в то время как на самом деле такая биекция есть, но эта биекция не будет определимой в теории.

Таким образом, хотя модель и счетная с точки зрения метатеории, теория попрежнему считает многие множества несчетными: внутри теории счетность означает наличие биекции, которая сама является множеством модели, а метатеоретическое перечисление тех же самых объектов такого множества давать не обязано.

Пожалуй, это можно сравнить с туннельным эффектом у гонщиков. В нормальных условиях они видят гораздо больше, чем в состоянии гонки, где их поле зрения сужается до минимально необходимого, чтобы дойти до цели. Или же с эффектом наблюдателя в теории относительности: снаружи наблюдатель видит все совсем не так, как наблюдатель, находящийся внутри системы (теории).

Аналогично, теория вещественно замкнутых полей имеет своей моделью, например, счетное множество вещественных алгебраических чисел, поскольку максимум, что она умеет требовать, — это наличие вещественных корней многочленов нечетной степени, а это — алгебраические числа, множество которых можно перечислить, опираясь на перечисление многочленов.

С другой стороны, важно понимать, что существование счетной модели не означает ее единственность. Так, у арифметики Пеано существуют нестандартные модели, включающие стандартную модель $\mathbb{N}$ лишь как начальный отрезок. В этих моделях существуют так называемые галактики нестандартных чисел, являющиеся копиями $\mathbb{Z}$. И снова может показаться, что мы сталкиваемся с каким-то противоречием, ведь в $\mathbb{Z}$ существуют бесконечно убывающие последовательности, а в арифметике Пеано их быть не может в силу принципа индукции. И тут мы снова понимаем, что с точки зрения внешнего наблюдателя такие последовательности есть, но ни доказать их наличие, ни даже определить их арифметика Пеано не способна, т.е. она их просто «не видит» как единый объект (область истинности некоторой своей формулы). И здесь получается, что модель как структура в мета-теории гораздо богаче моделируемой теории.

Мало того, счетные нестандартные модели арифметики не изоморфны стандартной модели. То есть класс счетных моделей может быть весьма разнообразным, что бы там ни думала про них сама теория.

Зафиксируем один стандартный способ получения таких нестандартных моделей, широко известный как *теорема компактности* для логики первого порядка.

**Теорема D2.12** (о компактности, Гёделя–Мальцева)**.** *Множество* $\Gamma$ *замкнутых формул первого порядка имеет модель тогда и только тогда, когда каждое конечное подмножество* $\Gamma' \subseteq \Gamma$ *имеет модель.*

Это — семантический аналог (тривиальной) компактности выводимости, уже отмеченной среди базовых свойств отношения $\vdash$ на стр. 94, и получается он из корректности и полноты вывода в один шаг: если каждое конечное $\Gamma' \subseteq \Gamma$ имеет модель, то по корректности каждое такое $\Gamma'$ непротиворечиво; следовательно, непротиворечиво и само $\Gamma$ (иначе вывод $\Gamma \vdash \bot$ уже осуществлялся бы на конечном фрагменте — в силу компактности выводимости); а тогда по полноте $\Gamma$ имеет модель. Обратное направление очевидно.

Нестандартная модель PA получается теперь так: добавим к ее аксиомам новую константу $c$ вместе с бесконечной схемой аксиом $\{c \neq S^n 0 \mid n \in \mathbb{N}\}$, где $S^n 0$ обозначает терм 0 с приписанными слева $n$ символами функции следования $S$. Каждый конечный фрагмент этой схемы выполняется в стандартной модели $\mathbb{N}$ (достаточно интерпретировать $c$ достаточно большим натуральным числом), поэтому по теореме компактности вся расширенная система аксиом имеет модель — обязательно содержащую элемент, который больше $S^n 0$ для каждого $n \in \mathbb{N}$. Явное описание таких моделей выходит за рамки этой книги (см. [53]).

Это различие между стандартной и нестандартными моделями арифметики оказывается гораздо глубже, чем простое отсутствие изоморфизма. Оно затрагивает саму их вычислительную природу, что элегантно демонстрирует теорема Тенненбаума. Она устанавливает фундаментальную связь между аксиоматикой и теорией алгоритмов, придавая стандартной модели особый, «конструктивный» статус.

**Теорема D2.13** (Тенненбаум, 1959)**.** *Единственной счетной вычислимой моделью арифметики Пеано (PA) является ее стандартная модель на ординале* $\omega$*. В любой счетной нестандартной модели PA по крайней мере одна из операций — сложение или умножение — не является вычислимой функцией.*

Таким образом, хотя аксиомы первого порядка не способны отличить стандартную модель от нестандартных, требование *вычислимости* операций мгновенно отсекает все «патологические» варианты. С точки зрения мета-теории, мы можем построить множество странных моделей, но как только мы требуем, чтобы эти модели были алгоритмически реализуемы, остается только одна — привычные нам натуральные числа.

Далее под *мощностью множества* будем понимать кардинальное число, предполагая, что работаем в ZFC. Напомним, что **кардинальное число** (кардинал) — это наименьший среди равномощных ординалов. Из аксиомы выбора следует, что для любого множества существует единственный равномощный ему кардинал. Счетный кардинал обозначается либо $\omega$, либо, следуя общей нумерации кардиналов, $\aleph_0$. Следующий за $\omega$ кардинал обозначается $\omega_1$ или $\aleph_1$. Мощность континуума часто обозначается $\mathfrak{c}$ или $2^{\aleph_0}$.

Вообще, для любого собственного подкласса класса ординалов существует единственная строго возрастающая взаимно однозначная нумерация элементов этого подкласса всеми ординалами. То есть, если имеется собственный класс $\mathscr{K} \subseteq \mathrm{Ord}$, то существует единственное определяемое отображение $F : \mathrm{Ord} \to \mathscr{K}$ такое, что $F(\alpha) < F(\beta) \leftrightarrow \alpha < \beta$ и $\forall \alpha \in \mathscr{K} : \exists \beta \in \mathrm{Ord} : F(\beta) = \alpha$. Таким способом нумеруются все бесконечные

кардиналы $\aleph_\alpha$ или, скажем, бет-последовательность:

$$\beth_0 = \omega, \quad \beth_{\alpha+1} = 2^{\beth_\alpha}, \quad \beth_\lambda = \sup\{\beth_\beta \mid \beta < \lambda\}.$$

Более подробно о кардинальных числах мы поговорим в разделе D4.3.4.

**Теорема D2.14** (Лёвенгейма-Скулема о повышении мощности)**.**
*Если теория $T$ имеет бесконечную модель мощности $\kappa$, то она имеет модель любой мощности $\tau > \kappa$.*

Объединяя две теоремы Лёвенгейма-Скулема, можно сказать, что если теория первого порядка в счетном языке имеет модель хотя бы одной бесконечной мощности, то она имеет модель любой бесконечной мощности. И таким образом мы замечаем удивительный факт, что первопорядковые теории в счетных языках плохо различают бесконечности с точки зрения внешнего наблюдателя (мета-теории).

Это подтверждает и следующая теорема, для формулировки которой нам потребуется дать определение. Теория $T$ называется $\kappa$-категоричной (категоричной в мощности $\kappa$), где $\kappa$ — кардинал, если все модели этой теории, носитель которых имеет мощность $\kappa$, изоморфны. Например, теория $\mathrm{DLO}_\infty$ (плотных линейных порядков без максимума и минимума) категорична в счетной мощности, а теория DTFA делимых абелевых групп без кручения категорична в мощности $\mathfrak{c}$ (и любой другой несчетной мощности).

**Теорема D2.15** (Мóрли о категоричности)**.** *Пусть $T$ — полная теория первого порядка в счетном языке. Если существует несчетная мощность $\kappa$ такая, что $T$ $\kappa$-категорична, то $T$ $\lambda$-категорична для любой несчетной мощности $\lambda$.*

Таким образом мы видим, что полные категоричные теории (первого порядка) умеют отличать только две бесконечности — счетную и несчетную. Причем, как мы увидим дальше, требование полноты здесь избыточно, т.к. категоричные теории оказываются полными автоматически.

### D2.2.4 Полнота теории

Раз уж мы столь подробно осветили тему полноты исчислений, нельзя не сказать хотя бы пару слов о полноте теорий, хотя мы это уже обсуждали в разделе B1.2.9 достаточно подробно.

Мы уже видели несколько примеров независимых утверждений, таких как Пятый постулат, Аксиома выбора и теорема Гудстейна, что означает для теорий наличие некой серой зоны в отношении выводимости: какие-то формулы мы можем вывести из аксиом (теоремы), какие можем опровергнуть (антитеоремы), а про какие-то наша теория ничего не знает. Возникает желание дополнить аксиоматику так, чтобы серая зона исчезла.

Теория называется **полной**, если всякая замкнутая формула языка этой теории либо доказуема, либо опровержима.

Оказывается, что иногда теорию можно пополнить вполне себе *перечислимым* множеством аксиом так, чтобы она стала полной, а иногда такое пошаговое пополнение принципиально невозможно, требуется некий трансцендентный скачок, чтобы получить полную теорию (как в упоминавшемся конструкте с ультрафильтром на алгебре Линденбаума). Между «сговорчивыми» (конструктивно достраиваемыми до полной) и

«строптивыми» теориями существует четкий водораздел под названием теорема Гёделя о неполноте (первая). Мы уже приводили ее в разделе B1.2.9, но такую теорему не грех повторить несколько раз.

**Теорема D2.16** (Гёделя о неполноте, первая)**.** *Если теория в языке первого порядка*

(G1) *непротиворечива;*

(G2) *перечислима (т.е. существует алгоритм, умеющий перечислять все ее теоремы);*

(G3) *может интерпретировать арифметику первого порядка,*

*то она не полна, т.е. существует такое предложение в языке этой теории, которое нельзя ни доказать, ни опровергнуть в системе ее аксиом.*

Теории, удовлетворяющие условиям (G1)–(G3) часто называют *геделевскими*.

Требование непротиворечивости — безусловное, поскольку в противоречивой теории выводится все, что угодно. Перечислимость — это некое конструктивное ограничение, которое заставляет нашу теорию быть более «сговорчивой», такую теорию проще анализировать алгоритмически, ее аксиомы и теоремы строятся некоторым регулярным образом примерно так же, как строится грамматика языка, т.е. «регулярность» — это залог «сговорчивости». Условие (G3), наоборот, тянет нашу теорию в сторону «строптивости», именно это условие позволяет выразить внутри самой теории предикат $\mathrm{Pr}(\ulcorner\varphi\urcorner)$, который говорит, что формула $\varphi$ доказуема в этой теории ($\ulcorner\varphi\urcorner$ означает взятие геделева номера формулы $\varphi$). Это делается с помощью специального кодирования формул и доказательств (геделевская нумерация) натуральными числами, что позволяет записать такой предикат в виде арифметической формулы. Конечно, строго говоря, теория доказывает лишь арифметические факты о натуральных числах: она не квантифицирует по формулам или формальным выводам своего собственного языка — это объекты метатеории, а присвоение им геделевых кодов есть интерпретация, которую мы задаем извне. Но даже этого вполне достаточно, чтобы предъявить пример формулы $G$ такой, что $G \leftrightarrow \neg\mathrm{Pr}(\ulcorner G\urcorner)$, т.е. истинность формулы равносильна ее недоказуемости. Мало того, в рамках второй теоремы о неполноте Гёдель в качестве такой формулы $G$ предъявил формулу, выражающую непротиворечивость теории: $\neg\mathrm{Pr}(\ulcorner\bot\urcorner)$. Иначе говоря, геделевская теория не способна ни доказать, ни опровергнуть свою собственную непротиворечивость.

Поэтому все геделевские теории «строптивые», но существует немало перечислимых теорий, которые не способны интерпретировать арифметику, и потому в большинстве своем являются «сговорчивыми», т.е. их можно относительно легко достроить до полных. К таковым теориям относятся, например,

- теория линейных порядков (достраивается до теории плотных линейных порядков без максимума и минимума);
- геометрия Тарского (полная);
- теория вещественно замкнутых полей (полная);
- теория алгебраически замкнутых полей характеристики 0 (полная);
- теория делимых абелевых групп без кручения (полная).

Однако чуть ниже мы увидим, что выразительная способность таких теорий оставляет желать лучшего.

С другой стороны, теории, способные многое выразить, такие как арифметика и теория множеств, обладают «геном строптивости» (G3), т.е. конструктивно принципиально непополняемы: в силу теоремы Гёделя о неполноте, сколько бы новых независимых аксиом мы не добавляли в их аксиоматику, полной теория не станет никогда. Качественный трансцендентный скачок тут происходит только в том случае, когда мы расширим такую «строптивую» теорию до множества всех истинных в ее стандартной модели формул (например, для арифметики Пеано это будет элементарная теория $Th(\mathbb{N})$). Но тогда теория станет неперечислимой, т.е. утратит «ген сговорчивости» (G2).

Таким образом, геделевские теории — это своего рода граница между пополняемыми и выразительными теориями первого порядка. В контексте изучения математики как иностранного языка, возможно, будет уместным сравнение этих двух типов теорий с разговорным и академическим языками в обычном языке или, скажем, с народной и высокой латынью средневековья.

**Теорема D2.17** (Łoś–Vaught test)**.** *Если выполняются два условия:*

**(1)** *формальная теория первого порядка имеет хотя бы одну бесконечную модель, но не имеет конечных моделей;*

**(2)** *теория является $\kappa$-категоричной для некоторого бесконечного кардинального числа $\kappa$,*

*тогда эта теория является полной.*[10]

С помощью этой теоремы можно доказать, например, такие факты: **1)** теория равенства с аксиомами, исключающими конечную область интерпретации (см. раздел B1.2.10), полна, поскольку она категорична в счетной мощности; **2)** теория $\mathrm{DLO}_\infty$ плотных линейных порядков без первого и последнего элемента (см. раздел B1.2.7) полна, поскольку она категорична в счетной мощности; **3)** теория DTFA делимых абелевых групп без кручения (см. раздел B1.2.7) полна, поскольку она категорична в несчетной мощности.

Из теста Лося-Воота и теоремы Морли мы получаем просто формулируемый факт: категоричная в какой-либо бесконечной мощности первопорядковая теория не является геделевой. Просто потому что такие теории полны, а геделевы теории — нет.

Говорят, что теория $T$ *допускает элиминацию кванторов*, если для всякой формулы $\varphi(\vec{p})$ языка этой теории существует бескванторная формула $\varphi_0(\vec{p})$ в языке этой теории такая, что $T \vdash \forall \vec{p}\ (\varphi \leftrightarrow \varphi_0)$. Простой пример: формула $(a \neq 0) \wedge \exists x\ (ax^2 + bx + c = 0)$ равносильна в RCF формуле $(a \neq 0) \wedge (b^2 - 4ac \geqslant 0)$. Заметим, что условие элиминации кванторов существенно лишь для предложений из «серой зоны», т.е. не являющихся теоремами или антитеоремами теории, а также для формул со свободными переменными, поскольку в любой теории всякая теорема доказуемо эквивалентна бескванторной формуле $\top$, всякая антитеорема — формуле $\bot$.

[10] Эта теорема была доказана Ежи Лосем (Jerzy Łoś) в 1954 году и независимо Робертом Вootом (Robert L. Vaught) также в 1954 году.

**Теорема D2.18** (Тарского-Зайденберга).
*Теория* RCF *допускает элиминацию кванторов.*[11]

Следующая теорема предоставляет еще один признак полноты теории, используя элиминацию кванторов.

**Теорема D2.19.** *Пусть $T$ — теория в некотором языке первого порядка $L$. Если*

**(1)** *теория $T$ допускает элиминацию кванторов;*

**(2)** *для любого замкнутого бескванторного предложения $\varphi$ языка $L$ теория $T$ доказывает либо $\varphi$, либо $\neg\varphi$,*

*тогда теория $T$ является полной.*

**Замечание**: Замкнутое бескванторное предложение строится из атомарных формул вида $P(t_1, \dots, t_n)$, где $t_k$ — термы без переменных, т.е. константы или комбинации констант и функциональных символов), а $P$ — предикатный символ, с помощью логических связок ($\neg$,□,□,$\to$,□). Например, если в языке есть константы $0, 1$ и предикат $<$, то $0 < 1$ и $\neg(1 = 0)$ — замкнутые бескванторные предложения.

Если теория $T$ допускает элиминацию кванторов, то любое замкнутое предложение $\sigma$ эквивалентно в $T$ некоторому замкнутому бескванторному предложению $\sigma'$, т.е. $T \vdash (\sigma \leftrightarrow \sigma')$. Если же выполняется второе условие теоремы — теория $T$ решает истинность всех замкнутых бескванторных предложений (т.е. для каждого такого $\sigma'$ либо $T \vdash \sigma'$, либо $T \vdash \neg\sigma'$), то она автоматически решает и истинность всех предложений. Следовательно, $T$ будет полной.

*Частный случай*: язык без констант. Если язык $L$ не содержит константных символов, то в нем нет нетривиальных замкнутых атомарных (или бескванторных) предложений, кроме тех, что эквивалентны $\top$ (истина) или $\bot$ (ложь). Таким образом, если теория $T$ в языке без констант непротиворечива и допускает элиминацию кванторов, то она автоматически полна.

Например, теория плотных линейных порядков без минимального и максимального элементов ($\mathrm{DLO}_\infty$) задается в языке без констант с одним предикатным символом $<$ (помимо $=$) и допускает элиминацию кванторов. Действительно, чтобы показать возможность элиминации кванторов, достаточно показать, что можно удалить один квантор существования. Любая формула, описывающая свойства $x$, сводится к одному из трех случаев:[12] 1) $x = p$; 2) $x < p$; 3) $q < x$, где $p, q$ — параметры (другие свободные переменные).

Формула $\exists x(x = p)$ равносильна бескванторной формуле $\top$ (ее свидетелем является параметр $p$).

Формула $\exists x(q < x) \wedge (x < p)$ равносильна формуле $(q < p)$ в силу аксиомы плотности порядка.

[11] Основная работа была проделана Альфредом Тарским. Он опубликовал свой результат об элиминации кванторов для вещественно замкнутых полей (и, как следствие, разрешимости элементарной алгебры и геометрии) в 1948 году в работе «A Decision Method for Elementary Algebra and Geometry». Абрахам Зайденберг в 1954 году предложил другое, более алгебраическое и, по мнению некоторых, более простое и естественное доказательство этого результата.

[12] Здесь мы сошлемся на известный факт о том, что любую формулу можно привести к предваренному виду (все кванторы впереди), а затем ее бескванторную часть привести к ДНФ, а также выразить квантор $\forall$ через $\exists$ и $\neg$, после чего останется только проносить $\exists$ в дизъюнкции атомарных конъюнкций, каковыми и являются представленные здесь случаи. Отметим также, что в силу связности порядка отрицания этих случаев сводятся к ним же, т.е. $\neg$ тоже устраним.

Формулы $\exists x(q < x)$ и $\exists x(x < p)$ равносильны формуле $\top$ в силу аксиомы отсутствия максимума и минимума.

Итак, $\mathrm{DLO}_\infty$ допускает элиминацию кванторов, при этом в ее языке нет констант, так что она полна.

Теория вещественно замкнутых полей (RCF) допускает элиминацию кванторов по теореме Тарского-Зайденберга. Замкнутые бескванторные предложения (отношения порядка и равенства между результатами полиномиальных выражений от констант) решаются аксиомами RCF. Отсюда следует ее полнота.

В завершение разговора о полноте теорий отметим, что сам термин «полнота» чрезвычайно нагружен в математике различными понятиями. Даже в этом курсе мы столкнулись со следующими видами полноты: семантическая полнота (она же полнота исчислений), полнота теории, полнота вещественных чисел, полная индукция. Поэтому данный термин нужно всегда использовать с осторожностью, указывая, какая именно полнота имеется в виду. Особенно это важно в лингвистическом аспекте изучения математики.

Таблица D2.2. Свойства некоторых первопорядковых теорий

| Теория | Гёделевость | Полнота | Катег. | Разреш. |
|---|---|---|---|---|
| Чистая теория равенства | негеделева | пополняема | ✓($\kappa \geqslant \omega$) | ✓ |
| Теория = с бесконечным носителем | негеделева | ✓ | ✓($\kappa \geqslant \omega$) | ✓ |
| $\mathrm{DLO}_\infty$ | негеделева | ✓ | ✓($\omega$) | ✓ |
| Теория групп | негеделева | x | x | x |
| DTFA | негеделева | ✓ | $\kappa > \omega$ | ✓ |
| ACF * | негеделева | пополняема | $\kappa > \omega$ | ✓ |
| Геометрия Тарского | негеделева | ✓ | x | ✓ |
| RCF | негеделева | ✓ | x | ✓ |
| Арифметика Пресбургера | негеделева | ✓ | x | ✓ |
| Q ** | геделева | существенно неполна*** | x | x |
| PA | геделева | существенно неполна | x | x |
| ZF/ZFC | геделева | существенно неполна | x | x |
| Th($\mathbb{N}$), Th($\mathbb{Z}$), Th($\mathbb{Q}$) | неперечислимая | ✓ | x | x |

* теория ACF алгебраически замкнутых полей достраивается до полной теории с помощью аксиомы, которая задает характеристику поля — 0 или простое $p$.

** аксиоматику Q мы дадим в следующем разделе, она отличается от PA отсутствием индукции и более слабым определением неравенства.

*** существенная неполнота означает, что эту теорию невозможно расширить до полной, сохраняя рекурсивную перечислимость аксиом.

### D2.2.5 Сводка результатов

Соберем изученный материал в короткую справочную таблицу классификации теорий (табл. D2.2) по таким признакам: геделевость или негеделевость (выделяя особо неперечислимый случай), полнота (пополняемость) или неполнота (существенная), категоричность (в счетной или несчетной мощности), разрешимость. Последнее свойство теорий мы не разбирали, но справочно заметим, что это очень полезное свойство теории, означающее, что существует алгоритм, который за конечное число шагов про любую замкнутую формулу языка теории может сообщить, является ли эта формула теоремой данной теории или не является (второе также важно уметь определять за конечное число шагов).

## D2.3. Упражнения

**Ex1.** Пусть $P$ — утверждение «Я в Париже», $F$ — «Я во Франции», $L$ — «Я в Лондоне», $E$ — «Я в Англии». Мы принимаем следующие географические факты как истинные посылки:

$$(P \to F) \wedge (L \to E).$$

Докажите, что из этих посылок логически следует утверждение:

$$(P \to E) \vee (L \to F)$$

(«Либо верно “если я в Париже, то я в Англии”, либо верно “если я в Лондоне, то я во Франции”»).

**Ex2.** Выведите правило *Введения существования* в заключении:

$$\varphi[a/t] \vdash \exists x \varphi[a/x],$$

где $t$ — терм.

**Ex3.** Используя аксиомы логики предикатов и правило Modus Ponens (а также Теорему о дедукции), выведите правило *Удаления всеобщности* в комбинации с импликацией (аксиома дистрибутивности):

$$\forall x(\varphi(x) \to \psi(x)) \vdash \forall x \varphi(x) \to \forall x \psi(x).$$

**Ex4.** Докажите следующую логическую эквивалентность (дистрибутивность квантора всеобщности относительно конъюнкции):

$$\vdash \forall x(\varphi(x) \wedge \psi(x)) \leftrightarrow (\forall x \varphi(x) \wedge \forall x \psi(x)).$$

**Ex5.** Докажите, что квантор существования дистрибутивен относительно дизъюнкции:

$$\vdash \exists x(\varphi(x) \vee \psi(x)) \leftrightarrow (\exists x \varphi(x) \vee \exists x \psi(x)).$$

**Ex6.** Докажите формулу «Принципа пьющего», которая классически общезначима, хотя и интуитивно парадоксальна:

$$\vdash \exists x(\varphi(x) \to \forall y \varphi(y)).$$

(Подсказка: Используйте Закон исключенного третьего для формулы $\forall y \varphi(y)$).

**Ex7.** Используя Теорему о дедукции, покажите, что если переменная $a$ не входит свободно в $\varphi$, то:

$$\vdash (\varphi \to \forall x \psi[a/x]) \leftrightarrow \forall x (\varphi \to \psi[a/x]).$$

**Ex8.** Выведите правило *Обобщения заключения*:

$$\Gamma \vdash \varphi \to \psi[a/x] \implies \Gamma \vdash \varphi \to \forall x \psi[a/x],$$

при условии, что $a$ не свободна в $\varphi$ и $\Gamma$.

**Ex9.** Докажите семантически, что из $\exists x \forall y \varphi(x, y)$ следует $\forall y \exists x \varphi(x, y)$.

**Ex10.** Пусть $\mathcal{M}_1 = \langle \mathbb{Q}, < \rangle$ и $\mathcal{M}_2 = \langle \mathbb{Z}, < \rangle$. Найдите предложение (замкнутую формулу) в языке порядка, которое истинно в $\mathcal{M}_1$, но ложно в $\mathcal{M}_2$.

**Ex11.** Рассмотрим язык, содержащий только символ сложения $+$.

1. Покажите, что в структуре $\langle \mathbb{N}, + \rangle$ (натуральные числа с нулем) отношение строгого порядка $x < y$ является определимым. Запишите соответствующую формулу.
2. Докажите, что в структуре $\langle \mathbb{Z}, + \rangle$ (целые числа) отношение $x < y$ НЕ определимо. (Подсказка: используйте автоморфизм $x \mapsto -x$).

**Ex12.** Рассмотрим структуру $\langle \mathbb{R}, \cdot \rangle$ (мультипликативная группа вещественных чисел).

1. Покажите, что множество неотрицательных чисел $\{x \in \mathbb{R} \mid x \geqslant 0\}$ определимо в этой структуре.
2. Покажите, что стандартное отношение порядка $x \leqslant y$ определимо в поле вещественных чисел $\langle \mathbb{R}, +, \cdot \rangle$, используя только алгебраические операции.

**Ex13.** Рассмотрим структуру $\langle \mathbb{R}, < \rangle$. Определите, какие из следующих множеств определимы в этой структуре:

1. Множество $\{0\}$;
2. Множество всех чисел, больших 5;
3. Интервал $(0, 1)$.

**Ex14.** Докажите, что структуры $\langle \mathbb{Q}, < \rangle$ и $\langle \mathbb{Q} \cup \{\pi\}, < \rangle$ (где $\pi$ рассматривается просто как еще одна точка в порядке) изоморфны.

**Ex15.** 1. Опишите счетную модель для теории $\mathrm{ACF}_0$ (Алгебраически замкнутые поля характеристики 0). (Подсказка: подумайте о замыкании $\mathbb{Q}$).

2. Докажите существование несчетной модели арифметики Пеано.

**Ex16.** Докажите, что теория структуры $\langle \mathbb{N}, < \rangle$ не является $\aleph_0$-категоричной. (Подсказка: рассмотрите модель, состоящую из двух копий $\mathbb{N}$, расположенных одна за другой).

**Ex17.** В теории плотных линейных порядков (DLO) элиминируйте кванторы из следующей формулы (найдите эквивалентную бескванторную формулу):

$$\exists x (a < x \wedge x < b).$$

**Ex18.** В теории DLO элиминируйте кванторы из формулы:

$$\forall x (a < x \to b < x).$$

**Ex19.** В теории равенства (с бесконечным носителем) элиминируйте квантор из формулы:

$$\exists x (x \neq a \wedge x \neq b).$$

**Ex20.** В теории вещественно замкнутых полей (RCF) определите условие на коэффициенты $a, b$ для формулы:

$$\exists x (ax + b > 0).$$

(Запишите эквивалентную бесквантерную формулу, включающую $a$ и $b$).

**Ex21.** В теории RCF элиминируйте квантор из формулы

$$\exists x (ax^2 + bx + c = 0).$$

**Ex22.** Пусть $L$ — язык с единственным символом бинарного предиката $\sim$. Пусть $T$ — теория, утверждающая, что:

- $\sim$ является отношением эквивалентности;
- Существует ровно два класса эквивалентности;
- Каждый класс эквивалентности бесконечен.

Используйте критерий Лося—Воота, чтобы доказать, что теория $T$ полна.

## Рекомендуемая литература

В этой главе мы заглянули в «машинное отделение» математики — в теорию логического вывода. Литература здесь отражает разные подходы к построению этого механизма.

Наиболее прямой и, возможно, самый интуитивный для начинающих — это аксиоматический (гильбертовский) подход, который и был подробно изложен в этой главе. Классическим учебником, который проводит по этому пути с образцовой ясностью, является «Введение в математическую логику» Э. Мендельсона [60]. В нем шаг за шагом, от простейших аксиом, строится вся конструкция исчисления высказываний и предикатов, доказываются ключевые метатеоремы.

Более современный и мощный взгляд на структуру доказательств предлагает теория структурного вывода, или теория секвенций, берущая начало от работ Г. Генцена [25]. Этот подход позволяет анализировать не только результат, но и саму «ткань» доказательства. Отличным введением в этот мир служит курс лекций С. Л. Кузнецова [70]. Для тех же, кто готов к глубокому погружению в самую суть теории доказательств, предназначен классический, хотя и непростой, труд К. Шютте [72].

Наконец, чтобы увидеть, как синтаксические конструкции логики «оживают» в математических структурах (моделях), стоит обратиться к учебнику Дж. Шёнфилда [61]. Он предлагает один из самых элегантных и кратких путей к центральным результатам теории моделей — теоремам о полноте, компактности и Лёвенгейма-Скулема, которые связывают миры синтаксиса и семантики, подробно рассмотренные во второй половине этой главы.

# ГЛАВА D3

# Арифметика

*Математика — царица наук, а теория чисел — царица математики.*

— Карл Фридрих Гаусс

Напомним, что первопорядковая арифметика Пеано задается в языке логики предикатов первого порядка с сигнатурой $\Sigma_{\text{PA}} \overset{\text{def}}{\rightleftharpoons} \langle =, 0, S, +, \cdot, < \rangle$ (помимо логических связок и кванторов). Предикатный символ неравенства $<$ можно как включать в сигнатуру, так и добавлять позже, используя его прямое определение через сложение (см. ниже (D3.2)). Здесь мы остановимся на варианте с рекурсивным определением неравенства, поэтому $<$ включено в сигнатуру сразу.

Приведем здесь еще раз полный список аксиом первопорядковой арифметики:

PA1 $a = a$; $(a = b) \to (b = a)$; $(a = b) \wedge (b = c) \to (a = c)$;

PA2 $a = b \to S(a) = S(b)$;

PA3 $S(a) = S(b) \to (a = b)$;

PA4 $S(a) \neq 0$;

PA5 $a + 0 = a$; $a + Sb = S(a + b)$;

PA6 $a \cdot 0 = 0$; $a \cdot Sb = ab + a$;

PA7 $\neg(a < 0)$; $(a < Sb) \leftrightarrow (a < b) \vee (a = b)$;

PA8 $\varphi[a/0] \wedge \forall x(\varphi[a/x] \to \varphi[a/Sx]) \to \forall y\ \varphi[a/y]$,

а также аксиомы и правила вывода логики предикатов:

PC1 универсальные замыкания всех подстановок всех формул PA во все тавтологии логики высказываний;

PC2 аксиомы для кванторов:

$$(\forall)\quad (\forall x\ \varphi[a/x]) \to \varphi[a/T]; \qquad (\exists)\quad \varphi[a/T] \to \exists x\ \varphi[a/x],$$

где $\varphi$ не содержит связанную переменную $x$, $T$ — любой терм теории;

PC3 правила вывода:

$$(MP)\quad \frac{\varphi,\quad \varphi \to \psi}{\psi}; \qquad (R1)\quad \frac{\varphi \to \psi}{\varphi \to \forall x\ \psi[a/x]};$$

$$(R1')\quad \frac{\psi}{\forall x\ \psi[a/x]}; \qquad (R2)\quad \frac{\psi \to \varphi}{(\exists x\ \psi[a/x]) \to \varphi},$$

где для правил (R1), (R1'), (R2) переменная $a$ не входит в $\varphi$ и ни в одну из активных (непогашенных) гипотез, от которых зависит вывод формулы в посылке этих правил.

Введем дополнительные предикаты по определению:

$$(a \leqslant b) \overset{\text{def}}{\leftrightarrow} (a < b) \vee (a = b), \quad (a > b) \overset{\text{def}}{\leftrightarrow} (b < a), \quad (a \geqslant b) \overset{\text{def}}{\leftrightarrow} (b \leqslant a).$$

## D3.1. Основные свойства

**Лемма D3.1.** $a \neq 0 \to \exists x\ a = Sx$.

*Доказательство.* Обозначим $\varphi(a) \equiv (a \neq 0 \to \exists x\ a = Sx)$ и докажем эту формулу индукцией по переменной $a$. При подстановке $[a/0]$ требуется доказать $0 \neq 0 \to \exists x\ 0 = Sx$. Эта формула истинна в силу ложного антецедента импликации (в силу PA1). Далее вводим гипотезу $\varphi(a)$, из которой нужно вывести $\varphi[a/Sa]$, т.е. формулу $Sa \neq 0 \to \exists x\ Sa = Sx$. Достаточно показать, что консеквент $\exists x\ Sa = Sx$ истинен. Для этого рассмотрим формулу $\psi(a,b) \equiv (Sa = Sb)$ и заметим, что подстановка $\psi[b/a]$ истинна, т.к. $Sa = Sa$ в силу первой аксиомы PA1, в которой мы произвели подстановку $[a/Sa]$. Кроме того, по правилу ($\exists$), понимая в нем под переменной $a$ переменную $b$, а под термом $T$ переменную $a$, получаем истинность импликации $\psi[b/a] \to \exists x\ \psi[b/x]$. Теперь по правилу MP от формул $\psi[b/a]$ и $\psi[b/a] \to \exists x\ \psi[b/x]$ приходим к формуле $\exists x\ \psi[b/x]$, т.е. $\exists x\ Sa = Sx$, что и требовалось. Далее, пользуясь тавтологией $\mathscr{A} \to (\mathscr{B} \to \mathscr{A})$ и правилом MP, подставляя вместо $\mathscr{A}$ формулу $\exists x\ Sa = Sx$ и вместо $\mathscr{B}$ формулу $Sa \neq 0$, получаем импликацию $Sa \neq 0 \to \exists x\ Sa = Sx$, т.е. формулу $\varphi[a/Sa]$.

Итак, в даже без использования гипотезы $\varphi(a)$ нам удалось вывести $\varphi[a/Sa]$. Следовательно, снова в силу тавтологии $\mathscr{A} \to (\mathscr{B} \to \mathscr{A})$ по правилу MP верна импликация $\varphi(a) \to \varphi[a/Sa]$, откуда по правилу обобщения (R1') получаем, что

$$\forall y\ \varphi[a/y] \to \varphi[a/Sy].$$

Теперь вместе с доказанной выше формулой $\varphi[a/0]$ по аксиоме индукции PA8 и по правилу MP приходим к выводу $\forall y\ \varphi[a/y]$. Снимая квантор по правилу ($\forall$), получаем утверждение леммы. □

**Замечание**: В доказательстве фактически не была использована индуктивная гипотеза $\varphi(a)$, и поэтому кажется, что использование индукции для доказательства леммы избыточно. Однако в данном случае индукция позволяет по сути использовать тот факт, что любое число есть либо ноль, либо последователь. Это зашито в посылке индукции. Не имея еще в запасе утверждения леммы, только с помощью индукции мы можем косвенно воспользоваться этим фактом и тем самым доказать лемму. Иначе говоря, аксиома индукции (и другие подобные схемы аксиом) не всегда применяется, так сказать, по прямому назначению. Имея лемму D3.1, мы теперь можем во многих случаях избежать применения индукции в доказательстве, просто рассматривая два возможных кейса: $a$ есть ноль или $a$ есть последователь. Тем не менее, лемма D3.1 не равносильна индукции, она гораздо слабее ее. Например, она не позволяет доказать коммутативность сложения в отсутствие индукции.

Арифметика с аксиомами PA1–PA6 плюс лемма D3.1 называется арифметикой **Робинсона** и обозначается Q. Неравенство в Q обычно задается определением в сильном

смысле (см. ниже). В этой арифметике невыводимы коммутативность и ассоциативность сложения и умножения, и многие другие полезные свойства натуральных чисел, что делает такую арифметику достаточно слабой. Однако арифметика Робинсона хороша тем, что она конечно аксиоматизируема (в ней нет схемы аксиом) и все еще можно реализовать кодирование формул по Гёделю, что делает ее (минимальной) геделевой теорией.

Еще одним свидетелем зазора между индукцией и леммой D3.1 является так называемая *сильная аксиома неравенства*, которую мы введем ниже, в ходе доказательства следующей основной теоремы.

**Теорема D3.1.** *В теории* PA *верны следующие теоремы (с учетом универсального замыкания формул):*

1° $a = b \to a + c = b + c$ [конгруэнтность $=$ относительно сложения];

2° $a + b = b + a$ [коммутативность сложения];

3° $a = b \to ac = bc$ [конгруэнтность $=$ относительно умножения];

4° $a + (b + c) = (a + b) + c$ [ассоциативность сложения];

5° $ab = ba$ [коммутативность умножения];

6° $a(b + c) = ab + ac$ [дистрибутивность];

7° $a(bc) = (ab)c$ [ассоциативность умножения];

8° $a = b \to (a < c) \leftrightarrow (b < c)$ [конгруэнтность $=$ относительно неравенства];

9° $a = b \to (c < a) \leftrightarrow (c < a)$ [конгруэнтность $=$ относительно неравенства];

10° $(a < b) \leftrightarrow (Sa < Sb)$ [согласованность порядка с $S$];

11° $(a + c = b + c) \to (a = b)$ [правило сокращения для $+$];

12° $(a < b) \leftrightarrow (a + c < b + c)$ [согласованность порядка с $+$];

13° $<$ есть линейный порядок;

14° $(c \neq 0) \to [(a < b) \leftrightarrow (ac < bc)$ [согласованность порядка с $\cdot$];

15° $(ac = bc) \wedge (c \neq 0) \to (a = b)$ [правило сокращения для $\cdot$];

16° $(a \leqslant b) \wedge (b < Sa) \to (b = a)$ [дискретность порядка];

17° $a \cdot S0 = a$ [нейтральность единицы];

18° $(a \cdot b = 0) \to (a = 0 \vee b = 0)$ [отсутствие делителей нуля].

*Доказательство.* Здесь с каждым шагом мы будем все меньше апеллировать к использованию аксиом логики и правил вывода, предполагая, что их применение на предыдущих шагах было достаточно убедительным. Это позволит нам сконцентрироваться на сути доказательств и не утонуть в море формальных преобразований.

**Конгруэнтность равенства относительно сложения** докажем индукцией по $c$. Пусть $\varphi(c) \overset{\text{def}}{\leftrightarrow} \forall x, y \ (x = y) \to (x + c = y + c)$. При замене $[c/0]$ необходимо показать, что $\forall x, y \ (x = y) \to (x + 0 = y + 0)$. Докажем вместо этого импликацию

$(a = b) \to (a + 0 = b + 0)$ со свободными переменными $a, b$. А для доказательства импликации воспользуемся теоремой о дедукции.

Введем гипотезу $(a = b)$. В силу PA5 имеем $a + 0 = a$ (более формально: в замкнутом виде PA5 имеет вид $\forall x\ (a + 0 = a)[a/x]$, откуда снятием квантора по аксиоме $(\forall)$ получаем $a + 0 = a$), откуда по транзитивности равенства заключаем, что $a + 0 = b$. Подставляя в PA5 $b$ вместо $a$ (а это делается тоже с помощью аксиомы $(\forall)$) видим, что $b + 0 = b$. Тогда в силу симметричности и транзитивности равенства приходим к $a + 0 = b + 0$.

Значит, по тереме о дедукции мы доказали импликацию $(a = b) \to (a + 0 = b + 0)$, после чего мы можем дважды навесить квантор всеобщности по правилу обобщения (R1'). В итоге получаем $\forall x, y\ (x = y) \to (x + 0 = y + 0)$, т.е. $\varphi[c/0]$.

Далее нужно доказать, что $\forall z\ \varphi(z) \to \varphi(Sz)$. Действуем похожим образом: докажем $\varphi(c) \to \varphi(Sc)$ и потом навесим квантор всеобщности по правилу обобщения. Введем индуктивную гипотезу $\varphi(c)$, т.е. $\forall x, y\ (x = y) \to (x + c = y + c)$. Здесь снова временно снимаем квантор всеобщности и рассматриваем формулу $(a = b) \to (a + c = b + c)$ в качестве гипотезы, при этом у нас переменные $a, b$ свежие, а переменная $c$ используется в гипотезе.

Введем еще одну гипотезу: $(a = b)$, тогда в рамках гипотез по правилу MP получаем формулу $a + c = b + c$. Далее, $a + Sc = S(a + c)$ по аксиоме PA5 (опять используем ее в замкнутой форме и снимаем квантор, заменяя переменные на нужные). Далее в аксиоме PA2, используя ее в замкнутой форме и снимая квантор всеобщности по аксиоме $(\forall)$ с заменой $[a/a + c; b/b + c]$, получаем формулу $(a + c = b + c) \to S(a + c) = S(b + c)$, что вместе с уже доказанным равенством $a + c = b + c$ по правилу MP дает нам $S(a + c) = S(b + c)$. Теперь по транзитивности равенства из доказанных выше формул получаем, что $a + Sc = S(b + c)$. Наконец, в силу PA5 и симметричности равенства имеем $S(b + c) = b + Sc$, откуда и из предыдущего равенства по транзитивности равенства получаем, что $a + Sc = b + Sc$.

По теореме о дедукции заключаем, что в рамках гипотезы $(a = b) \to (a + c = b + c)$ мы доказали импликацию $(a = b) \to (a + Sc = b + Sc)$, а значит, опять в силу теоремы о дедукции, мы доказали импликацию

$$[(a = b) \to (a + c = b + c)] \to [(a = b) \to (a + Sc = b + Sc)].$$

Далее, чтобы перейти к формуле $\varphi(c)$, сначала воспользуемся аксиомой $(\forall)$:

$$[\forall x, y\ (x = y) \to (x + c = y + c)] \to [(a = b) \to (a + c = b + c)],$$

откуда по предыдущему

$$[\forall x, y\ (x = y) \to (x + c = y + c)] \to [(a = b) \to (a + Sc = b + Sc)],$$

а поскольку слева в антецеденте импликации нет свободных переменных $a, b$, можно применить правило Бернайса (R1) и ввести квантор всеобщности в консеквент:

$$[\forall x, y\ (x = y) \to (x + c = y + c)] \to [\forall x, y\ (x = y) \to (x + Sc = y + Sc)],$$

что соответствует импликации $\varphi(c) \to \varphi(Sc)$, и это верно без ограничений на переменную $c$, а значит, по правилу обобщения: $\forall z\ \varphi(z) \to \varphi(Sz)$.

Таким образом у нас выведены формулы $\varphi(0)$ и $\forall z\ \varphi(z) \to \varphi(Sz)$. Чтобы соединить их конъюнкцией, воспользуемся тавтологией $\mathscr{A} \to (\mathscr{B} \to (\mathscr{A} \wedge \mathscr{B}))$, где вместо

$\mathscr{A}$ подставим $\varphi(0)$, а вместо $\mathscr{B}$ подставим $\forall z\ \varphi(z) \to \varphi(Sz)$, и дважды применим MP, после чего получим формулу $\varphi(0) \wedge \forall z(\varphi(z) \to \varphi(Sz))$, которая представляет собой антецедент аксиомы индукции PA8 с точностью до выбора связанных переменных.

Применяя правило MP, получаем, что $\forall z\ \varphi(z)$, что и требовалось.

**Коммутативность сложения** $(a + b = b + a)$ будем доказывать индукцией по $b$, точнее, будем вести индукцию по формуле $\varphi(b) \overset{\text{def}}{\leftrightarrow} \forall x\ x + b = b + x$. База этой индукции $\varphi(0)$ нами уже была доказана на стр. 118. Так что у нас есть тождество $\forall x\ x + 0 = 0 + x$. Введем гипотезу (Г1) $\forall x\ x + b = b + x$ и докажем отсюда, что $\forall x\ x + Sb = Sb + x$. Эту формулу мы тоже получим индукцией по формуле $\psi(c) \overset{\text{def}}{\leftrightarrow} c + Sb = Sb + c$.

Очевидно, что $\psi(0)$, т.к. это база первой индукции (в формулу $a + 0 = 0 + a$ вместо $a$ подставляем $Sb$, пользуясь аксиомой $(\forall)$ и MP). Введем гипотезу (Г2) $c + Sb = Sb + c$ и докажем, что $Sc + Sb = Sb + Sc$:

$$Sc + Sb \overset{\text{PA5}}{=\!=} S(Sc + b) \overset{\text{Г1,PA2}}{=\!=} S(b + Sc) \overset{\text{PA5,PA2}}{=\!=} SS(b + c) \overset{\text{Г1,PA2}}{=\!=}$$
$$SS(c + b) \overset{\text{PA5,PA2}}{=\!=} S(c + Sb) \overset{\text{Г2,PA2}}{=\!=} S(Sb + c) \overset{\text{PA5}}{=\!=} Sb + Sc.$$

Заметим, что почти всюду мы пишем использование PA2, которая позволяет заменять равное на равное под знаком оператора $S$, но на самом деле эта замена требует также использования аксиомы $(\forall)$, поскольку мы берем аксиомы PA в замкнутом виде и снимаем квантор $\forall$, заменяя переменные нужными нам термами, а затем мы также пользуемся правилом MP, чтобы от импликации в аксиоме PA2 перейти к тождеству из ее консеквента.

Итак, мы показали переход от формулы $\psi(c)$ к формуле $\psi(Sc)$ в рамках гипотезы (Г1), причем $c$ — это свободная переменная, не входящая в формулу внешней индукции по $b$, т.е. никак не связанная с гипотезой (Г1), значит,

$$(\text{Г1}) \vdash \psi(0) \wedge \forall x\ (\psi(x) \to \psi(Sx)),$$

откуда уже по индукции и в силу MP заключаем, что

$$(\text{Г1}) \vdash \forall x\ \psi(x),$$

т.е. в рамках гипотезы $\forall x\ x + b = b + x$ мы доказали $\forall x\ x + Sb = Sb + x$, т.е. теперь мы имеем

$$\varphi(0) \wedge \forall y\ (\varphi(y) \to \varphi(Sy)),$$

и теперь уже отсюда при помощи индукции и правила MP мы получаем окончательно формулу $\forall y\ \varphi(y)$, т.е. $\forall y \forall x\ x + y = y + x$, что и завершает доказательство коммутативности сложения.

Из коммутативности сложения легко следует конгруэнтность равенства относительно сложения по второму аргументу:

$$(a = b) \to (c + a = c + b),$$

так что в дальнейшем мы можем применять конгруэнтность равенства относительно сложения по любому из аргументов.

**Конгруэнтность равенства относительно умножения** также докажем индукцией по $c$. Пусть $\varphi(c) \overset{\text{def}}{\leftrightarrow} \forall x, y\ (x = y) \to (xc = yc)$. При $c = 0$ необходимо показать, что $\forall x, y\ (x = y) \to (x \cdot 0 = y \cdot 0)$. Докажем вместо этого импликацию $(a = b) \to (a \cdot 0 = b \cdot$

0) со свободными переменными $a, b$. А для доказательства импликации воспользуемся теоремой о дедукции.

Введем гипотезу $(a = b)$. В силу PA6 имеем $a \cdot 0 = 0$. Подставляя в PA6 $b$ вместо $a$, видим также, что $b \cdot 0 = 0$. Тогда в силу симметричности и транзитивности равенства приходим к $a \cdot 0 = b \cdot 0$.

Значит, по тереме о дедукции мы доказали импликацию $(a = b) \to (a \cdot 0 = b \cdot 0)$, после чего мы можем дважды навесить квантор всеобщности по правилу обобщения. В итоге получаем $\forall x, y\ (x = y) \to (x \cdot 0 = y \cdot 0)$, т.е. $\varphi(0)$.

Далее мы снижаем градус формальности и продвигаемся более широкими шагами. Нам необходимо показать в рамках гипотезы $(a = b) \to (ac = bc)$, что $(a = b) \to (a \cdot Sc = b \cdot Sc)$. Вводим гипотезу $a = b$, далее вычисляем по аксиомам:

$$a \cdot Sc \overset{\text{PA6}}{=\!=} ac + a \overset{Cong^+}{=\!=} bc + a \overset{Cong^+}{=\!=} bc + b \overset{\text{PA6}}{=\!=} b \cdot Sc,$$

где $Cong^+$ обозначает применение конгруэнтности сложения (по любому из аргументов).

Мы показали индуктивный переход для формулы $\varphi(c)$ (с учетом навешивания кванторов так же, как мы это делали при доказательстве конгруэнтности сложения).

Значит, по индукции и правилу MP заключаем, что $\forall z\ \varphi(z)$, что и требовалось.

**Ассоциативность сложения** доказывается индукцией по $c$. Обозначим

$$\varphi(c) \overset{\text{def}}{\rightleftharpoons} \forall x, y\ (x + (y + c) = (x + y) + c).$$

При $c = 0$ нужно получить равенство $(a + (b + 0) = (a + b) + 0)$ и затем замкнуть его кванторами по свободным переменным.

$$a + (b + 0) \overset{\text{PA5},Cong^+}{=\!=} a + b \overset{\text{PA5}}{=\!=} (a + b) + 0.$$

Конгруэнтность равенства относительно сложения здесь потребовалась для того, чтобы из равенства $b + 0 = b$ извлечь равенство $a + (b + 0) = a + b$.

Чтобы доказать индуктивный переход $\varphi(c) \to \varphi(Sc)$, докажем его сначала в бескванторной форме, вводя гипотезу (Г) $(a + (b + c) = (a + b) + c)$:

$$a + (b + Sc) \overset{\text{PA5},Cong^+}{=\!=} a + S(b + c) \overset{\text{PA5}}{=\!=} S(a + (b + c)) \overset{\text{PA2},\Gamma}{=\!=} S((a + b) + c) \overset{\text{PA5}}{=\!=} (a + b) + Sc,$$

где, как и выше, мы не указываем использование аксиомы $(\forall)$ при применении аксиом PA. Таким образом, в силу теоремы о дедукции, верна импликация:

$$[(a + (b + c) = (a + b) + c)] \to [(a + (b + Sc) = (a + b) + Sc)].$$

Далее, рассуждая так же, как при доказательстве конгруэнтности сложения, переходим к импликации с кванторами и получаем вывод $\varphi(c) \to \varphi(Sc)$. И далее по правилу обобщения получаем $\forall z\ \varphi(z) \to \varphi(Sz)$. Остается применить индукцию и получить окончательный вывод $\forall z\ \varphi(z)$.

**Коммутативность умножения** $ab = ba$ будем доказывать двумя вложенными индукциями аналогично доказательству коммутативности сложения. Внешняя индукция идет по $b$. Но сначала надо доказать, что $0 \cdot a = 0$ при любом $a$. Это делается индукцией по $a$. Действительно, $0 \cdot 0 = 0$ (PA6) и в рамках гипотезы $0 \cdot a = 0$ имеем

$$0 \cdot Sa \overset{\text{PA6}}{=\!=} (0 \cdot a) + 0 \overset{\text{PA5}}{=\!=} 0 \cdot a \overset{\text{гипотеза}}{=\!=\!=} 0,$$

так что в силу индукции $\forall x\ 0 \cdot x = 0$.

Теперь равенство $ab = ba$ при $b = 0$ очевидно, поскольку $a \cdot 0 = 0$ по аксиоме PA6 и $0 \cdot a = 0$ по доказанному.

Проверим индуктивный переход. Введем гипотезу (Г1) $\forall x\ xb = bx$. Необходимо доказать, что $\forall x\ x \cdot Sb = (Sb) \cdot x$. Докажем эту формулу индукцией в рамках гипотезы (Г1). При $x = 0$ равенство верно, т.к. оно является следствием полученного выше равенства для $b = 0$. Дальше действуем без кванторов для удобства. Введем гипотезу (Г2) $c \cdot Sb = (Sb) \cdot c$ и проверим равенство для $Sc$:

$$Sc \cdot Sb \overset{\text{PA6}}{=\!=} (Sc)b + Sc \overset{\text{Г1},Cong^+}{=\!=} bSc + Sc \overset{\text{PA5}}{=\!=} S(bSc + c) \overset{\text{PA6},Cong^+,\text{PA2}}{=\!=\!=} S((bc + b) + c),$$

$$Sb \cdot Sc \overset{\text{PA6}}{=\!=} (Sb)c + Sb \overset{\text{Г2},Cong^+}{=\!=} cSb + Sb \overset{\text{PA5}}{=\!=} S(cSb + b) \overset{\text{PA6},Cong^+,\text{PA2}}{=\!=\!=} S((cb + c) + b).$$

Справа у нас получились два терма, равенство которых устанавливается с помощью PA2, гипотезы Г1, конгруэнтности сложения, коммутативности сложения и ассоциативности сложения. Таким образом по транзитивности равенства получаем $Sc \cdot Sb = Sb \cdot Sc$, что завершает индуктивный переход для формулы $\forall x\ x \cdot Sb = (Sb) \cdot x$, и вместе с этим завершается индуктивный переход по переменной $b$ для формулы $\forall x\ xb = bx$, так что окончательно получаем $\forall x, y\ xy = yx$.

Из доказанной выше конгруэнтности равенства относительно умножения по первому аргументу и коммутативности умножения следует также и конгруэнтность равенства относительно умножения по второму аргументу.

**Дистрибутивность** сложения с умножением доказываем индукцией по $c$. Пусть $c = 0$, тогда

$$a(b + 0) = ab + a \cdot 0$$

в силу PA5, PA6, конгруэнтности сложения и умножения. Пусть верно, что $a(b + c) = ab + ac$, тогда

$$a(b + Sc) = a \cdot S(b + c) = a(b + c) + a = ab + (ac + a) = ab + aSc,$$

где мы воспользовались аксиомами PA5, PA6, гипотезой, ассоциативностью сложения, конгруэнтностью равенства относительно сложения и умножения. Тем самым индуктивный переход получен, и дистрибутивность доказана.

**Ассоциативность умножения** докажем индукцией по $c$. При $c = 0$ имеем

$$a(b \cdot 0) = a \cdot 0 = 0, \quad (ab) \cdot 0 = 0.$$

Вводя гипотезу $a(bc) = (ab)c$, получаем, что

$$a(bSc) = a(bc + b) = a(bc) + ab = (ab)c + ab = (ab)Sc,$$

что дает индуктивный переход и завершает доказательство ассоциативности умножения.

Теперь, имея ассоциативность и коммутативность сложения и умножения, мы можем автоматически расставлять скобки и менять местам операнды так, как нам выгодно для дальнейших выкладок. Мы также не будем больше ссылаться на свойство дистрибутивности и конгруэнтности равенства относительно сложения и умножения, поскольку они привычны на уровне автоматизма с детства. Важно, что мы их уже доказали в нашей системе аксиом.

Докажем одно вспомогательное утверждение, которое сильно упростит работу с неравенством.

**Лемма D3.2** (сильная аксиома неравенства)**.**

$$\text{PA7'} \qquad (a < b) \leftrightarrow \exists x\ b = a + Sx.$$

*Доказательство.* Воспользуемся индукцией по переменной $b$.

При $b = 0$ требуется вывести формулу $(a < 0) \leftrightarrow \exists x\ 0 = a + Sx$. Слева стоит ложная формула $a < 0$ (аксиома PA7). Справа, используя PA5 с подстановкой $[a/a, b/x]$, получаем $\exists x\ 0 = S(a + x)$, что ложно в силу PA4. Так что у нас в обеих частях эквиваленции стоят ложные формулы, и вся эквиваленция истинна при любом $a$. База индукции получена.

Введем индуктивную гипотезу $(a < b) \leftrightarrow \exists x\ b = a + Sx$ и докажем отсюда формулу $(a < Sb) \leftrightarrow \exists x\ Sb = a + Sx$.

Докажем слева направо. Пусть $a < Sb$, тогда $a = b$ или $a < b$ (PA7). Далее, пользуясь тавтологией $((\mathscr{A} \to \mathscr{C}) \wedge (\mathscr{B} \to \mathscr{C})) \to ((\mathscr{A} \vee \mathscr{B}) \to \mathscr{C})$, проведем вывод формулы $\exists x\ Sb = a + Sx$ методом разбора случаев, т.е. сначала покажем две импликации

$$(a = b) \to \exists x\ Sb = a + Sx, \quad (a < b) \to \exists x\ Sb = a + Sx, \tag{D3.1}$$

затем соединим их конъюнкцией, пользуясь тавтологией $\mathscr{A} \to (\mathscr{B} \to (\mathscr{A} \wedge \mathscr{B}))$, и затем по правилу MP получим импликацию $(a = b) \vee (a < b) \to \exists x\ Sb = a + Sx$, откуда уже по теореме о дедукции получим $(a < Sb) \to \exists x\ Sb = a + Sx$.

Докажем первую импликацию в (D3.1). Пусть $a = b$. Из аксиомы PA2 имеем $(a = b) \to (Sa = Sb)$, следовательно, $Sa = Sb$. Кроме того, $Sa = a + S0$ (PA2, PA5). Тогда $Sb = a + S0$, откуда получаем формулу $\exists x\ Sb = a + Sx$. Пользуясь теоремой о дедукции и гипотезой $a = b$, выводим первую импликацию в (D3.1).

Докажем вторую импликацию в (D3.1). Введем гипотезу $a < b$. Из индуктивной гипотезы получаем формулу $\exists x\ b = a + Sx$. Формула под квантором равносильна $Sb = a + S(Sx)$ (PA5, PA2, PA3), следовательно, $\exists y\ Sb = a + Sy$ (где $y = Sx$). Пользуясь теоремой о дедукции и гипотезой $a < b$, выводим вторую импликацию в (D3.1).

Отсюда, как уже упоминалось, выводится $(a = b) \vee (a < b) \to \exists x\ Sb = a + Sx$ и, как следствие, $(a < Sb) \to \exists x\ Sb = a + Sx$.

Обратно, пусть $\exists x\ Sb = a + Sx$. Поскольку $Sb = a + Sx$ равносильно $b = a + x$ (PA5, PA3, PA2), рассмотрим альтернативу (лемма D3.1): $(x = 0) \vee (x = Sy)$. Далее идем методом разбора случаев.

Пусть $x = 0$, тогда $b = a + 0 = a$. А из $a = b$ по аксиоме PA7 следует $a < Sb$.

Пусть $x = Sy$. Тогда из $b = a + x$ получаем, что $b = a + Sy$, откуда по индуктивной гипотезе получаем, что $a < b$, откуда уже по аксиоме PA7 приходим к формуле $a < Sb$.

Таким образом, по правилу разбора случаев и теореме о дедукции приходим к импликации $(\exists x\ Sb = a + Sx) \to (a < Sb)$.

Объединяя обе выведенные импликации в конъюнкцию, получаем формулу $(a < Sb) \leftrightarrow \exists x\ Sb = a + Sx$, и на этом индукция по переменной $b$ завершена. □

Сильное определение неравенства позволяет упростить ряд доказательств для неравенства, которые мы рассмотрим ниже. Заметим, что сильным оно называется потому, что для его получения из слабого определения (PA7) обязательно требуется индукция (что мы видели при доказательстве леммы). В то же время, если неравенство определить по формуле PA7', то доказательство PA7 может обойтись без индукции, если использовать утверждение леммы D3.1.

Действительно, пусть $<$ определено по формуле PA7', докажем, что для него выполняется PA7. Во-первых, нужно проверить, что $\neg(a < 0)$. Если предположить обратное

$a < 0$, то в силу PA7' имеем $\exists x\ 0 = a + Sx$, но в силу PA5 под квантором имеем $0 = S(a+x)$, а это противоречит PA4.

Докажем рекурсивную часть PA7: $(a < Sb) \leftrightarrow (a < b) \vee (a = b)$:

$$(a < Sb) \leftrightarrow \exists x\ Sb = a + Sx \leftrightarrow \exists x\ Sb = S(a + x) \leftrightarrow \exists x\ (b = a + x),$$

где мы использовали PA5, PA3, PA2, PA1. Теперь, в силу леммы D3.1 существует две альтернативы для $x$: $x = 0$ или $x = Sy$ для некоторого $y$. В первом случае равенство $b = a + x$ равносильно $b = a$ (PA5). Во втором случае $b = a + Sx$, что по определению PA7' равносильно $a < b$. Таким образом, $a < Sb$ равносильно $(a = b) \vee (a < b)$.

Этим мы завершили доказательство теоремы B2.3, приведенной в первой части книги.

В арифметике Робинсона Q, где вместо индукции используется лемма D3.1, наши два определения неравенства неравносильны (слабое выводится из сильного, но не наоборот).

**Конгруэнтность равенства относительно неравенства** по первому аргументу: $a = b \to (a < c) \leftrightarrow (b < c)$. Воспользуемся сильным определением неравенства. Поскольку неравенство $a < c$ равносильно формуле $\exists x\ c = a + Sx$, в рамках гипотезы $a = b$ эта формула равносильна $\exists x\ c = b + Sx$, а последняя формула равносильна неравенству $b < c$.

Аналогично получаем конгруэнтность равенства относительно неравенства по второму аргументу: $a = b \to (c < a) \leftrightarrow (c < b)$.

$$(c < a) \leftrightarrow \exists x\ a = c + Sx \leftrightarrow \exists x\ b = c + Sx \leftrightarrow (c < b)$$

в рамках гипотезы $a = b$.

Таким образом мы имеем конгруэнтность равенства относительно всех операций и предикатов нашей сигнатуры арифметики.

Докажем, что **порядок согласован с операцией** $S$, т.е. $(a < b) \leftrightarrow (Sa < Sb)$. Имея в распоряжении сильное определение неравенства, мы можем обойтись без индукции. Действительно,

$$(a < b) \leftrightarrow \exists x\ b = a + Sx \leftrightarrow \exists x\ Sb = S(a + Sx) \leftrightarrow \exists x\ Sb = Sa + Sx \leftrightarrow (Sa < Sb),$$

где мы воспользовались серий тождеств:

$$S(a + Sx) = S(Sx + a) = Sx + Sa = Sa + Sx,$$

которые следуют из выше доказанных свойств сложения.

Докажем **правило сокращения для сложения**: $a + c = b + c \to a = b$. Действуем индукцией по $c$. При $c = 0$ оно тавтологично. Примем гипотезу $a + c = b + c \to a = b$. Далее

$$(a + Sc = b + Sc) \to S(a + c) = S(b + c) \to a + c = b + c \to a = b.$$

Индуктивный шаг доказан. Вместе с конгруэнтностью это дает нам эквиваленцию

$$(a = b) \leftrightarrow (a + c = b + c)$$

для любых $a, b, c$.

Докажем, что **порядок согласован с операцией** $+$, т.е. $(a < b) \leftrightarrow (a + c < b + c)$.

$$(a < b) \leftrightarrow \exists x\ b = a + Sx \leftrightarrow \exists x\ b + c = a + Sx + c \leftrightarrow \exists x\ b + c = (a + c) + Sx \leftrightarrow (a + c < b + c).$$

Докажем, что отношение $<$ является строгим линейным порядком, т.е. оно антирефлексивно, транзитивно и связно.

Антирефлексивность $\neg(a < a)$: если $a < a$, то $\exists x\ a + 0 = a + Sx$, где по правилу сокращения получим $Sx = 0$, что противоречит PA4.

Транзитивность: $((a < b) \wedge (b < c)) \to (a < c)$. Из $b = a + Sx$ и $c = b + Sy$ следует, что $c = a + Sx + Sy = a + S(Sx + y)$, откуда $c = a + Sz$, где $z = Sx + y$, т.е. $a < c$.

Связность: $(a < b) \vee (a = b) \vee (b < a)$. Докажем индукцией по $a$. При $a = 0$ необходимо проверить формулу $(0 < b) \vee (0 = b) \vee (b < 0)$. По лемме D3.1 либо $b = 0$, либо $b = Sx$ при некотором $x$. В первом случае целевая формула верна за счет равенства, во втором случае перепишем равенство $b = Sx$ следующим образом: $b = 0 + Sx$, откуда по сильному определению неравенства получаем, что $0 < b$, и целевая формула снова верна.

Индуктивная гипотеза: $(a < b) \vee (a = b) \vee (b < a)$ для любого $b$. Нужно доказать, что $(Sa < b) \vee (Sa = b) \vee (b < Sa)$ для любого $b$. Если верно $(a = b) \vee (b < a)$, то по аксиоме PA7 имеем $b < Sa$. Если верно $a < b$, то $b = a + Sx = S(a + x) = S(x + a) = x + Sa = Sa + x$. Тогда если $x = 0$, то $Sa = b$, а если $x = Sy$, то $b = Sa + Sy$, т.е. по аксиоме PA7 имеем $Sa < b$. Во всех случаях мы получаем $(Sa < b) \vee (Sa = b) \vee (b < Sa)$ для любого $b$. Индукция завершена.

Кроме того, верно свойство *антисимметричности*: $(a < b) \to \neg(b < a)$. Действительно, если $(a < b) \wedge (b < a)$, то по транзитивности получаем $a < a$, что противоречит антирефлексивности. Антисимметричность превращает свойство связности в закон трихотомии: верна одна и только одна из альтернатив $(a < b)$, $(a = b)$, $(b < a)$.

Докажем, что **порядок согласован с операцией** $\cdot$, т.е. $(c \neq 0) \to [(a < b) \leftrightarrow (ac < bc)]$. Пусть $c \neq 0$, тогда $c = Sx$ по лемме D3.1. Пусть также $a < b$, тогда $b = a + Sy$ для некоторого $y$, тогда $bc = ac + cSy = ac + (yc + c) = ac + (yc + Sx) = ac + S(yc + x)$, откуда по сильному определению неравенства $ac < bc$. Таким образом доказана импликация в одну сторону.

Нам осталось показать, что если $c \neq 0$ и $ac < bc$, то $a < b$. Предположим, что это не верно, тогда по свойству трихотомии порядка имеем две альтернативы: $a = b$ или $b < a$. В первом случае будем иметь $ac = bc$ в силу конгруэнтности равенства относительно умножения, а во втором случае получим $bc < ac$ по первой части доказательства согласованности порядка с умножением (в рамках гипотезы $c \neq 0$). Тогда с учетом гипотезы $ac < bc$ и транзитивности неравенства получаем, что $ac < ac$, что противоречит антирефлексивности неравенства. Следовательно, предположение не верно, и $a < b$.

Докажем **правило сокращения для умножения**: $(ac = bc) \wedge (c \neq 0) \to (a = b)$. Предположим, что это не так, т.е. $(ac = bc) \wedge (c \neq 0) \wedge (a \neq b)$, тогда в силу трихотомии неравенства верно либо $a < b$, либо $b < a$. Пусть первое. Тогда по доказанному выше $ac < bc$, что исключает равенство $ac = bc$. Аналогично и в случае $b < a$. Следовательно, наше предположение не верно.

Докажем **дискретность порядка**: $(a \leqslant b) \wedge (b < Sa) \to (a = b)$. Пусть $(a \leqslant b) \wedge (b < Sa)$, тогда нам нужно исключить случай $a < b$. Предположим, что $a < b$. Из $b < Sa$ по аксиоме PA7 имеем $b < a$ или $b = a$, что вместе с предположением дает $a < a$. Противоречие.

Это свойство показывает, что между $a$ и $Sa$ на шкале натуральных чисел нет промежуточных чисел.

**Нейтральность единицы** $a \cdot S0 = a$ следует из аксиом и уже доказанных свойств: $a \cdot S0 = a \cdot 0 + a = a$.

**Отсутствие делителей нуля** $(ab = 0) \to (a = 0 \vee b = 0)$. Допустим, что $(a \neq 0) \wedge (b \neq 0)$, тогда по лемме D3.1 $a = Sx$ и $b = Sy$, откуда

$$ab = Sx \cdot Sy = Sx \cdot y + Sx = S(Sx \cdot y + x) \neq 0.$$

Теорема доказана полностью. □

Совокупность доказанных свойств говорит нам о том, что натуральные числа в аксиоматике Пеано образуют дискретное упорядоченное коммутативное полукольцо с единицей.

Теперь нам осталось полностью закрыть вопрос с конгруэнтностью равенства, доказав данные нами ранее общие формулы (B1.9).

**Теорема D3.2** (Конгруэнтность). *Пусть $T, T_1, T_2$ — произвольные термы языка PA, $\varphi$ — произвольная формула языка PA, тогда*

$$(T_1 = T_2) \to T[a/T_1] = T[a/T_2]; \tag{D3.2}$$
$$(T_1 = T_2) \to (\varphi[a/T_1] \leftrightarrow \varphi[a/T_2]), \tag{D3.3}$$

*причем указанные формулы справедливы и для любой другой свободной переменной (не только $a$).*

*Доказательство.* Теорема доказывается индукцией по построению термов и формул, а в качестве базы используются свойства конгруэнтности равенства, доказанные в теореме D3.1.

Для начала введем понятие *высоты терма* $H[T]$ и *высоты формулы* $H[\varphi]$, которое определяется рекурсивно, следуя правилам построения термов и формул:

**1)** для свободных переменных и констант: $H[a] = 0$, $H[0] = 0$ (в PA есть только одна константа 0);

**2)** для функциональных символов: $H[S(T)] = 1 + H[T]$, $H[T_1 + T_2] = 1 + \max(H[T_1], H[T_2])$, $H[T_1 \cdot T_2] = 1 + \max(H[T_1], H[T_2])$;

**3)** для атомарных формул: $H[T_1 = T_2] = 0$ (мы исключаем предикат $a < b$ из сигнатуры, считая, что он вводится определением PA7', это делает язык PA проще для анализа);

**4)** для логических связок и кванторов: $H[\neg\varphi] = 1 + H[\varphi]$, $H[\varphi \wedge \psi] = 1 + \max(H[\varphi], H[\psi])$, $H[\exists x\ \varphi[a/x]] = 1 + H[\varphi]$ (мы также сокращаем сигнатуру языка логики предикатов до символов $\neg, \wedge, \exists$, т.к. остальные логические связки и квантор выражаются через них).

Например, $H[\underbrace{S \ldots S}_{n} 0] = n$.

Доказательство (D3.2) и (D3.3) производится *полной* индукцией (см. раздел B2.1.3) по высоте термов и формул. Напомним, что в полной индукции формально не требуется отдельная проверка для случая $n = 0$, однако в этом случае индуктивный переход от меньшей чем $n = 0$ высоты к высоте $n = 0$ имеет тождественно истинную посылку индуктивной гипотезы, поэтому проверка индуктивного шага для $n = 0$ все равно должна проверяться отдельно.

**Доказательство для термов**.

Пусть $n = 0$, т.е. терм $T$ является атомарным, т.е. это либо переменная, либо константа. Здесь может быть три варианта:

**1)** $T \overset{\text{def}}{\rightleftharpoons} a$, т.е. терм $T$ есть та переменная, вместо которой производится подстановка, тогда (D3.2) имеет вид: $(T_1 = T_2) \to (T_1 = T_2)$, что является тавтологией;

**2)** $T \overset{\text{def}}{\rightleftharpoons} b$, т.е. терм $T$ есть переменная, отличная от переменной подстановки, тогда подстановка ничего не меняет, и (D3.2) имеет вид: $(T_1 = T_2) \to (b = b)$, что истинно в силу истинности консеквента;

**3)** $T \overset{\text{def}}{\rightleftharpoons} 0$ — здесь аналогичная ситуация: $(T_1 = T_2) \to (0 = 0)$.

Далее доказывается индуктивный переход для $n > 0$. Предположим, что (D3.2) выполняется для термов $T'$, высота которых меньше $n$. Надо показать конгруэнтность для терма $T$, высота дерева разбора которого равна $n$.

Например, пусть $T \overset{\text{def}}{\rightleftharpoons} S(T')$. В рамках индуктивной гипотезы выполняется импликация $(T_1 = T_2) \to (T'[a/T_1] = T'[a/T_2])$. Тогда берем аксиому PA2 и подставляем в нее вместо переменных $a, b$ термы $T'[a/T_1]$ и $T'[a/T_2]$, получаем импликацию $(T'[a/T_1] = T'[a/T_2]) \to S(T'[a/T_1]) = S(T'[a/T_2])$, откуда по транзитивности импликации приходим к формуле $(T_1 = T_2) \to S(T'[a/T_1]) = S(T'[a/T_2])$. Но термы в последнем равенстве — это графически (т.е. как текстовые строки) те же термы, которые получаются сразу из терма $T$: $S(T'[a/T_1]) \equiv T[a/T_1]$ и $S(T'[a/T_2]) \equiv T[a/T_2]$, где $\equiv$ означает графическое равенство термов. Таким образом, верна импликация $(T_1 = T_2) \to T[a/T_1] = T[a/T_2]$.

Аналогично действуем для двух других случаев конструкции терма $T$ — через сложение и умножение, применяя конгруэнтность, доказанную в теореме D3.1. В итоге у нас индуктивный переход доказан, и конгруэнтность равенства относительно термов доказана.

**Доказательство для формул.**

Пусть высота формулы $\varphi$ равна нулю, тогда это формула вида $T' = T''$, где в термах $T', T''$ подстановочная переменная $a$ может присутствовать, а может и отсутствовать, а также они могут быть замкнутыми. Необходимо показать импликацию

$$(T_1 = T_2) \to (T'[a/T_1] = T''[a/T_1]) \leftrightarrow (T'[a/T_2] = T''[a/T_2]).$$

Пусть $T_1 = T_2$ и для краткости обозначим $L_1 \equiv T'[a/T_1]$, $L_2 \equiv T'[a/T_2]$, $R_1 \equiv T''[a/T_1]$, $R_1 \equiv T''[a/T_2]$. Из доказанного для термов имеем: $T'[a/T_1] = T'[a/T_2]$, т.е. $L_1 = L_2$, и аналогично $T''[a/T_1] = T''[a/T_2]$, т.е. $R_1 = R_2$. Тогда по свойствам равенства (соответствующие подстановки в аксиому PA1) выводим, что $(L_1 = R_1) \leftrightarrow (L_2 = R_2)$, а это и есть требуемая эквиваленция.

Пусть теперь $n > 0$, тогда формула $\varphi$ имеет один из трех видов: $\neg\psi$, либо $\psi_1 \wedge \psi_2$, либо $\exists x\ \psi[b/x]$, где высота формул $\psi, \psi_1, \psi_2$ меньше $n$, т.е. для них действует индуктивная гипотеза (D3.3). Здесь квантором связывается переменная $b$, чтобы $a$ оставить как переменную подстановки (при этом ее может и не быть в формуле).

Пусть $\varphi \overset{\text{def}}{\leftrightarrow} \neg\psi$ и пусть $T_1 = T_2$. По предположению индукции имеем $(\psi[a/T_1] \leftrightarrow \psi[a/T_2])$. Здесь мы можем навесить на обе части эквиваленции отрицание по правилам исчисления высказываний, так что получим $\neg\psi[a/T_1] \leftrightarrow \neg\psi[a/T_2]$, откуда по теореме о дедукции получаем импликацию $(T_1 = T_2) \to \varphi[a/T_1] \leftrightarrow \varphi[a/T_2])$.

Аналогично поступаем для случая $\varphi \overset{\text{def}}{\leftrightarrow} \psi_1 \wedge \psi_2$.

Рассмотрим случай $\varphi \overset{\text{def}}{\leftrightarrow} \exists x\ \ \psi[b/x]$. Пусть $T_1 = T_2$, тогда по предположению индукции $\psi[a/T_1] \leftrightarrow \psi[a/T_2]$. Отсюда мы можем перейти к эквиваленции

$(\exists x \;\; \psi[a/T_1, b/x] \;\leftrightarrow\; \exists x \;\; \psi[a/T_2, b/x])$, воспользовавшись леммой D2.8. И таким образом получаем эквиваленцию $\varphi[a/T_1] \leftrightarrow \varphi[a/T_2]$.

Тем самым индуктивный переход доказан, и мы имеем конгруэнтность равенства относительно всех формул языка PA.

**Замечание**: мы не указывали здесь явным образом наличие свободных параметров у формул и термов для экономии места, хотя на самом деле все эти рассуждения должны проводится в предположении, что формулы и термы могут содержать произвольные свободные параметры $p_1, \ldots, p_k$. Это нужно для того, чтобы уметь переходить к формулам с кванторами, в которых количество параметров сокращается. □

Данная теорема сформулирована как схема теорем с привлечением нетерминальных символов, и потому не является теоремой PA в собственном смысле.

Несмотря на то, что формулировка и доказательство этой теоремы принадлежат мета-теории, реализация такой схемы для конкретных термов и формул доказуема средствами самой PA. Так, например, если вместо терма $T$ подставить элементарный терм $a + c$, а вместо термов $T_1$ и $T_2$ взять переменные $a$ и $b$, то подстановка $(T_1 = T_2) \to T[a/T_1] = T[a/T_2]$ превратится в пункт 1° теоремы D3.1. Собственно, имея общее мета-теоретическое доказательство, из него нетрудно «вытащить» доказательство для каждой конкретной формулы, ведь основная идея этого мета-доказательства состоит в том, что получение конгруэнции для более сложной формулы или терма сводится к получению конгруэнйии для более простых формул и термов при помощи аксиом PA, а для самых простых формул и термов у нас уже есть теорема D3.1.

Теорема о конгруэнтности, по сути, легитимизирует фундаментальный математический прием — замену равного на равное — внутри формальной системы PA. Это не просто техническая деталь, а мета-математическое обоснование корректности алгебраических преобразований.

## D3.2. Индукция

Напомним обозначения, введенные в разделе B2.1.3:

$$\begin{aligned} Ind_a[\varphi] &\overset{\text{def}}{\leftrightarrow} \varphi[a/0] \wedge \forall x \; (\varphi[a/x] \to \varphi[a/Sx]); \\ Prog_a[\varphi] &\overset{\text{def}}{\leftrightarrow} \forall x \; (\forall y < x : \; \varphi[a/y]) \to \varphi[a/x]; \\ Tot_a[\varphi] &\overset{\text{def}}{\leftrightarrow} \forall y \; \varphi[a/y], \end{aligned}$$

где формула $\varphi$ может содержать параметры, т.е. свободные переменные, отличные от $a$. Как обычно, для краткости мы их не указываем.

В этих обозначениях аксиома PA8 записывается как $Ind_a[\varphi] \to Tot_a[\varphi]$ и называется *локальной индукцией*. Кроме того, мы определили схему формул

$$Prog_a[\varphi] \to Tot_a[\varphi] \tag{D3.4}$$

как *полную индукцию* (иногда ее называют *возвратной*).

**Теорема D3.3.** *Схема полной индукции равносильна схеме локальной индукции над арифметикой Робинсона Q (с конгруэнтностью равенства).*

*Доказательство.* Покажем, что полная индукция влечет локальную. Для этого сначала докажем, что $Ind_a[\varphi] \to Prog_a[\varphi]$. Введем гипотезы: $Ind_a[\varphi]$ и антецедент импликации формулы прогрессивности $\forall y < a : \varphi(y)$). Необходимо проверить ее консеквент, т.е. формулу $\varphi(a)$. По лемме D3.1 (она входит в аксиоматику Q) для $a$ есть альтернатива: $a = 0$ или $a = Sz$ при некотором $z$.

Пусть $a = 0$, тогда $\varphi(a)$ истинна в силу гипотезы $Ind_a[\varphi]$.

Пусть $a = Sz$, тогда $z < a$ по аксиоме PA7 ($z < Sz$) и конгруэнтности равенства относительно неравенства, а тогда из гипотезы $\forall y < a : \varphi(y)$) по аксиоме ($\forall$) вытекает, что $\varphi(z)$, откуда в силу гипотезы $Ind_a[\varphi]$ получаем, что $\varphi(Sz)$, т.е. $\varphi(a)$.

Таким образом мы показали $Ind_a[\varphi] \to Prog_a[\varphi]$ (правило обобщения и теорема о дедукции).

Предположим, что верна схема полной индукции, т.е. $Prog_a[\varphi] \to Tot_a[\varphi]$ для любой формулы $\varphi$. Отсюда по доказанной импликации $Ind_a[\varphi] \to Prog_a[\varphi]$ и по свойству транзитивности импликации получаем, что $Ind_a[\varphi] \to Tot_a[\varphi]$, т.е. верна локальная индукция.

Отметим, что в данном случае для каждой *конкретной* формулы $\varphi$ из полной индукции следует локальная. Чтобы доказать обратное, мы вынуждены будем доказывать, что из всей схемы локальной индукции следует схема полной индукции, т.е. для одной отдельно взятой формулы это не работает.

Покажем, что локальная индукция влечет полную. Пусть $Ind_a[\psi] \to Tot_a[\psi]$ для любой формулы $\psi$. Введем гипотезу $Prog_a[\varphi]$. Пусть также $\psi(b) \overset{\text{def}}{\leftrightarrow} \forall y < b : \varphi[a/y]$. Применим локальную индукцию к формуле $\psi(b)$ в рамках гипотезы.

$\psi(0)$ истинно, поскольку $\psi(0) \leftrightarrow \forall y < 0 : \varphi(y)$. Раскрывая ограниченный квантор по определению (B2.2), получаем $\psi(0) \leftrightarrow \forall y\ (y < 0) \to \varphi(y)$. Импликация под квантором истинна в силу ложности $y < 0$ (PA7), следовательно, $\psi(0)$.

Покажем индуктивный шаг $b \to Sb$. Предположим, что $\psi(b)$, т.е. $\forall y < b : \varphi(y)$, тогда в силу гипотезы $Prog_a[\varphi]$ получаем $\varphi(b)$. Далее, $\psi(b)$ и $\varphi(b)$ вместе влекут $\forall y \leqslant b : \varphi(y)$, а последнее равносильно формуле $\forall y < Sb : \varphi(y)$, т.к. $(y \leqslant b) \leftrightarrow (y < Sb)$ (PA7), а последняя формула есть по определению $\psi(Sb)$. Таким образом $\psi(b) \to \psi(Sb)$, и индуктивный шаг доказан.

Применяя локальную индукцию к формуле $\psi$, получаем ее тотальность: $\forall z\ \psi(z)$. Теперь отсюда по аксиоме ($\forall$), заменяя $z$ на $Sa$, получаем $\psi(Sa)$, где переменная $a$ не связана никакой гипотезой. Раскрывая $\psi(Sa)$ по определению, получаем $\forall y < Sa : \varphi(y)$, откуда снова по аксиоме ($\forall$) получаем, заменяя $y$ на $a$, что $(a < Sa) \to \varphi(a)$. Антецедент последней импликации истинен (PA7), откуда мы выводим $\varphi(a)$.

Теперь, поскольку переменная $a$ свободна и не связана гипотезами, по правилу обобщения приходим к формуле $Tot_a[\varphi]$, и вывод формулы полной индукции для $\varphi$ получен. □

The fact that this equivalence is provable over a theory as weak as Q is a typical result in the field of Reverse Mathematics. This branch of logic seeks to determine the minimal axiomatic system required to prove a given theorem. In this case, the equivalence between the different forms of induction does not require the full power of PA, but only the axioms of Robinson's arithmetic (with congruence).

**Замечание**: тот факт, что эквивалентность индукций доказана над более слабой теорией (а именно, арифметика Робинсона с конгруэнцией равенства в виде (D3.2) и (D3.2)), является типичным результатом в науке под названием Обратная математика. Эта наука занимается поиском минимальных аксиоматик, достаточных для дока-

зательства известных теорем. В частности, здесь мы видим, что полная мощь PA не требуется, но некоторые ее следствия (лемма D3.1 и конгруэнтность) необходимы.

**Следствие D3.1.** *Следующая схема, которая называется фундированностью натуральных чисел,*

$$(WOP) \qquad (\exists y\ \varphi(y)) \to \exists x\ \varphi(x) \wedge \forall y < x :\ \neg\varphi(y),$$

*эквивалентна схеме локальной индукции. Формула $\varphi$ может содержать параметры.*

В разделе B2.1.3 мы показали, что схема WOP равносильна схеме полной индукции в чистом исчислении предикатов (без участия аксиом PA), поэтому с учетом теоремы D3.3, схема WOP равносильна схеме локальной индукции над базовой теорией Q (с аксиомами конгруэнтности (D3.2) и (D3.3)).

**Следствие D3.2.** *Принцип Ферма невозможности бесконечного спуска*

$$(\exists y\ \varphi(y)) \to \neg(\forall x\ (\varphi(x) \to \exists y < x :\ \varphi(y)))$$

*эквивалентен схеме индукции. Формула $\varphi$ может содержать параметры.*

Этот принцип, как было показано там же, тоже равносилен схеме полной индукции в чистом исчислении предикатов, а значит, эквивалентен локальной индукции над базовой теорией Q (с аксиомами конгруэнтности (D3.2) и (D3.3)).

В итоге можно сделать такой вывод: над базовой теорией Q (+конгруэнтность) следующие принципы равносильны

- схема локальной индукции;
- схема полной индукции;
- фундированность натуральных чисел;
- невозможность бесконечного спуска,

причем последние три равносильны в чистом исчислении предикатов.

## D3.3. Элементарная теория делимости

Покажем, как можно определить в PA некоторые простые функции. Например, часто используется функция предшественника $P(a)$. Это свежий функциональный символ, требующий своей аксиомы:

$$b = P(a) \overset{\text{def}}{\leftrightarrow} (a = 0 \to b = 0) \wedge (a \neq 0 \to S(b) = a).$$

Из леммы D3.1 следует, что это определение корректно задает тотальную функцию, т.е. для каждого $a$ число $b$ определено и единственно. Кроме того, для него работает конгруэнтность равенства, т.е. $(T_1 = T_2) \to P(T_1) = P(T_2)$, которая следует из того, что вместо равенства $P(T_1) = P(T_2)$ можно написать формулу $\exists x\ x = P(T_1) \wedge x = P(T_2)$, которая позволяет уйти от символа $P$ по определению.[1]

[1] Понятно, что внутри термов $T_1, T_2$ тоже могут встречаться символы $P$, но их количество конечно, и их подстановку в любой терм также можно раскрыть по определению. Тем самым мы за конечное число шагов можем развернуть формулу с участием символов $P$ в более длинную формулу без таковых. Например, если нам встречается выражение $a = b + P(c)$, то мы заменяем его формулой $\exists x\ (a = b + x) \wedge (x = P(c))$, после чего раскрываем равенство $x = P(c)$ по определению.

На самом деле, можно доказать одну общую мета-теорему о том, что если какой-то свежий функциональный символ $F$ вводится формулой в «старой» сигнатуре, для которой уже имеет место конгруэнтность равенства, то в таком случае конгруэнтность распространяется и на символ $F$, и на все термы и формулы, его содержащие. Проще всего такую теорему доказывать внешней (т.е. в мета-теории) индукцией по сложности формул, где сложность определяется количеством вхождений символа $F$ в данную формулу. Каждое раскрытие одного вхождения $F$ снижает сложность формулы в указанном смысле (хотя и увеличивает ее сложность в смысле сложности $H[\varphi]$, которую мы использовали ранее) и в итоге сводит к формулам без символа $F$, для которых уже все доказано.

Далее определим функцию **монус** (усеченное вычитание), которая на мета-уровне задается так:

$$a \dot{-} b = \begin{cases} c, & (b + c = a) \wedge (b < a), \\ 0, & b \geqslant a, \end{cases}$$

а в языке арифметики Пеано это записывается аксиомой:

$$(a \dot{-} b = c) \overset{\text{def}}{\leftrightarrow} (b < a \wedge b + c = a) \vee (b \geqslant a \wedge c = 0).$$

Для этого определения также можно доказать конгруэнтность равенства и корректность. Монус обладает следующими свойствами, которые мы оставим в качестве упражнения:

1° $a \dot{-} b \leqslant a$, причем $(a \dot{-} b = a) \leftrightarrow (a = 0 \vee b = 0)$;

2° $(a \dot{-} b = 0) \leftrightarrow (a \leqslant b)$;

3° $(a = (a \dot{-} b) + b) \leftrightarrow (b \leqslant a)$;

4° $(a + b) \dot{-} a = b$;

5° $a \dot{-} (b + c) = (a \dot{-} b) \dot{-} c$;

6° $c \cdot (a \dot{-} b) = (c \cdot a) \dot{-} (c \cdot b)$;

7° $(a \leqslant b) \to (a \dot{-} c \leqslant b \dot{-} c)$;

8° $(a \leqslant b) \to (c \dot{-} b \leqslant c \dot{-} a)$.

Кроме того, монус можно использовать для определения некоторых функций:

$$\max(a, b) \overset{\text{def}}{\rightleftharpoons} a + (b \dot{-} a), \qquad \min(a, b) \overset{\text{def}}{\rightleftharpoons} a \dot{-} (a \dot{-} b),$$
$$|a - b| \overset{\text{def}}{\rightleftharpoons} (a \dot{-} b) + (b \dot{-} a), \qquad [a = b] \overset{\text{def}}{\rightleftharpoons} 1 \dot{-} (|a - b|),$$

в последнем примере равенство не нужно воспринимать как арифметический предикат, эту запись нужно рассматривать целиком вместе с квадратными скобками как обозначение функции, равной 1 когда $a = b$, и 0 в противном случае (такой предикат называется *нотацией Айверсона*). И более сложное определение:

$$if(a = b, c, d) \overset{\text{def}}{\rightleftharpoons} ([a = b] \cdot c) + ((1 \dot{-} [a = b]) \cdot d),$$

которое выражает функцию, равную $c$, когда $a = b$, и $d$ в противном случае.

**Теорема D3.4** (о делении с остатком)**.** *Для любых натуральных чисел $a$ (делимое) и $b \neq 0$ (делитель) существуют единственные натуральные числа $q$ (неполное частное) и $r$ (остаток) такие, что $a = bq + r$ и $q \leqslant a,\ r < b$.*

*Доказательство.* Пусть даны числа $a \geqslant 0$ и $b > 0$. Определим формулу

$$\varphi(a, b, k) \overset{\text{def}}{\leftrightarrow} \exists x\ (a = bx + k).$$

Данная формула истинна на всех таких $k$, которые получаются вычитанием из $a$ чисел, кратных $b$.

Формула $\varphi$ истинна при некотором $k$, а именно, при $k = a$ (в качестве свидетеля нужно взять $x = 0$), следовательно, в силу принципа фундированности (WOP) существует наименьший $k$, удовлетворяющий этой формуле. Обозначим этот наименьший $k$ через $r$.

Поскольку $\varphi(a, b, r)$, то существует такой $q$, что $a = bq + r$. При этом очевидно, что $r < b$, т.к. в противном случае число $r' = r \dot{-} b$ также удовлетворяло бы формуле $\varphi$ (при $x = q+1$) в противоречии с тем, что $r$ — наименьшее из таких чисел. Кроме того, $q \leqslant a$, т.к. в противном случае ($q > a$) мы бы получили, что $bq + r > a$ для любого $r$, т.к. $b \geqslant 1$.

Осталось доказать единственность пары чисел $q, r$. Предположим, что пара $q', r'$ так же удовлетворяет равенству $a = bq' + r'$ и условию $r' < b$. Тогда из $a = bq + r$ получаем, что $bq + r = bq' + r'$.

Далее пользуемся трихотомией неравенства: $(r' < r) \vee (r' = r) \vee (r' > r)$. Легко видеть, что

$$(r = r') \leftrightarrow (bq = bq') \leftrightarrow (q = q'),$$

где мы использовали свойства сокращения для сложения и умножения.

Пусть $r' < r$, тогда $r = (r \dot{-} r') + r'$, откуда и из равенства $bq + r = bq' + r'$, подставляя $r$ и сокращая на $r'$, получаем, что $bq' + (r \dot{-} r') = bq$, откуда по сильному определению неравенства имеем $bq' \leqslant bq$, откуда, сокращая на $b \neq 0$, приходим к $q' \leqslant q$. Но по предыдущему $q' = q$ невозможно при условии $r' < r$, значит, $q' < q$.

Тогда $q = q' + Sx$ для некоторого $x$, откуда $bq = bq' + bx + b$ и, следовательно, $bx + b = r \dot{-} r'$. И здесь мы получаем противоречие, поскольку $r \dot{-} r' \leqslant r < b$, в то время как $bx + b \geqslant b$.

Следовательно, случай $r' < r$ невозможен. Аналогично исключается и случай $r' > r$. Таким образом, единственность неполного частного и остатка доказана. □

Приведенное доказательство уже практически выдержано в обычном математическом стиле, и поэтому занимает всего полстраницы. Если бы мы написали его столь же подробно, как, например, доказательство коммутативности сложения, оно оказалось бы в несколько раз длиннее и намного более сложным для восприятия. Поэтому, конечно, такие тщательные доказательства, как в теореме D3.1, нужны лишь тогда, когда перед нами стоит задача подтвердить способность формальной системы выразить и доказать известный нам арсенал средств и убедиться в том, что любое наше общематематическое доказательство может быть сведено к такому «математическому ассемблеру», каковым является формальный язык логики предикатов.

Пользуясь теоремой D3.4 о делении с остатком, несложно определить трехместный предикат $r = \mathrm{rem}(a, b)$, выражающий, что число $r$ есть остаток от деления $a$ на $b$:

$$r = \mathrm{rem}(a, b) \overset{\text{def}}{\leftrightarrow} (r < b) \wedge \exists q \leqslant a : (bq + r = a),$$

который к тому же является $\Delta_0$-формулой, т.е. не содержит неограниченных кванторов. Заметим, что мы можем расширить сигнатуру языка PA бинарным функциональным символом rem, введя для него данную формулу в качестве аксиомы, и тогда равенство в этой формуле мы можем понимать как настоящее равенство арифметики. При этом, как уже отмечалось ранее, такое определение расширяет конгруэнтность равенства на новый функциональный символ и все термы и формулы, его содержащие. Кроме того, все теоремы, которые могут быть доказаны в расширенном языке, эквивалентны соответствующим теоремам в исходном языке, если их раскрыть, используя данное определение. Поэтому, если мы хотим оставаться в исходном языке, то можем считать, что добавили только сокращение для формулы, а если нам удобнее понимать rem как функцию, то можем считать, что действуем в расширенном языке. В последнем случае нам тогда следует доопределить $\mathrm{rem}(a,b)$ на случай $b = 0$, например, нулем, поскольку в функциональный символ мы можем подставлять любой терм, в том числе константу 0, и следить во всех выкладках за тем, чтобы второй аргумент этой функции всегда оставался положительным, чтобы не получить некорректные результаты. Но как правило первого подхода достаточно.

Тот факт, что формула $r = \mathrm{rem}(a,b)$ определяет график функции (при $b \neq 0$), т.е. $r$ определяется однозначно для данных $a, b$, следует напрямую из утверждения единственности в теореме о делении с остатком.

Скажем, что число $b$ есть **делитель** числа $a$ (синоним: $a$ делится на $b$), если $\mathrm{rem}(a,b) = 0$, что короче записывается так: $b \mid a$. Давая определения, всегда полезно проверять крайние случаи. В данном случае имеем: $d \mid 0$ для любого $d$, в том числе $0 \mid 0$, однако $0 \nmid a$ при $a > 0$.

Определим такое понятие как *наибольший общий делитель* (gcd):

$$d = \gcd(a,b) \overset{\text{def}}{\leftrightarrow} (d \mid a) \wedge (d \mid b) \wedge \forall x\, ((x \mid a) \wedge (x \mid b) \to (x \leqslant d)).$$

С точки зрения изучения математики как языка весьма полезно время от времени записывать такие определения. Заметим, что если $a = b = 0$, то наибольшего общего делителя не существует, формула $d = \gcd(0,0)$ является ложной при любом $d$. Во всех остальных случаях $\gcd(a,b)$ существует. Например, если $a > 0, b = 0$, то $\gcd(a,b) = a$.

Далее мы можем определить предикат

$$a \perp b \overset{\text{def}}{\leftrightarrow} 1 = \gcd(a,b),$$

который выражает факт **взаимной простоты** чисел $a$ и $b$. Заметим, что $a \perp 1$ при любом $a$, включая $a = 0$.

Аналогично определим предикат «быть простым числом»

$$Prime(a) \overset{\text{def}}{\leftrightarrow} (a > 1) \wedge \forall x\, ((x \mid a) \to (x = 1 \vee x = a)).$$

А здесь мы сразу запретили числу $a$ быть 0 или 1. Подробно понятие простого числа мы обсуждали в разделе A2.1, в том числе выяснили необходимость такого запрета.

**Лемма D3.3** (о простом делителе). *Если число $a$ имеет нетривиальный делитель ($> 1$), то оно имеет и простой делитель.*

*Доказательство.* Применим полную индукцию по числу $a$. Для случаев $a = 0$ и $a = 1$ проверка тривиальна: у нуля все простые числа являются делителями, а у единицы

нет никаких нетривиальных делителей. Для $a = 2$ ответ очевиден, т.к. 2 есть простое число. Далее можем применять индуктивный переход, предполагая, что для всех чисел меньше $a$ утверждение верно. Если $a$ имеет только два делителя (1 и $a$), то оно уже простое. Если у $a$ есть еще какой-то делитель $b$, то $a = bq$ при некотором $q$ (теорема о делении с остатком), причем $1 < b, q < a$, а для них работает предположение индукции, так что существует простое $p \mid b$, а значит $p \mid a$. Индукция завершена. □

Покажем еще несколько простых фактов из теории чисел.

**Лемма D3.4** (тождество Безу)**.**
*Для любых $a$ и $b$, одновременно не равных нулю, существуют такие $s$ и $t$, что* $\gcd(a, b) = |as - bt|$.

*Доказательство.* Для $a = 0$ или $b = 0$ (при условии, что они одновременно не равны 0) доказательство очевидно. Поэтому пусть $a, b > 0$. Рассмотрим такую формулу:

$$\varphi(a, b, d) \overset{\text{def}}{\leftrightarrow} (d > 0) \wedge \exists s, t\ (d = |as - bt|),$$

т.е. эта формула истинна для тех и только тех $d$, которые являются линейными комбинациями $a$ и $b$. У этой формулы есть свидетели, например, $d = a$, поскольку в этом случае $d = |a \cdot 1 - b \cdot 0|$. Следовательно, применяя WOP, находим наименьший такой $d$, который обозначим за $d_0$, кроме того, $d_0 = |as - bt|$ для некоторых $s, t$.

Покажем, что $d_0 \mid a$. По теореме о делении с остатком $a = qd_0 + r$ или $r = a \div qd_0$, $r < d_0$. Для определенности предположим, что $as \geqslant bt$, тогда $r = a \div q(as \div bt)$, откуда видно, что $r$ является линейной комбинацией $a$ и $b$, т.е. $\varphi(a, b, r)$ и при этом $r < d_0$. Поскольку $d_0$ есть минимальный свидетель $\varphi$, $r$ не может быть положительным, а значит, $r = 0$, откуда следует, что $d_0 \mid a$. Аналогично доказывается, что $d_0 \mid b$. Таким образом $d_0$ есть делитель $a$ и $b$.

Пусть теперь какой-то $d$ тоже является их делителем, т.е. $a = kd$ и $b = ld$, тогда подставим в представление $d_0$ эти выражения, получим: $d_0 = |kds - ldt|$, откуда будет следовать, что[2] $d \mid d_0$, а значит, $d \leqslant d_0$. □

Итак, наибольший общий делитель $a, b$ есть их линейная комбинация.

**Лемма D3.5** (Эвклида)**.**
*Если $p$ — простое число и $p \mid ab$, то $(p \mid a) \vee (p \mid b)$.*

*Доказательство.* Предположим, что $p \nmid a$, тогда $\gcd(a, p) = 1$, и в силу тождества Безу имеем $1 = |as - pt|$ для некоторых $s, t$. Умножим обе части равенства на $b$: $b = |abs - ptb|$. Разность делится на $p$, т.к. $ab$ делится на $p$, следовательно, $p \mid b$.

Аналогично, если $p \nmid b$, то приходим к $p \mid a$. □

Лемма Эвклида является фундаментальным свойством целых чисел, а ее обобщение на произвольные кольца позволяет рассматривать т.н. *факториальные кольца*, обладающие свойствами, очень похожими на свойства кольца целых чисел.

**Лемма D3.6** (Гаусса)**.** *Если $c \mid ab$ и $c \perp b$, то $c \mid a$.*

[2] Делитель одного из множителей делит произведение, а делитель всех слагаемых делит сумму. Элементарные свойства делимости мы не будем здесь доказывать.

*Доказательство.* Поскольку $c \perp b$, по тождеству Безу $1 = |cs - bt|$ и, следовательно, $a = |acs - abt|$, откуда видно, что $c \mid a$. □

Доказанные леммы прямиком выводят нас на **Основную теорему арифметики** (ОТА): *всякое натуральное число $n > 1$ есть произведение простых чисел, причем это разложение единственно с точностью до порядка множителей*. И снова мы утыкаемся здесь в проблему, что без возможности говорить о произвольных конечных наборах чисел мы не в состоянии даже сформулировать ОТА!

Уместна следующая аналогия с разговорным языком. Представим себе, что мы пытаемся рассказать историю на языке, в котором есть только местоимения единственного числа (он, она, оно) и собственные имена, но нет существительных для групп (семья, толпа, команда). Мы можем сказать: «Он любит ее». Но мы не можем сказать: «Команда выиграла матч».

Язык PA без кодирования — это как разговорный язык без существительных для групп. Он может говорить только об отдельных числах. Но удивительная сила PA заключается в том, что в этом языке мы можем (с помощью гениального решения Гёделя) рассуждать о кодах произвольных конечных последовательностей. Число-код становится именем для целой последовательности $\langle x_1, \dots, x_n \rangle$. И как только у нас появляется это имя, мы можем делать утверждения о самой последовательности: какова ее длина, из чего она состоит, является ли она перестановкой другой последовательности и т.д. В том числе формулировать и доказывать ОТА и многие другие теоремы теории чисел.

Этот, на первый взгляд, чисто технический прием кодирования имеет колоссальное философское и практическое значение. Способность языка арифметики с помощью чисел-кодов описывать собственные синтаксические конструкции (формулы, доказательства) и операции над ними (вывод) лежит в основе теории вычислимости. Именно геделевское кодирование позволяет доказать существование универсальной вычислимой функции — теоретического аналога современного компьютера, способного выполнить любой алгоритм, если ему на вход подать число-код этого алгоритма.

Таким образом, «язык», на котором работает любой искусственный интеллект, в конечном счете сводится к арифметике. Вся сложность его программ, архитектур нейронных сетей и алгоритмов обучения может быть закодирована натуральными числами и описана формулами языка PA. Это и есть та самая «архитектура математической мысли», о которой говорится в подзаголовке книги, воплощенная в кремнии.

## D3.4. Кодирование последовательностей

Мы рассмотрим здесь классический способ кодирования последовательностей, идея которого принадлежит Гёделю. Способ основан на использовании китайской теоремы об остатках, которая позволяет волшебным образом кодировать произвольные последовательности натуральных чисел всего лишь парами специально подобранных чисел.

Но для начала получим еще один важный результат.

**Теорема D3.5.** *Пусть $a \perp b$, тогда для любого $c$ и любого $r < b$ существует $i < b$ такое, что $r = \mathrm{rem}(c + ai, b)$.*

По сути, теорема утверждает, что отображение $i \mapsto \mathrm{rem}(c + ai)$ является сюръекцией (а заодно и инъекцией) как функция, аргументы и значения которой лежат в множестве $\{0, \dots, b - 1\}$.

*Доказательство.* Во-первых, рассмотрим крайние случаи, когда $b$ есть ноль или единица. Ясно, что при $b = 0$ теорема тавтологична из-за ложной посылки. При $b = 1$ и любом $a$ для $r$ и $i$ остается единственный вариант $r = 0 = i$, и он, очевидно, верен, т.к. $\forall x\ \mathrm{rem}(x, 1) = 0$.

Пусть теперь $b > 1$ (откуда автоматически следует, что $a > 0$). Заметим, что если мы докажем теорему для $c = 0$, то для других $c$ она доказывается легко. Действительно, пусть требуется получить $r = \mathrm{rem}(c + ai, b)$, т.е. $c + ai = bq + r$ при некотором $q$. В то же время $c = bq' + r'$, где $r' < b$. Отсюда легко видеть, что $q' \leqslant q$ (иначе получаем $c \geqslant bq + b + r' > bq + r = c + ai \geqslant c$), тогда $ai = b(q \dot{-} q') + (r \dot{-} r')$, если $r \geqslant r'$, и $ai = b(q \dot{-} q' \dot{-} 1) + (b \dot{-} r') + r$, если $r < r'$ (в этом случае исключено равенство $q = q'$). В обоих случаях мы знаем, чему должен быть равен $\mathrm{rem}(ai, b)$ — это либо $r \dot{-} \mathrm{rem}(c, b)$, либо $(b \dot{-} \mathrm{rem}(c, b)) + r$.

Осталось доказать теорему для $c = 0$. Этот случай тоже можно упростить, а именно, доказать его только для $r = 1$. Действительно, если мы нашли $i$ такое, что $\mathrm{rem}(ai, b) = 1$, то для любого $r < b$ нужно взять $\mathrm{rem}(ri, b)$ вместо $i$, т.к. если $ai = bq+1$, то $a\,\mathrm{rem}(ri, b) = a(ri \dot{-} bq') = ari \dot{-} abq' = (bq + 1)r \dot{-} abq' = bq'' + r$.

Осталось доказать теорему для $c = 0$ и $b = 1$, т.е. что найдется такое $i$, что $\mathrm{rem}(ai, b) = 1$. По тождеству Безу $1 = |as - bt|$ при некоторых $s, t$, т.к. $a \perp b$. Тогда, как легко видеть, $\mathrm{rem}(as, b) = 1$, т.е. $s$ — это искомое $i$. □

**Теорема D3.6** (китайская теорема об остатках (КТО)). *Пусть $m_0, \ldots, m_{n-1}$ попарно взаимно простые числа, тогда для любых натуральных чисел $x_i < m_i$ существует такое число $N$, что $x_i = \mathrm{rem}(N, m_i)$ для всех $i \leqslant n$. Кроме того, если числа $N_1$ и $N_2$ удовлетворяют таким условиям, то $|N_1 - N_2|$ делится на $m_0 \cdot \ldots \cdot m_{n-1}$.*

Представьте, что у вас есть несколько будильников. Первый звонит каждые $m_0$ минут, второй — каждые $m_1$ минут, и так далее. Если вы знаете, сколько времени прошло с последнего звонка каждого будильника $(x_0, x_1, \ldots, x_{n-1})$, и периоды $m_i$ попарно взаимно просты, то вы можете однозначно определить момент времени по модулю $m_0 \cdot m_1 \cdot \ldots \cdot m_{n-1}$.

Приведенный вариант китайской теоремы об остатках требует квантификации по двум последовательностям $m_i$ и $x_i$, что невозможно без умения кодировать произвольные последовательности одним (или двумя) натуральным числом. Поэтому стандартный вариант этой теоремы мы сможем доказать только после определения кодирования последовательностей. Проблема в том, что для кодирования последовательностей нам тоже нужна КТО, но в урезанном виде, а именно, когда обе последовательности (модулей и остатков) задаются некоторой формулой языка PA с ограниченным числом параметров. Поскольку в самостоятельном виде такая усеченная формулировка КТО с точки зрения теории чисел не интересна, мы встроим ее непосредственно в доказательство леммы, обеспечивающей кодирование последовательностей.

Далее определим $\beta$-функцию Гёделя:

$$b = \beta(c, d, i) \overset{\text{def}}{\leftrightarrow} b = \mathrm{rem}(c, 1 + (i + 1) \cdot d),$$

или в функциональной записи $\beta(c, d, i) = \mathrm{rem}(c, 1 + (i + 1) \cdot d)$. Отметим, что это определение также является $\Delta_0$-формулой.

Идея кодировки состоит в том, что произвольная конечная последовательность $\langle x_0, x_1, \ldots, x_{n-1}\rangle$ кодируется не одним числом, а парой чисел $\langle c, d\rangle$. Затем эту пару можно «упаковать» в одно число $a$ с помощью стандартной диагональной нумерации Кантора:

$a = 1/2(c+d)(c+d+1)+d$, которая легко определима в PA.[3] Число $d$ выбирается так, чтобы модули $m_i = 1 + (i+1)d$ для $i < n$ были попарно взаимно простыми, что обеспечивает возможность применить КТО и найти такое $c$, чтобы выполнялась система равенств с остатками:

$$(x_0 = \beta(c,d,0)) \wedge (x_1 = \beta(c,d,1)) \wedge \ldots \wedge (x_{n-1} = \beta(c,d,n-1)), \tag{D3.5}$$

означающая, что нам удалось зашифровать последовательность $\langle x_0, x_1, \ldots, x_{n-1}\rangle$ двумя числами. В некоторых источниках используется кодирование последовательности $\langle n, x_0, x_1, \ldots, x_{n-1}\rangle$, в которой на первом месте стоит ее длина. В таком случае мы можем сразу же извлечь длину закодированной последовательности как $\beta(c,d,0)$, чтобы в дальнейшем использовать это ограничение.

Стоит подчеркнуть, что сама по себе $\beta$-функция тотальна, т.е. ее значение корректно определено для любых натуральных $c, d, i$, включая нулевые значения. Это значит, что в принципе любая пара чисел $c, d$ (или одно число, если мы используем канторовское кодирование пар) определяет какую-то бесконечную последовательность (которая стабилизируется, т.к. начиная с некоторого $i$ значение $\beta$-функции становится равным $c$), а значит, и какую-то конечную последовательность произвольной наперед заданной длины. [4]

Заслуга китайской теоремы об остатках состоит в том, что верно и обратное: если у нас уже каким-то способом задана конечная последовательность (произвольно выбранной длины), то ей обязательно соответствует некоторый код $\langle c, d\rangle$, причем таких кодов на самом деле бесконечно много, т.к. $c$ определяется с точностью до слагаемого, кратного произведению всех модулей $m_i = 1 + (i+1)d$ (при данной длине последовательности).

Далее мы докажем не прямую теорему о кодировании, которая говорит, что для каждой последовательности существует код в виде пары чисел $c, d$, поскольку мы еще не умеем квантифицировать по последовательностям, а рекурсивную теорему о дописывании, которая говорит, что, имея код какой-то последовательности, мы можем построить код последовательности, продолженной одним произвольным числом. Эту теорему будет удобно использовать в доказательствах по индукции.

**Теорема D3.7** (о дописывании последовательности)**.** *Пусть даны числа $c, d \geqslant 0$ и $n > 0$. Тогда для любого $x$ существуют числа $c', d' > 0$ такие, что*

$$(\forall i < n : \beta(c,d,i) = \beta(c',d',i)) \wedge (x = \beta(c',d',n)),$$

*Доказательство.* Введем локальные обозначения:

$$m_i \overset{\text{def}}{\rightleftharpoons} 1 + (i+1)d', \quad x_i \overset{\text{def}}{\rightleftharpoons} \beta(c,d,i), \quad x_n \overset{\text{def}}{\rightleftharpoons} x.$$

[3] Рекомендуем проверить самостоятельно, что диагональная нумерация Кантора есть биекция между парами натуральных чисел и натуральными числами. Канторовская нумерация хороша тем, что она не использует в своем определении ничего, кроме базовых арифметических операций.

[4] Существует и другой, алгебраически изящный, но менее практичный для целей формализации PA способ кодирования конечных двоичных последовательностей — матрицами из свободной полугруппы $SL_2(\mathbb{N})$ (см. Часть I, раздел B2.3.2). Однако, в отличие от $\beta$-функции, предикат, «извлекающий» $i$-й элемент из кода-матрицы, был бы чрезвычайно сложной формулой в языке PA, поскольку процесс декодирования эквивалентен разложению в непрерывную дробь. Это делает данный метод неудобным для доказательства теорем о неполноте, где простота и низкая арифметическая сложность предиката доказуемости имеют решающее значение.

**Шаг 1**: выбор $d'$. Нам нужно, чтобы $d'$ гарантировало выполнение двух условий: **а)** модули должны быть больше, чем кодируемые числа, т.е. для любого $i \leqslant n$ должно быть $x_i < m_i$. **б)** модули $m_i$ для $i \leqslant n$ должны быть попарно взаимно простыми.

Оба условия можно удовлетворить одним махом. Возьмем число $M$, которое больше всех членов последовательности $x_i$ и ее длины $n+1$. Фактически нужно взять $\max(n, x_0, \ldots, x_n) + 1$, а формально в условиях PA достаточно показать, что такое $M$ существует. Для этого по индукции докажем формулу

$$\varphi(c,d,k) \overset{\text{def}}{\leftrightarrow} (k \leqslant n) \to \exists M\ \forall i \leqslant k : (M > x_i) \wedge (M > k),$$

где индукция ведется по переменной $k$. Действительно, при $k = 0$ свидетелем будет $M = \max(x_0, 1) + 1$. Далее, если $\varphi(c,d,k)$ верно, то есть имеется свидетель $M$ для данного $k$, то для $k+1$ есть два варианта: $k+1 \leqslant n$ и $k+1 > n$. Во втором случае формула истинна из-за ложности антецедента импликации, а в первом случае в качестве свидетеля можно взять $\max(M, x_{k+1}) + 1$. Этим завершается индукция по $k$, откуда следует, что $\forall k\ \varphi(c,d,k)$, а значит, по правилу конкретизации $\varphi(c,d,n)$, что означает наличие нужного нам $M$.

Теперь выберем $d' > 0$ как такое число, которое кратно всем числам от 1 до $M$. В обычной теории чисел, мы сказали бы, что таким числом может быть факториал $M!$. Однако пока у нас нет еще кодирования последовательностей, мы не можем определить функцию факториала, но мы можем доказать по индукции, что $\forall M \exists d' > 0 : \forall i \leqslant M : i \mid d'$. В индуктивном шаге доказательства как раз и будет скрываться определение факториала.

Проверка условия **а)**: очевидно, что $x_i < M \leqslant d' < 1 + (i+1)d' = m_i$. Условие выполнено.

Проверка условия **б)**: допустим, что модули $m_i = 1 + (i+1)d'$ и $m_j = 1 + (j+1)d'$, где $i \neq j$, не взаимно просты. Значит, у них есть общий нетривиальный делитель, а значит, и общий простой делитель $p$. Тогда $p$ делит их разность: $p \mid |m_j - m_i|$, то есть $p \mid d'|j-i|$. Следовательно, $p$ делит либо $|j-i|$, либо $d'$ (лемма Эвклида). Но $p$ не может делить $d'$. Если бы $p \mid d'$, то так как $m_i = 1 + (i+1)d'$, остаток от деления $m_i$ на $p$ был бы 1. Но мы предположили, что $p \mid m_i$, т.е. остаток равен 0. Противоречие. Значит, $p$ должен делить $|j-i|$. Но $|j-i| \leqslant n < M$. Любое число, меньшее $M$, и любой его простой делитель (включая $p$) являются делителями числа $d'$ по его построению. Таким образом, из $p \mid |j-i|$ следует $p \mid d'$. А это, как мы только что видели, невозможно. Вывод: никакого общего нетривиального делителя у двух различных модулей не существует, т.е. модули $m_i$ попарно взаимно просты.

**Шаг 2**: Применение китайской теоремы об остатках. Теперь, когда мы нашли $d'$ и получили набор попарно взаимно простых модулей $m_0, \ldots, m_n$, определяемых формулой $1 + (i+1)d'$ $(i \leqslant n)$, КТО утверждает, что для набора $x_0, \ldots, x_n$ существует число $c'$ такое, что $x_i = \mathrm{rem}(c', m_i)$ для $i \leqslant n$. Здесь мы встроим доказательство КТО для нашего конкретного случая модулей и остатков.

Рассмотрим формулу в рамках уже доказанных свойств $x_i$ и $m_i$:

$$\varphi(c,d,d',n,x,k) \overset{\text{def}}{\leftrightarrow} (k \leqslant n) \to \exists C\ \forall i \leqslant k : x_i = \beta(C,d',i),$$

где $x_i = \beta(c,d,i)$ при $i < n$ и $x_n = x$. Докажем ее индукцией по $k$.

При $k = 0$ требуется проверить, что $\exists C\ x_0 = \beta(C,d',0)$, т.е. что $x_0 = \mathrm{rem}(C, 1+d')$ при некотором $C$. Поскольку $x_0 < 1 + d'$, можно в качестве $C$ взять само $x_0$.

Индуктивная гипотеза: $\varphi(c,d,d',n,x,k)$. Нужно доказать $\varphi(c,d,d',n,x,k+1)$. Из гипотезы следует, что существует такое $C_k$, что для всех $i \leqslant k$ имеем $x_i = \beta(C_k,d',i)$, т.е. $x_i = \mathrm{rem}(C_k,m_i)$. Нужно построить $C_{k+1}$ так, чтобы для всех $i \leqslant k+1$ было $x_i = \mathrm{rem}(C_{k+1},m_i)$.

Индукцией несложно показать, что для любого $i \leqslant k$ существует $D_i > 0$, кратное всем $m_0,\ldots,m_i$ ($\forall j \leqslant i : m_j \mid D_i$), затем конкретизировать $i$, подставив в место него $k$, и по принципу WOP (он эквивалентен индукции) выбрать наименьшее из таковых $D_k$. Фактически это означает, что $D_k$ есть наименьшее общее кратное $m_0,\ldots,m_k$. А так как все $m_i$ попарно взаимно просты, то[5] $D_k = m_0 \cdot \ldots \cdot m_k$.

Заметим, что $D_k \perp m_{k+1}$, т.к. если простое $p \mid D_k$, то существует $i \leqslant k$ такое, что $p \mid m_i$. Действительно, если $p \mid D_k$ и $\forall i \leqslant k : p \nmid m_i$, то $D_k = pq$, при этом $m_i \mid D_k$ и $\forall i \leqslant k : m_i \perp p$, откуда по лемме Гаусса $\forall i \leqslant k : m_i \mid q$ в противоречии с минимальностью $D_k$. Следовательно, если $p \mid D_k$, то $\exists i \leqslant k : p \mid m_i$. Но тогда этот $m_i$ не взаимно прост с $m_{k+1}$ в противоречии с их построением.

Имеем: $D_k \perp m_{k+1}$, $x_{k+1} < m_{k+1}$, тогда по теореме D3.5 существует $j < m_{k+1}$ такое, что $x_{k+1} = \mathrm{rem}(C_k + D_k \cdot j, m_{k+1})$. Положим $C_{k+1} \overset{\text{def}}{\rightleftharpoons} C_k + D_k \cdot j$. Далее заметим, что для $i \leqslant k$ имеем $\mathrm{rem}(C_k + D_k \cdot j, m_i) = \mathrm{rem}(C_k, m_i) = x_i$, т.к. $m_i \mid D_k$.

Таким образом, для $C = C_{k+1}$ получаем, что $\forall i \leqslant k+1 : x_i = \mathrm{rem}(C,m_i) = \beta(C,d',i)$, т.е. верна формула $\varphi(c,d,d',n,x,k+1)$. На этом индукция завершается.

Делая подстановку $[k/n]$ в формуле $\varphi$, приходим к тому, что $\exists C \ \ \forall i \leqslant n : x_i = \beta(C,d',i)$. Выбирая в качестве искомого $c'$ данное $C$, завершаем доказательство теоремы. □

С этой теоремой мы теперь можем строить конечные начальные отрезки, возникающие в рекурсивных определениях. Например, мы хотим определить формулу графика экспоненты с основанием $b$:

$$y = b^n \overset{\text{def}}{\leftrightarrow} \exists c,d\ (\beta(c,d,0) = 1) \wedge (\beta(c,d,n) = y) \wedge \forall i < n : (\beta(c,d,i+1) = b \cdot \beta(c,d,i)). \quad \text{(D3.6)}$$

Фактически эта формула утверждает следующее: существует код $c,d$ такой последовательности $\langle x_0,\ldots,x_n\rangle$, что $x_0 = 1$, для каждого $i < n$ $x_{i+1} = b \cdot x_i$ и $x_n = y$, т.е. утверждается не просто существование числа $b^n$, а всего отрезка функции экспоненты от 0 до $n$. Более того, имя код $c,d$, мы можем восстановить всю последовательность до $n$-го члена (что происходит после $n$ — формула не уточняет).

Для доказательства корректности определения и тотальности экспоненты нам нужна предыдущая теорема. Корректность означает, что такие $c,d$ с указанными свойствами действительно существуют для каждого $n$. Тотальность — это формула $\forall n \exists y\ (y = b^n)$, которая следует из корректности. Доказываем индукцией по $n$. При $n = 0$ требуется доказать, что существуют $y,c,d$ такие, что $\beta(c,d,0) = y = 1$. Так как $\beta(c,d,0) = \mathrm{rem}(c,1+d)$, то достаточно взять $c = 1$ и $d = 1$. Пусть для $n$ такой $y$ существует, т.е. есть необходимые $c,d$, определяющие график экспоненты от 0 до $n$. Тогда по теореме D3.7 для $x = b \cdot y$ существуют $c',d'$ такие, что

$$b \cdot y = \beta(c',d',n+1) = b \cdot \beta(c,d,n) \wedge \forall i \leqslant n : \beta(c',d',i) = \beta(c,d,i),$$

[5] Опять-таки, напрямую мы не можем определить такое произведение, поэтому пользуемся индукцией.

т.е. в качестве значения $y$, соответствующего $n+1$, берется $b \cdot y$, где $y$ соответствует $n$. Индукционный шаг завершен.

Для доказательства функциональности этого соответствия, т.е. условия, что если $y = b^n$ и $y' = b^n$, то $y = y'$, можно взять одну пару $c, d$ и вторую пару $c', d'$ — свидетелей формулы (D3.6), и убедиться полной индукцией, что они задают одну и ту же последовательность для $i = 0, \ldots, n$.

Таким образом у нас имеется формула языка PA, определяющая функцию $y = b^n$, причем эта формула принадлежит классу $\Sigma_1$-формул, т.е. это формула с ограниченными кванторами, предваренная несколькими неограниченными кванторами существования.

Итак, леммы о дописывании достаточно для первых нетривиальных рекурсивных функций, в частности, для функции $y = 2^n$ (достаточно взять $b = 2$). Это уже дает достаточную кодирующую силу для многих последующих синтаксических конструкций: ограниченных произведений, конечных списков символов и, в конечном счете, формулировок КТО и ОТА в виде настоящих формул о кодах последовательностей.

Здесь возникает естественный вопрос: почему же тогда различают арифметику с экспонентой и арифметику без экспоненты? Ответ зависит от того, что именно имеется в виду. Если речь идет о полной PA, то добавление нового функционального символа для экспоненты вместе с определяющими его аксиомами дает лишь консервативное расширение (расширение с помощью определений): формулы становятся короче, а доказательства читабельнее, но новых арифметических следствий не появляется, поскольку PA уже доказывает, что график экспоненты тотален и функционален. Однако в слабых фрагментах арифметики ситуация меняется. Например, в теориях лишь с ограниченной индукцией тотальность экспоненты может быть недоказуемой, и добавление ее в качестве аксиомы действительно увеличивает силу теории. Таким образом, в полной PA экспонента «спрятана» внутри самой теории, тогда как в более слабых арифметиках она отмечает реальную границу того, что теория способна доказать.

Здесь мы вплотную подошли к центральному результату теории доказательств, который характеризует класс всех вычислимых (частично рекурсивных) функций.

**Теорема D3.8** (основная теорема формальной арифметики)**.** *График любой (частично) рекурсивной функции можно определить* $\Sigma_1$*-формулой арифметики* PA*.*

Доказательство данной теоремы уже не входит в круг задач этой книги, но на примере с определением экспоненты уже хорошо видно, как это возможно сделать в общем виде, отталкиваясь от рекурсивного определения функции.

Наконец, ответим на главный вопрос этого раздела — *как мы теперь можем определять квантификацию по произвольным конечным последовательностям?* Ответ уже был продемонстрирован на примере (D3.6) определения экспоненты: нужно ввести новые кванторы с использованием кодов последовательностей.

Так, если мы хотим сказать, что для любой (или некоторой) последовательности $\langle x_0, \ldots, x_n \rangle$ выполняется какое-то свойство $\varphi$, то мы должны будем написать $\forall c, d$ (соответственно, $\exists c, d$) и далее в свойстве $\varphi$ всюду заменить $x_i$ на $\beta(c, d, i)$, используя ограниченные кванторы по переменной $i$ ($\forall i \leqslant n$ или $\exists i \leqslant n$). Хотя не каждая пара $c, d$ является осмысленным кодом, предикат $\varphi$ строится настолько строгим, что он будет истинным только для тех кодов, которые декодируются в последовательности с нужными свойствами, и ложным для всех остальных кодов.

Вот как будет формулироваться этим способом китайская теорема об остатках в общем виде (первая часть, про существование $N$):

$$\forall n\ \forall c,d\ [\forall i,j \leqslant n : (i \neq j) \to \beta(c,d,i) \perp \beta(c,d,j)] \to$$
$$\forall c',d' \Big( [\forall i \leqslant n : \beta(c',d',i) < \beta(c,d,i)] \to [\exists N\ \forall i \leqslant n : \beta(c',d',i) = \mathrm{rem}(N, \beta(c,d,i))] \Big).$$

В посылке заявляется, что все члены последовательности $\langle m_0, \dots, m_n \rangle$ (где $m_i = \beta(c,d,i)$), попарно взаимно просты, а в выводе для произвольной последовательности $\langle x_0, \dots, x_n \rangle$ заявляется, что если все $x_i < m_i$ (где $x_i = \beta(c',d',i)$), то существует такое $N$, что $x_i = \mathrm{rem}(N, m_i)$ для всех $i \leqslant n$. Как видим, мы обошлись замкнутой формулой языка PA с добавленными предикатами, выражающими функцию остатка и $\beta$-функцию Гёделя.

Аналогично можно выразить, например, **основную теорему арифметики**. Но для более компактного и понятного ее написания введем еще несколько вспомогательных предикатов:

$$a = Prod(c,d,m) \overset{\text{def}}{\leftrightarrow} \exists c',d'\ (a = \beta(c',d',m)) \wedge \beta(c',d',0) = \beta(c,d,0) \wedge$$
$$\forall i < m : \beta(c',d',i+1) = \beta(c',d',i) \cdot \beta(c,d,i+1)$$

выражает, что $a$ есть произведение всех первых $m+1$ членов последовательности, закодированной $c,d$;

$$Factor(c,d,n,m) \overset{\text{def}}{\leftrightarrow} (n = Prod(c,d,m)) \wedge (\forall i \leqslant m : Prime(\beta(c,d,i))) \wedge$$
$$(\forall i < m : \beta(c,d,i) \leqslant \beta(c,d,i+1))$$

который выражает тот факт, что $c,d$ кодируют возрастающую факторизационную последовательность числа $n$, включающую ровно $m+1$ простых факторов.

Тогда формулировка ОТА имеет вид:

**Теорема D3.9** (основная теорема арифметики)**.** *Для любого натурального $n > 1$ существует единственное разложение в произведение простых чисел:*

$$\forall n > 1 : [\exists m \exists c,d\ Factor(c,d,n,m)] \wedge \forall c',c'',d',d'',m',m''$$
$$[Factor(c',d',n,m') \wedge Factor(c'',d'',n,m'') \to$$
$$(m' = m'') \wedge \forall i \leqslant m' : \beta(c',d',i) = \beta(c'',d'',i)],$$

*т.е. для любого $n$, во-первых, существует его возрастающая факторизационная последовательность, во-вторых, она единственная.*

Тот факт, что разложение числа на простые множители определяется с точностью до порядка множителей, мы выразили тем, что отсортированная в порядке возрастания последовательность факторов единственная.

Отметим, что представленный здесь способ кодирования — далеко не единственный. Более того, в зависимости от выбранной аксиоматики можно использовать наиболее комфортные способы кодирования. Например, если мы сразу включаем в список аксиом определение экспоненты и аксиому ее тотальности, то кодирование становится чем-то вроде легкой прогулки в летнем саду. Если же мы, наоборот, стремимся к

минимализму вроде арифметики Робинсона, то внутреннее тотальное кодирование силами арифметики становится невозможным, хотя мета-теоретическими методами все еще можно кодировать последовательности, а для каждого конкретного случая кода можно найти его реализацию в Q, что позволяет доказать теорему Гёделя о неполноте даже для Q. Промежуточные варианты используют, например, кратное применение канторовского диагонального кодирования для последовательностей заданной конечной длины, кодирование полиномиальным способом (в позиционной системе счисления) для последовательностей с равномерно ограниченными значениями и т.п.

## D3.5. К теоремам Гёделя и Тарского

Теперь у нас есть все ингредиенты, необходимые для того, чтобы сжимать конечные списки натуральных чисел в отдельные квантифицируемые объекты теории PA: $\beta$-функция Гёделя из раздела D3.4, при желании — диагональная нумерация Кантора, конкретные иллюстрации вроде экспоненты (D3.6), а также приведенные выше внутренние формулировки КТО и ОТА. Зафиксируем инъективное присвоение чисел каждому символу логического алфавита и арифметической сигнатуры — та же идея, что и присвоение кодовых позиций символам в Unicode. Любая формула есть конечная строка символов, а значит, она определяет конечную последовательность числовых кодов. Как и в разделе D3.4, закодируем эту последовательность парой $\langle c, d\rangle$ с помощью $\beta$-функции Гёделя, а затем объединим $c$ и $d$ в одно натуральное число диагональной нумерацией Кантора. Это число — при зафиксированном присвоении кодов символам — мы и называем *геделевым номером* $\ulcorner \gamma \urcorner$ выражения $\gamma$, в согласии с обозначением, введенным в главе D2. Формальные доказательства, представленные в виде конечных структурированных списков формул и шагов вывода, получают числовые коды посредством того же механизма.

Обозначим через $\mathscr{L}(\mathrm{PA})$ множество всех формул этого языка. Как и в разделе C1.4.3, будем обозначать через $\mathbb{N}$ построенную там стандартную модель PA. Напомним (см. теорему о корректности вывода на стр. 219), что первопорядковый вывод корректен. Следовательно, PA *корректна* относительно своей стандартной модели $\mathbb{N}$: всякая теорема PA истинна в $\mathbb{N}$. Эта семантическая связь принципиально важна для приводимых ниже доказательств неполноты.

Для любого натурального числа $n$ обозначим через $\underline{n}$ соответствующий нумерал теории PA, определяемый как $\underbrace{S \ldots S}_{n} 0$.

**Теорема D3.10** (лемма о диагонализации)**.** *Для всякой формулы* $\Phi(a)$ *языка* $\mathscr{L}(\mathrm{PA})$*, содержащей свободно не более одной переменной* $a$*, существует такое предложение* $\theta$*, что*

$$\mathrm{PA} \vdash \theta \leftrightarrow \Phi(\underline{\ulcorner \theta \urcorner}).$$

*Доказательство.* На мета-уровне определим тотальную примитивно рекурсивную функцию $F : \omega \to \omega$ следующим образом. Если $n$ есть геделев номер некоторой формулы $\psi(a)$, содержащей свободно не более переменной $a$, положим $F(n) \stackrel{\text{def}}{=\!=} \ulcorner \psi(\underline{n}) \urcorner$, где $\psi(\underline{n})$ обозначает результат подстановки нумерала $\underline{n}$ вместо каждого свободного вхождения $a$ в $\psi$ (если $a$ не входит свободно в $\psi$, строка не меняется). В противном

случае положим $F(n) \stackrel{\text{def}}{\rightleftharpoons} 0$. Тогда для всякой формулы $\psi(a) \in \mathscr{L}(\mathrm{PA})$

$$F(\ulcorner \psi(a) \urcorner) = \ulcorner \psi(\underline{\ulcorner \psi(a) \urcorner}) \urcorner.$$

По теореме D3.8 выберем $\Sigma_1$-формулу $\delta(a, b)$, сильно представляющую $F$: ее график правильно определяется в $\mathbb{N}$, и при этом

$$\mathrm{PA} \vdash \forall y \left[\delta(\underline{n}, y) \leftrightarrow y = \underline{F(n)}\right] \quad \text{для каждого } n \in \omega.$$

Отсюда для всех $n, m \in \omega$ имеем:[6]

$$\mathbb{N} \vDash \delta(\underline{n}, \underline{m}) \quad \Longleftrightarrow \quad F(n) = m.$$

Для данной формулы $\Phi(a)$ определим $\xi(a) \stackrel{\text{def}}{\leftrightarrow} \exists y\, [\delta(a, y) \wedge \Phi(y)]$. Положим $\theta \stackrel{\text{def}}{\leftrightarrow} \xi(\underline{\ulcorner \xi(a) \urcorner})$. Тогда в PA

$$\begin{aligned}
\theta &\leftrightarrow \exists y\, [\delta(\underline{\ulcorner \xi(a) \urcorner}, y) \wedge \Phi(y)] \\
&\leftrightarrow \exists y\, [y = \underline{F(\ulcorner \xi(a) \urcorner)} \wedge \Phi(y)] \\
&\leftrightarrow \Phi(\underline{F(\ulcorner \xi(a) \urcorner)}) \\
&\leftrightarrow \Phi(\underline{\ulcorner \xi(\underline{\ulcorner \xi(a) \urcorner}) \urcorner}) \\
&\leftrightarrow \Phi(\underline{\ulcorner \theta \urcorner}).
\end{aligned}$$

□

Закодировав формулы, можно закодировать и доказательства как примитивно рекурсивные конечные объекты: по данному $n$ за конечное число шагов можно определить, является ли $n$ кодом формального доказательства в PA, и если да, то прочитать геделев номер его последней формулы.

Соответственно, существует такая формула $\mathrm{Pr}(u, v) \in \mathscr{L}(\mathrm{PA})$, что $\mathbb{N} \vDash \mathrm{Pr}(\underline{k}, \underline{\ell})$ выполняется тогда и только тогда, когда $\ell$ кодирует доказательство формулы с геделевым номером $k$. Более того, формулу Pr можно выбрать в классе $\Delta_0$ (при любой стандартной арифметизации); следовательно, формула $\exists v\, \mathrm{Pr}(u, v)$ принадлежит классу $\Sigma_1$.

**Теорема D3.11** (Гёделя первая о неполноте)**.**
*Если* PA *непротиворечива, то существует предложение* $G \in \mathscr{L}(\mathrm{PA})$ *такое, что*

$$\mathrm{PA} \nvdash G \quad \textit{и} \quad \mathrm{PA} \nvdash \neg G.$$

*Доказательство.* Пусть $G$ — диагональная неподвижная точка для формулы $\neg \exists x\, \mathrm{Pr}(a, x)$, существующая по теореме D3.10. Тогда

$$\mathrm{PA} \vdash G \leftrightarrow \neg \exists x\, \mathrm{Pr}(\underline{\ulcorner G \urcorner}, x).$$

Если $\mathrm{PA} \vdash G$, то пусть $p$ — код какого-нибудь формального доказательства формулы $G$. Тогда $\mathbb{N} \vDash \mathrm{Pr}(\underline{\ulcorner G \urcorner}, \underline{p})$. По самому смыслу Pr (это формализованная примитивно рекурсивная проверка того, что $p$ есть корректный вывод, последняя строка которого

[6] Здесь $\mathbb{N} \vDash (\ldots)$ — выполнимость в стандартной модели, введенной в главе D2.

имеет код $\ulcorner G \urcorner$) отсюда получаем $\mathrm{PA} \vdash \mathrm{Pr}(\underline{\ulcorner G \urcorner}, \underline{p})$, а значит, $\mathrm{PA} \vdash \exists x\, \mathrm{Pr}(\underline{\ulcorner G \urcorner}, x)$.[7] Вместе с эквиваленцией для $G$ это дает противоречие в PA.

Если же $\mathrm{PA} \vdash \neg G$, то $\mathrm{PA} \vdash \exists x\, \mathrm{Pr}(\underline{\ulcorner G \urcorner}, x)$. Последнее предложение принадлежит классу $\Sigma_1$ и потому истинно в $\mathbb{N}$ по корректности. Значит, существует (стандартное) доказательство формулы $G$, т.е. $\mathrm{PA} \vdash G$. Вместе с $\mathrm{PA} \vdash \neg G$ мы снова получаем противоречие с непротиворечивостью PA.

Итак, ни $G$, ни $\neg G$ не выводимы. □

**Теорема D3.12** (Гёделя вторая о неполноте)**.**
*Пусть* $\mathrm{Con}(\mathrm{PA}) \overset{\text{def}}{\leftrightarrow} \neg\exists x\, \mathrm{Pr}(\underline{\ulcorner 0{=}1 \urcorner}, x)$. *Если* PA *непротиворечива, то* $\mathrm{PA} \nvdash \mathrm{Con}(\mathrm{PA})$.

*Доказательство.* Оставим то же самое предложение $G$. Формализация доказательства теоремы D3.11 внутри PA дает

$$\mathrm{PA} \vdash \mathrm{Con}(\mathrm{PA}) \to \neg\exists x\, \mathrm{Pr}(\underline{\ulcorner G \urcorner}, x).$$

Комбинируя это с диагональной эквиваленцией для $G$, получаем $\mathrm{PA} \vdash \mathrm{Con}(\mathrm{PA}) \to G$. Значит, если $\mathrm{PA} \vdash \mathrm{Con}(\mathrm{PA})$, то $\mathrm{PA} \vdash G$ — в противоречии с теоремой D3.11. □

**Теорема D3.13** (Тарского о невыразимости истины)**.** *Не существует формулы* $T(a)$ *языка* $\mathscr{L}(\mathrm{PA})$ *с единственной свободной переменной* $a$ *такой, что для всякого предложения* $\varphi \in \mathscr{L}(\mathrm{PA})$

$$\mathbb{N} \vDash T(\underline{\ulcorner \varphi \urcorner}) \quad \Longleftrightarrow \quad \mathbb{N} \vDash \varphi.$$

*Доказательство.* Предположим, что такая формула $T(a)$ существует. Применим теорему D3.10 к формуле $\neg T(a)$ и получим предложение $\lambda$ со свойством

$$\mathrm{PA} \vdash \lambda \leftrightarrow \neg T(\underline{\ulcorner \lambda \urcorner}).$$

По корректности

$$\mathbb{N} \vDash \lambda \quad \Longleftrightarrow \quad \mathbb{N} \vDash \neg T(\underline{\ulcorner \lambda \urcorner}).$$

Но определяющее свойство формулы $T$ дает: $\mathbb{N} \vDash T(\underline{\ulcorner \lambda \urcorner})$ тогда и только тогда, когда $\mathbb{N} \vDash \lambda$. Значит, $\mathbb{N} \vDash \lambda$ равносильно $\mathbb{N} \vDash \neg\lambda$, что невозможно. □

Подведем итоги раздела про арифметику. Начав с аксиоматики, мы доказали ряд стандартных алгебраических свойств натуральных чисел и общее утверждение о конгруэнтности равенства. Затем мы разобрались с принципами, равносильными индукции, в частности, принципом вполне упорядоченности (WOP). Далее мы определили несколько полезных арифметических операций и обсудили два эквивалентных подхода к их определению — путем обогащения сигнатуры функциональными символами и прямым определением формулы, описывающей график функции.

Затем мы привели и доказали несколько простых фактов из теории чисел, связанных со свойствами делимости. Все приведенные доказательства были выполнены строго в рамках первопорядковой арифметики без использования квантификации по последовательностям или множествам. Это позволило нам далее доказать основную теорему о дописывании последовательности, которая делает возможным давать рекурсивные

[7] Здесь используется тонкий переход от доказуемости $G$ к доказуемости предиката доказуемости. В модальных логиках для этого вводится специальное правило вывода под названием «правило необходимости» (Necessitation), а в PA можно воспользоваться $\Sigma_1$-полнотой (еще один замечательный факт о формальной арифметике).

определения последовательностей, кодируя их «на лету» парой подходящих чисел (или одним числом, если использовать нумерацию Кантора).

Имея такой инструмент, мы теперь можем говорить о последовательностях, как об объектах теории PA, поскольку можем их кодировать определенным образом. Это выводит первопорядковую арифметику Пеано на новый уровень по своей доказательной силе, т.к. позволяет оперировать произвольными конечными множествами, а значит, и произвольными отношениями и функциями на конечных множествах, что уже гораздо удобнее, чем только лишь оперирование числами и предикатами.

Мощь такого «скачка» проявляется, например, в том, что в PA становится возможным говорить не только о целых и рациональных числах, но также о так называемых вычислимых вещественных числах и функциях. Действительно, умея кодировать последовательности произвольной длины, мы можем одной формулой $\varphi(n, q)$, где $q$ — рациональное, закодировать сходящуюся последовательность рациональных чисел. Вещественные числа, являющиеся пределами таких последовательностей, называются **вычислимыми**. Множество вычислимых чисел содержит в себе все алгебраические числа, а также многие другие, оставаясь при этом счетным множеством.

Умея кодировать вычислимые числа, множество которых плотно в $\mathbb{R}$, мы можем кодировать многие вещественные функции, определяя их вычислимые значения в вычислимых точках. Для вычислимых функций в PA можно доказать ряд обычных свойств, известных из анализа, например, лемму о промежуточном значении, теорему о достижении максимума для непрерывной на отрезке функции, тождество $e^{x+y} = e^x \cdot e^y$ для вычислимых $x, y$, тригонометрическое тождество $\sin^2(x)+\cos^2(x) = 1$ для вычислимых $x$, и т.п.

Все свойства вычислимых чисел и функций выделяют под общим названием «вычислимый анализ», который можно реализовать (путем кодирования последовательностей) в PA. Таким образом, PA, являясь первопорядковой теорией в счетном языке, уже дает нам практически весь аппарат вещественного анализа, по крайней мере тот, который используется в вычислительной математике, компьютерных системах и большинстве приложений.

Тем не менее, некоторые вещи остаются за рамками досягаемости PA. Главный пример — аксиома полноты вещественных чисел. Она недоказуема в PA, потому что требует рассмотрения произвольных, не обязательно вычислимым образом заданных множеств вещественных чисел. Это — территория более сильных теорий, таких как теория множеств ZFC.

## D3.6. Упражнения

**Ex1.** Постройте формальный вывод для $a + S(0) = S(a)$.

**Ex2.** Докажите свойство $\forall x(x \cdot S(0) = x)$ (мультипликативная единица).

**Ex3.** Докажите свойство дискретности: если $a < b$, то $S(a) \leqslant b$, используя сильное определение неравенства ($a < b \overset{\text{def}}{\leftrightarrow} \exists x(b = a + Sx)$) и Лемму D3.1.

**Ex4.** Используя аксиомы арифметики Пеано (конкретно PA5), докажите следующее свойство сложения:

$$S(a) + b = S(a + b).$$

*Подсказка: Используйте индукцию по $b$.*

**Ex5.** Докажите свойства неравенства для усеченного вычитания: $a \dot{-} b \leqslant a$, и $(a \dot{-} b = a) \leftrightarrow (a = 0 \vee b = 0)$.

**Ex6.** Докажите свойство восстановления: $(a = (a \dot{-} b) + b) \leftrightarrow (b \leqslant a)$.

**Ex7.** Докажите свойство обратной операции: $(a + b) \dot{-} a = b$.

**Ex8.** Докажите псевдо-ассоциативное свойство: $a \dot{-} (b + c) = (a \dot{-} b) \dot{-} c$.

**Ex9.** Докажите дистрибутивность умножения относительно усеченного вычитания: $c \cdot (a \dot{-} b) = (c \cdot a) \dot{-} (c \cdot b)$.

**Ex10.** Докажите монотонность по уменьшаемому: $(a \leqslant b) \to (a \dot{-} c \leqslant b \dot{-} c)$.

**Ex11.** Докажите антимонотонность по вычитаемому: $(a \leqslant b) \to (c \dot{-} b \leqslant c \dot{-} a)$.

**Ex12.** Формально определите отношение «Остаток» $R(a, b, r)$ ($r$ является остатком от деления $a$ на $b$).

**Ex13.** Докажите, что если $a \mid b$ и $b \mid a$, то $a = b$.

**Ex14.** Найдите натуральные числа $s, t$, удовлетворяющие тождеству Безу для $a = 12, b = 18$ (примечание: в натуральных числах $gcd(a, b) = (a \cdot s) \dot{-} (b \cdot t)$ или наоборот).

**Ex15.** Вычислите значение $\beta$-функции Гёделя $\beta(c, d, i) = \mathrm{rem}(c, 1 + (i + 1)d)$ для:

1. $\beta(10, 3, 0)$.
2. $\beta(10, 3, 1)$.
3. $\beta(10, 3, 2)$.

**Ex16.** Вычислите значение $\beta$-функции Гёделя $\beta(c, d, i)$ для параметров $c = 13, d = 2$ и индексов $i = 0, 1$. Какую последовательность из двух элементов это кодирует?

**Ex17.** Найдите пару $(c, d)$, которая кодирует последовательность $\langle 1, 2\rangle$ длины 2.

**Ex18.** Докажите, что для любой последовательности $a_0, \ldots, a_n$ существует бесконечно много пар $(c, d)$, кодирующих её.

**Ex19.** Используя определение множества целых чисел $Z = (\omega \times \{0\}) \cup (\{0\} \times \omega)$ из Раздела C1.4.3, выпишите пары, представляющие числа 5 и $-3$.

**Ex20.** Вычислите сумму $\langle 0, 5\rangle +_{\mathbb{Z}} \langle 3, 0\rangle$ (соответствующую $5 + (-3)$), используя определение сложения для этой модели.

**Ex21.** Вычислите сумму $\langle 0, 2\rangle +_{\mathbb{Z}} \langle 5, 0\rangle$ (соответствующую $2 + (-5)$), используя определение сложения.

**Ex22.** Вычислите произведение двух отрицательных чисел $\langle 2, 0\rangle \cdot_{\mathbb{Z}} \langle 3, 0\rangle$, используя определение умножения.

**Ex23.** Вычислите произведение $\langle 0, 3\rangle \cdot_{\mathbb{Z}} \langle 2, 0\rangle$ (соответствующее $3 \cdot (-2)$) и проверьте, что результат верен.

**Ex24.** Пусть $\varphi(a)$ — формула PA с одной свободной переменной. Найдите неподвижную точку $\theta$ (такую, что PA $\vdash \theta \leftrightarrow \varphi(\underline{\ulcorner \theta \urcorner})$) в каждом из следующих случаев, при любой корректной геделевской нумерации:

1. $\varphi(a)$ тождественно ложна (например, $a \neq a$);
2. $\varphi(a)$ тождественно истинна (например, $a = a$).

**Ex25.** В этом и следующем упражнении предполагается упрощенная конкатенационная геделевская нумерация: формула кодируется напрямую, заменой символов на конкретные цифры в десятичной записи. Пусть $\varphi(a)$ выражает тот факт, что число $a$ оканчивается цифрой 6.

1. Запишите формулу языка PA, выражающую это свойство $\varphi(a)$.
2. Пусть нумерация устроена так, что закрывающая скобка «)» имеет код 6. Найдите *ложную* неподвижную точку для формулы $\varphi(a)$.
3. При тех же условиях найдите *истинную* неподвижную точку для формулы $\varphi(a)$.

**Ex26.** Предположим конкатенационное кодирование, при котором конкретные символы имеют следующие цифровые коды: $\ulcorner 0 \urcorner \rightleftharpoons^{\text{def}} 1$, $\ulcorner S \urcorner \rightleftharpoons^{\text{def}} 2$, $\ulcorner + \urcorner \rightleftharpoons^{\text{def}} 3$, $\ulcorner = \urcorner \rightleftharpoons^{\text{def}} 4$ (коды остальных символов для этой задачи не важны).

1. Запишите формулу $\varphi(a)$ в PA, выражающую «$a$ не делится на 3».
2. Найдите неподвижную точку для формулы $\varphi(a)$. (*Подсказка:* переберите простейшие атомарные формулы вроде $0 = 0$ или $0 + 0 = 0$, вычислите их десятичный код и проверьте, делится ли он на 3.)

## Рекомендуемая литература

Арифметика — это не только первая серьезная математическая теория, с которой мы знакомимся, но и арена, на которой были разыграны величайшие драмы оснований математики XX века. Литература по этой теме огромна, но можно выделить несколько ключевых направлений, напрямую связанных с материалом этой главы.

Центральным сюжетом, безусловно, являются теоремы Гёделя о неполноте. Несмотря на то, что их доказательство можно найти почти в любом учебнике по логике, ни одно изложение не сравнится по глубине и полноте с соответствующими главами «Введения в метаматематику» Клини [28], уже упомянутого нами ранее. Именно там с предельной дотошностью вводятся понятия рекурсивных функций и проводится вся процедура геделевской нумерации, синтаксические основы которой были заложены в этой главе через кодирование последовательностей. Альтернативное, более современное изложение, тесно увязывающее логику и теорию алгоритмов, можно найти в замечательных лекциях Н. К. Верещагина и А. Шеня [42, 43]. В качестве же исключительно ясного и педагогичного руководства, посвященного именно этим теоремам, настоятельно рекомендуем книгу Питера Смита «An Introduction to Gödel's Theorems» [62].

После осознания факта неполноты возникает естественный вопрос: а какие именно содержательные утверждения арифметика не в силах доказать? Ответ на этот вопрос открыл целое направление исследований. Статья Кёрби и Пэрис [54] стала знаковой, предъявив первое «естественное» комбинаторное утверждение (вариацию теоремы Рамсея), независимое от аксиом Пеано. Для тех, кто желает профессионально разобраться в зоопарке моделей арифметики и тонкостях независимости, настольной книгой должен стать специализированный труд Ричарда Кея «Модели арифметики Пеано» [53]. В нем детально исследуются нестандартные модели, существование которых является следствием теорем компактности и Лёвенгейма–Скулема, и которые дают семантическое объяснение феномену неполноты.

# ГЛАВА D4

# Теория множеств

*Сущность математики — в ее свободе.*

— Георг Кантор

Напомним, что первопорядковая теория множеств ZF задается в языке логики предикатов первого порядка с сигнатурой (помимо логических связок и кванторов) $\Sigma_{\mathrm{ZF}} \overset{\text{def}}{=\!=} \langle =, \in \rangle$. В качестве переменных используются латинские буквы (возможно, с индексами и/или акцентами), а также могут использоваться греческие буквы в ограниченных по классам кванторах.

Приведем здесь еще раз полный список аксиом ZF, сформулированных в исходном языке, т.е. без применения сокращений:

ZF1 Конгруэнтность: $(a = b) \to ((a \in M) \leftrightarrow (b \in M))$.

ZF2 Экстенсиональность: $(A = B) \leftrightarrow (\forall x\ (x \in A) \leftrightarrow (x \in B))$.

ZF3 Степень: $\exists P\ \forall x\ (x \in P) \leftrightarrow \forall y (y \in x \to y \in A)$.

ZF4 Объединение: $\exists U\ \forall x\ (x \in U) \leftrightarrow (\exists a \in A :\ x \in a)$.

ZF5 Регулярность: $(\exists x \in A) \to \exists X \in A :\ \forall y \in X :\ (y \notin A)$.

ZF6 Подстановка $[\varphi]$: $(\forall x \in A : \exists! y : \varphi(x, y, \vec{p})) \to (\exists Y\ \forall y\ ((y \in Y) \leftrightarrow \exists x \in A : \varphi(x, y, \vec{p})))$.

ZF7 Бесконечность:

$$\exists X\ (\exists z \in X : \forall y (y \notin z)) \wedge (\forall x \in X : \exists y \in X :\ \forall z (z \in y \leftrightarrow z \in x \vee z = x)),$$

а также аксиомы и правила вывода логики предикатов:

PC1 универсальные замыкания всех подстановок всех формул языка ZF во все тавтологии логики высказываний;

PC2 аксиомы для кванторов:

$$(\forall)\quad (\forall x\ \varphi[a/x]) \to \varphi[a/T]; \qquad (\exists)\quad \varphi[a/T] \to \exists x\ \varphi[a/x],$$

где $\varphi$ не содержит связанную переменную $x$, $T$ — любой терм теории;

PC3 правила вывода:

$$(MP)\quad \frac{\varphi,\quad \varphi \to \psi}{\psi}; \qquad (R1)\quad \frac{\varphi \to \psi}{\varphi \to \forall x\ \psi[a/x]};$$

$$(R1')\quad \frac{\psi}{\forall x\ \psi[a/x]}; \qquad (R2)\quad \frac{\psi \to \varphi}{(\exists x\ \psi[a/x]) \to \varphi},$$

где для правил (R1), (R1'), (R2) переменная $a$ не входит в $\varphi$ и ни в одну из активных (непогашенных) гипотез, от которых зависит вывод формулы в посылке этих правил.

# D4.1. Основные свойства

Первое, что нужно сделать, пока наш язык максимально беден, — это доказать конгруэнтность равенства относительно термов и формул, т.е. вывести законы подстановки (B1.9).

Во-первых, требуется получить стандартные свойства равенства: рефлексивность, симметричность и транзитивность. Эти свойства прямо следуют из аксиомы экстенсиональности, например,

$$(A = B) \leftrightarrow [\forall x(x \in A) \leftrightarrow (x \in B)] \leftrightarrow [\forall x(x \in B) \leftrightarrow (x \in A)] \leftrightarrow (B = A),$$

что верно по свойствам симметричности эквиваленции.

Во-вторых, заметим, что в чистом языке теории множеств термы — это в точности переменные (ввиду отсутствия констант и функциональных символов). Поэтому проверка конгруэнтности равенства относительно термов тривиальна:

$$(T_1 = T_2) \to (T_1 = T_2), \text{ либо } (T_1 = T_2) \to (b = b)$$

для любых термов $T_1$ и $T_2$, т.к. подстановка терма $T$ в терм $a$ вместо $a$ дает терм $T$, а подстановка терма $T$ в терм $b$ вместо $a$ ничего не меняет.

В-третьих, доказательство конгруэнтности для формул проводим индукцией по высоте формулы, которая определяется рекурсивно (в мета-теории, например, в арифметике PA, в которой при помощи кодирования последовательностей закодирован язык ZFC):

$$H[a = b] = 0; \quad H[a \in b] = 0; \quad H[\neg\varphi] = 1 + H[\varphi];$$
$$H[\varphi \wedge \psi] = 1 + \max(H[\varphi], H[\psi]); \quad H[\exists x\ \varphi[a/x]] = 1 + H[\varphi],$$

где мы также считаем язык логики максимально бедным, предполагая, что $\vee, \to, \leftrightarrow, \forall$ выражаются через базовые связки $\neg, \wedge$ и квантор $\exists$.

Далее схема доказательства полностью соответствует схеме доказательства конгруэнтности в PA, которая была разобрана в теореме D3.2.

Пусть высота формулы равна нулю, т.е. это атомарная формула. Атомарных формул у нас всего две:

1. $(a = b)$: здесь нам нужно проверить, что

   $$(T_1 = T_2) \to ((T_1 = b) \leftrightarrow (T_2 = b)),$$

   что верно в силу свойств равенства;

2. $(a \in b)$: здесь нужно проверить две формулы:

   $$(T_1 = T_2) \to ((T_1 \in b) \leftrightarrow (T_2 \in b)), \quad (T_1 = T_2) \to ((a \in T_1) \leftrightarrow (a \in T_2)),$$

   которые получаются соответствующими подстановками в аксиомы конгруэнтности и экстенсиональности.[1]

[1] Здесь стоит отметить, что аксиому экстенсиональности нужно разделить на две части, представив как конъюнкцию двух импликаций, и первая импликация $(A = B) \to (\forall x\ (x \in A) \leftrightarrow (x \in B))$ будет как раз недостающей аксиомой конгруэнтности, сохраняющей подстановку равных во второй аргумент предиката принадлежности.

Таким образом для атомарных формул конгруэнтность следует непосредственно из аксиом. Введем индуктивную гипотезу о том, что для формул высоты не больше $n$ конгруэнтность выполняется. Пусть формула $\varphi$ имеет высоту не больше, чем $n$. Тогда по предположению индукции

$$(T_1 = T_2) \to (\varphi[a/T_1] \leftrightarrow \varphi[a/T_2]),$$

а консеквент данной импликации эквивалентен $\neg\varphi[a/T_1] \leftrightarrow \neg\varphi[a/T_2]$ в силу исчисления предикатов, откуда следует конгруэнтность для $\neg\varphi$. Аналогично рассматривается случай конъюнкции. Случай квантора существования следует из леммы D2.8. На этом индукция завершена.

Итак, в простейшем языке конгруэнтность получена.

Теперь мы обогатим язык стандартными символами операций, отношений и констант, которые были определены и подробно рассмотрены в разделе C1.1. При расширении языка необходимо доказывать расширение конгруэнтности равенства на эти новые символы.

Пусть, например, у нас есть определение для пересечения множеств

$$\forall x\ (x \in A \cap B) \overset{\text{def}}{\leftrightarrow} (x \in A \wedge x \in B). \tag{D4.1}$$

Необходимо тогда, чтобы выполнялись свойства:

$$(T_1 = T_2) \to (T_1 \in A \cap B \leftrightarrow T_2 \in A \cap B), \quad (T_1 = T_2) \to (A \cap B \in T_1 \leftrightarrow A \cap B \in T_2),$$
$$(T_1 = T_2) \to (a \in T_1 \cap B \leftrightarrow a \in T_2 \cap B), \quad (T_1 = T_2) \to (a \in A \cap T_1 \leftrightarrow a \in A \cap T_2).$$

Первая формула получается подстановкой $T_1$ и $T_2$ вместо $x$ в определение (D4.1) по свойствам равенства. Вторая формула следует из теоремы B2.6, а третья и четвертая получаются на индуктивном шаге, когда мы доказываем конгруэнтность равенства относительно термов индукцией по их сложности (поскольку терм $T_1 \cap B$ сложнее, чем терм $T_1$).

Действуя так для всех новых введенных функциональных и предикатных символов, мы можем показать конгруэнтность равенства относительно всех формул расширенного языка.

Но, как уже отмечалось при рассмотрении арифметики, мы всегда можем считать формулы вроде (D4.1) синтаксическим сахаром или мета-теоретическим сокращением для более длинных формул исходного языка, и в таком случае проверка конгруэнтности автоматически сводится к уже доказанной конгруэнтности в первоначальном языке.[2]

**Теорема D4.1** (базовые свойства операций)**.** *Пусть $A, B, C \in \mathscr{P}(U)$, где $U$ — произвольное непустое множество, тогда справедливые следующие свойства.*

1° *Коммутативность: $A \cup B = B \cup A$ и $A \cap B = B \cap A$.*

2° *Ассоциативность: $(A \cup B) \cup C = A \cup (B \cup C)$ и $(A \cap B) \cap C = A \cap (B \cap C)$.*

3° *Дистрибутивность: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ и $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.*

[2] Кроме того, как мы уже говорили, часто вообще конгруэнтность по всем термам и формулам предполагается заданной аксиоматически, и проверки не требует. Но поскольку мы здесь включили элементарную аксиому конгруэнтности, а также для воспитания в себе более глубокой уверенности во внутренней согласованности нашего формализма, хотя бы краткое доказательство ее экстраполяции на весь язык оказывается чрезвычайно полезным шагом.

4° *Нейтральные элементы:* $A \cup \varnothing = A$ *и* $A \cap U = A$.

5° *Закон исключенного третьего:* $A \cup (U \setminus A) = U$.

6° *Закон противоречия:* $A \cap (U \setminus A) = \varnothing$.

7° *Идемпотентность:* $A \cup A = A$ *и* $A \cap A = A$.

8° *Законы поглощения:* $A \cup (A \cap B) = A$ *и* $A \cap (A \cup B) = A$.

9° *Законы де Моргана:* $U \setminus (A \cup B) = (U \setminus A) \cap (U \setminus B)$ *и* $U \setminus (A \cap B) = (U \setminus A) \cup (U \setminus B)$.

10° *Разность множеств:* $A \setminus B = A \cap (U \setminus B)$.

11° *Симметрическая разность:* $A \triangle B = (A \setminus B) \cup (B \setminus A) = (A \cap (U \setminus B)) \cup (B \cap (U \setminus A))$.

12° $\langle \mathscr{P}(U), \triangle \rangle$ *— абелева группа, т.е.*

- 12.1° *ассоциативность:* $(A \triangle B) \triangle C = A \triangle (B \triangle C)$;
- 12.2° *коммутативность:* $A \triangle B = B \triangle A$;
- 12.3° *нейтральный элемент:* $A \triangle \varnothing = A$;
- 12.4° *обратный элемент:* $A \triangle A = \varnothing$;

13° *Дистрибутивность:* $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.

Все эти свойства на самом деле есть прямые следствия логических операций, и эту связь мы подробно обсуждали в разделе A2.4.

Чтобы без проблем пользоваться дополнением множества $\setminus A$ до универсума, которое соответствует логическому отрицанию, мы рассмотрели все операции на универсуме $U$, т.к. в этом случае результат операции всегда является множеством, причем содержащимся в том же $U$. В принципе, мы могли бы в качестве $U$ взять класс всех множеств, определяемый формулой $x = x$, и все эти свойства остались бы верными, учитывая, что символ класса здесь стоит только справа в отношении $\in$. Но таковые допущения нам не требуются, поскольку в каждом конкретном случае можно найти достаточно большое множество $U$, внутри которого все происходит. Поэтому для краткости записей мы вообще можем забыть о множестве $U$ и вместо $U \setminus A$ писать $\setminus A$, называя это множество дополнением к $A$. Кроме того, пересечение множеств удобно записывать как умножение, т.е. вообще опуская операцию $\cap$. Учитывая эти сокращения, запись $A \setminus B$ можно понимать как $A \cap (U \setminus B)$, и это равенство, как легко видеть, действительно верно при условии, что $A, B \in \mathscr{P}(U)$.

Посмотрим доказательство свойств приведенной теоремы на примере доказательства ассоциативности операции симметрической разности:

$$[x \in (A \triangle B) \triangle C] \leftrightarrow [x \in (A \triangle B) \setminus C] \vee [x \in C \setminus (A \triangle B)] \leftrightarrow$$
$$[((x \in A \setminus B) \vee (x \in B \setminus A)) \wedge (x \notin C)] \vee [(x \in C) \wedge \neg((x \in A \setminus B) \vee (x \in B \setminus A))] \leftrightarrow$$
$$[(\mathscr{A}\,\neg\mathscr{B} \vee \mathscr{B}\,\neg\mathscr{A})\,\neg\mathscr{C}] \vee [\mathscr{C}\,\neg(\mathscr{A}\,\neg\mathscr{B} \vee \mathscr{B}\,\neg\mathscr{A})] \equiv$$
$$[(\mathscr{A}\,\neg\mathscr{B} \vee \mathscr{B}\,\neg\mathscr{A})\,\neg\mathscr{C}] \vee [\mathscr{C}\,(\neg\mathscr{A} \vee \mathscr{B})(\neg\mathscr{B} \vee \mathscr{A})] \equiv$$
$$\mathscr{A}\,\neg\mathscr{B}\neg\mathscr{C} \vee \neg\mathscr{A}\,\mathscr{B}\neg\mathscr{C} \vee \neg\mathscr{A}\,\neg\mathscr{B}\mathscr{C} \vee \mathscr{A}\,\mathscr{B}\mathscr{C},$$

где мы воспользовались обозначениями $(x \in A) \overset{\text{def}}{\rightleftharpoons} \mathscr{A}$, $(x \in B) \overset{\text{def}}{\rightleftharpoons} \mathscr{B}$, $(x \in C) \overset{\text{def}}{\rightleftharpoons} \mathscr{C}$, и перешли к вычислениям в логике высказываний, а также записывали конъюнкцию как умножение.

С другой стороны,

$$[x \in A \triangle (B \triangle C)] \leftrightarrow [x \in A \setminus (B \triangle C)] \vee [x \in (B \triangle C) \setminus A] \leftrightarrow$$
$$[\mathscr{A} \neg(\mathscr{B} \neg \mathscr{C} \vee \mathscr{C} \neg \mathscr{B})] \vee [\neg \mathscr{A} (\mathscr{B} \neg \mathscr{C} \vee \mathscr{C} \neg \mathscr{B})] \equiv$$
$$[\mathscr{A} (\neg \mathscr{B} \vee \mathscr{C})(\mathscr{B} \vee \neg \mathscr{C})] \vee [\neg \mathscr{A} \mathscr{B} \neg \mathscr{C} \vee \neg \mathscr{A} \neg \mathscr{B} \mathscr{C}] \equiv$$
$$\mathscr{A} \neg \mathscr{B} \neg \mathscr{C} \vee \mathscr{A} \mathscr{B} \mathscr{C} \vee \neg \mathscr{A} \mathscr{B} \neg \mathscr{C} \vee \neg \mathscr{A} \neg \mathscr{B} \mathscr{C}.$$

Как видим, в обоих случаях получена одна и та же формула с точностью до коммутативности дизъюнкции. Тем самым свойство 12.1 доказано.

При таких переобозначениях большинство из перечисленных свойств являются точными копиями тавтологий, которые были перечислены в разделе D2.1. И на самом деле большинство сложных тождеств с множествами гораздо легче вычислять в чистой логике высказываний.

Здесь мы должны ввести необходимые определения из общей алгебры. Пусть задана структура $\langle M; 0, 1, \neg, \vee, \wedge \rangle$, в которой операции и константы связаны следующими аксиомами:

BA1 ассоциативность $\vee, \wedge$;

BA2 коммутативность $\vee, \wedge$;

BA3 взаимная дистрибутивность $\vee, \wedge$;

BA4 идемпотентность $\vee, \wedge$;

BA5 законы поглощения для $\vee, \wedge$;

BA6 правила для констант: $a \wedge 0 = 0$, $a \wedge 1 = a$, $a \vee 0 = a$, $a \vee 1 = 1$;

BA7 $a \vee \neg a = 1$, $a \wedge \neg a = 0$.

Такая структура называется **булевой алгеброй**.

Как видим, булеан $M = \mathscr{P}(U)$ удовлетворяет этому определению, если константа 0 — это пустое множество, 1 — множество $M$, $\neg$ — дополнение, $\wedge$ — пересечение, $\vee$ — объединение. В связи с этим с этим существует термин *алгебра множеств*, под которым понимается булева алгебра, построенная указанным способом на булеане некоторого непустого множества.

На булевой алгебре также обычно вводится предикат неравенства, определяемый по правилу

$$a \leqslant b \overset{\text{def}}{\leftrightarrow} a \wedge b = a, \tag{D4.2}$$

который в алгебре множеств соответствует предикату $A \subseteq B$.

Булева алгебра обобщается более широким понятием — *ограниченная решетка*. Скажем, что структура $\langle M; \leqslant \rangle$ называется **решеткой**, если

L1 отношение $\leqslant$ является нестрогим частичным порядком;

L2 для любых $a, b \in U$ существует $\sup\{a, b\}$ и $\inf\{a, b\}$,

где $\sup\{a, b\} = \min\{x \mid a \leqslant x \wedge b \leqslant x\}$, $\inf\{a, b\} = \max\{x \mid x \leqslant a \wedge x \leqslant b\}$. Решетка называется *ограниченной*, если в ней существуют элементы, обозначаемые $\top, \bot$ (или $1, 0$) такие, что $\top = \max M$, $\bot = \min M$.

Несложно показать, что если на булевой алгебре вводится отношение порядка по правилу (D4.2), то оно является частичным порядком и

$$a \wedge b = \inf\{a, b\}, \quad a \vee b = \sup\{a, b\}, \tag{D4.3}$$

а кроме того, $1 = \max M$, $0 = \min M$ относительно данного порядка, так что всякая булева алгебра является ограниченной решеткой.

Более того, имея произвольную решетку, мы можем задать операции $\vee, \wedge$ по правилу (D4.3), и окажется, что они обладают свойствами BA1, BA2, BA4, BA5. Если же для этих операций работают законы дистрибутивности, то такая решетка называется *дистрибутивной*. Если дистрибутивная решетка является ограниченной решеткой, то ее константы удовлетворяют свойству BA6. Иначе говоря, ограниченная дистрибутивная решетка — это почти булева алгебра.

Чтобы ограниченная дистрибутивная решетка стала булевой алгеброй, нужно определить операцию отрицания и добавить для нее условия BA7. Отрицание чаще всего вводят через еще одну операцию, которая обозначается $\to$ (как импликация) и должна удовлетворять правилу

$$a \leqslant (b \to c) \overset{\text{def}}{\leftrightarrow} (a \wedge b) \leqslant c. \tag{D4.4}$$

Операция $\to$ называется *относительным псевдодополнением* или *импликацией*, а ограниченная решетка с такой операцией называется *гейтинговой алгеброй*. Заметим, что если мы воспринимаем операцию $\to$ как логическую импликацию, а отношение $\leqslant$ — как логическую выводимость, то условие (D4.4) можно прочитать как теорему о дедукции: $\mathscr{A} \vdash (\mathscr{B} \to \mathscr{C}) \Leftrightarrow (\mathscr{A} \wedge \mathscr{B}) \vdash \mathscr{C}$. При такой интерпретации можно сказать, что гейтинговы алгебры — это ограниченные решетки с «теоремой о дедукции».

Интересно отметить, что гейтингова алгебра обязательно дистрибутивна. Причем этот факт можно доказать «в лоб», а можно воспользоваться фактом, что гейтинговы алгебры — это в точности модели интуиционистской логики высказываний,[3] откуда дистрибутивность следует ввиду наличия таковой в логике высказываний.

Если относительное псевдодополнение существует для данной ограниченной решетки, то в ней несложно определить унарную операцию *абсолютного псевдодополнения* (отрицания), полагая $\neg a \overset{\text{def}}{=\!=} a \to 0$, или, если забыть про $\to$, то отрицание вводится аксиомой $(a \leqslant \neg b) \overset{\text{def}}{\leftrightarrow} (a \wedge b = 0)$. Абсолютное псевдодополнение автоматически удовлетворяет закону противоречия[4] $a \wedge \neg a = 0$, но не обязано удовлетворять закону исключенного третьего $a \vee \neg a = 1$ (который равносилен тождеству $\neg\neg a = a$).

Наконец, если в гейтинговой алгебре работает закон исключенного третьего, то есть полностью выполняется условие BA7, то такая алгебра является булевой алгеброй.

Отметим основное свойство булевой алгебры, называемое **принципом двойственности**: если в каком-либо истинном тождестве, записанном в сигнатуре булевой алгебры, заменить 0 на 1 и наоборот, а также $\wedge$ на $\vee$ и наоборот, то полученное тождество тоже будет истинным. Это свойство прямо следует из аксиом булевой алгебры, которые инвариантны относительно такой замены. Поэтому пары символов 0 и 1, $\wedge$ и $\vee$ называются двойственными. Отрицание $\neg$ при этом называется самодвойственной операцией.

[3] В интуиционистской логике высказываний список аксиом состоит из аксиом A1–A8 (т.е. без закона исключенного третьего), приведенных в разделе D2.1, а правила вывода ровно те же самые: подстановка и Modus Ponens.

[4] Действительно, из определения $\neg$ и коммутативности $\wedge$ следует, что $(a \leqslant \neg b) \leftrightarrow (b \leqslant \neg a)$, откуда, подставляя $\neg a$ вместо $b$, получаем $(a \leqslant \neg\neg a) \leftrightarrow (\neg a \leqslant \neg a)$, т.е. в силу рефлексивности неравенства всегда имеем $a \leqslant \neg\neg a$, а это равносильно $a \wedge \neg a = 0$ по определению $\neg$.

Отметим также, что если на булевой алгебре вводится отношение $\leqslant$ по формуле D4.2, то двойственным ему отношением будет обратное отношение, т.е. $\geqslant$.

Несмотря на свое название, булева алгебра не является алгеброй в смысле определения алгебры над кольцом. Действительно, именно в силу свойства двойственности операций булева алгебра не может быть кольцом, т.к. в кольце операции сложения и умножения не являются двойственными друг другу.

Тем не менее, существует способ найти в булевой алгебре такие операции, которые уже будут удовлетворять аксиомам кольца. А именно, определим операции сложения и умножения по формулам

$$a + b \stackrel{\text{def}}{=\!=} (a \wedge \neg b) \vee (\neg a \wedge b); \quad a \cdot b \stackrel{\text{def}}{=\!=} a \wedge b, \tag{D4.5}$$

т.е. сложение определяется в точности так, как задается симметрическая разность в алгебре множеств.

Тогда структура $\langle M, 0, 1, +, \cdot\rangle$ (с теми же константами) будет кольцом. Более того, это будет коммутативное кольцо с единицей, в котором умножение идемпотентно, т.е. $a \cdot a = a$ для всех элементов кольца.

Кольца с единицей, в которых умножение идемпотентно, называются **булевыми кольцами**. Идемпотентность умножения обеспечивает кольцу сразу два замечательных свойства, а именно: **а)** характеристику 2, т.е. $a + a = 0$ для всех $a \in M$; **б)** коммутативность умножения, т.е. $ab = ba$ для всех $a, b \in M$.

Действительно, $a + a = (a + a)(a + a) = a \cdot a + a \cdot a + a \cdot a + a \cdot a = (a + a) + (a + a)$, откуда следует $a + a = 0$, или $a = -a$ (каждый элемент сам себе противоположен по сложению). Далее, $a + b = (a + b)(a + b) = a \cdot a + a \cdot b + b \cdot a + b \cdot b = (a + b) + (ab + ba)$, откуда $ab + ba = 0$, а так как $ba = -(ba)$, то $ab = ba$.

Множество $\mathscr{P}(U)$ с операциями $\triangle, \cap$ естественным образом является примером булева кольца в силу теоремы D4.1.

Булево кольцо и булева алгебра связаны двусторонним образом (можно сказать, что они «двойственны» друг другу) в том смысле, что как из булевой алгебры без каких-либо дополнительных условий получается булево кольцо, так и из булева кольца без дополнительных условий получается булева алгебра. Действительно, пусть задано булево кольцо $\langle M, 0, 1, +, \cdot\rangle$, тогда операции $\wedge, \neg, \vee$ булевой алгебры задаются так:

$$a \wedge b \stackrel{\text{def}}{=\!=} a \cdot b, \quad \neg a \stackrel{\text{def}}{=\!=} 1 + a, \quad a \vee b \stackrel{\text{def}}{=\!=} a + b + a \cdot b.$$

Вот как, например, проверяется закон исключенного третьего для этих операций: $a \vee \neg a = a + \neg a + a \cdot \neg a = a + (1 + a) + a \cdot (1 + a) = 1$, так как $a \cdot (1 + a) = a + a \cdot a = a + a = 0$.

## D4.2. Конечные и бесконечные множества

От изучения алгебры множеств, т.е. теоретико-множественных операций, переходим теперь непосредственно к изучению свойств множеств.

В разделе C1.1 мы подробно рассмотрели, как аксиома бесконечности вводит в теорию множеств индуктивные множества и, в частности, наименьшее индуктивное множество, которое обозначается $\omega$. Мы также многократно использовали понятие *мощность множества*, не давая ему конкретного определения. В этом разделе нам предстоит детально разобраться с этим и смежными понятиями и навести порядок в использованной ранее терминологии.

### D4.2.1 Сравнение мощностей

Во-первых, напомним, что два множества $A$ и $B$ называются **равномощными** (обозначение: $A \simeq B$), если между ними существует биекция. Для каждого множества $A$ существует собственно класс множеств, равномощных ему, который мы обозначаем за $\mathrm{Card}(A)$ и называем *кардинальностью* множества $A$. Трудность этого определения состоит в том, что мы вводим в употребление целый класс множеств, не являющийся объектом теории ZF. Соответственно, кардинальностей можно описать ровно столько, сколько мы можем написать для них формул. Кроме того, сравнивать и оперировать собственно классами в теории без классов становится совсем неудобно, когда мы хотим рассматривать арифметику и топологию мощностей, т.е. изучать их алгебраическими методами.

Поэтому под мощностью множества мы будем понимать специально выбранные для этого эталонные множества, существование которых, вообще говоря, базируется на аксиоме выбора, но для некоторого класса множеств мы сможем обойтись и без нее, используя множество $\omega$.

Во-вторых, дадим следующие определения. Множество называется **конечным**, если оно равномощно некоторому натуральному числу $n \in \omega$. Например, множество из трех элементов равномощно натуральному числу $3 = \{0, 1, 2\}$. Если $A \simeq n$, то мы пишем $|A| = n$, а число $n$ называем **мощностью** множества $X$. **Бесконечные** множества — все остальные.

Среди бесконечных множеств особое место занимают счетные, поскольку для них есть стандартное мерило — множество $\omega$. Говорят, что множество $A$ **счетно**, если $A \simeq \omega$. При этом $\omega$ называется мощностью $A$, что записывается как $|A| = \omega$. Это определение является естественным продолжением определения конечного множества.

Конечные и счетные множества вместе называются *не более чем счетными*, а все остальные — *несчетными*.[5]

Как много существует несчетных множеств, различных в смысле мощности? Отчасти ответить на этот вопрос помогает одна из фундаментальных теорем теории множеств.

**Теорема D4.2** (Кантора)**.** *Никакое множество не равномощно своему булеану:*

$$A \not\simeq \mathscr{P}(A).$$

*Доказательство.* Предположим, что $A \simeq \mathscr{P}(A)$, т.е. существует биекция $f : A \leftrightarrow \mathscr{P}(A)$. Теперь, поскольку $f(a)$ — это подмножество $A$, мы вправе ожидать, что для некоторых $a$ может случиться попадание $a \in f(a)$, а для других — нет. Пользуясь аксиомой выделения, мы можем определить множество

$$X = \{a \in A \mid a \notin f(a)\}.$$

Так как $X \in \mathscr{P}(A)$, а функция $f$ — сюръекция, то существует такое $x \in A$, что $f(x) = X$. Вопрос: как соотносятся $x$ и $X$? Может ли быть, что $x \in X$, поскольку $x \in A$ и $X \subseteq A$?

Допустим, что $x \in X$, тогда $x$ удовлетворяет формуле, определяющей $X$, т.е. $x \notin f(x)$. Но $f(x) = X$. Получаем, что $x \notin X$. С другой стороны, если $x \notin X$, то $x$ удовлетворяет отрицанию формулы, определяющей $X$, т.е. $x \in f(x)$, т.е. $x \in X$.

[5] Иногда в учебниках можно встретить использование термина «счетное» как для счетных, так и для конечных множеств.

Мы получили ситуацию, аналогичную парадоксу Рассела: $(x \in X) \leftrightarrow (x \notin X)$, т.е. вывели противоречие. К счастью, а данном случае у нас есть посылка, которую мы тем самым опровергли, а именно предположение $A \simeq \mathscr{P}(A)$.

Таким образом, $A \not\simeq \mathscr{P}(A)$. □

Заметим, что хотя множества $A$ и $\mathscr{P}(A)$ неравномощны, мы можем судить о соотношении их мощностей. Скажем, что множество $A$ *не мощнее*, чем $B$ (обозначение: $A \preccurlyeq B$), если в $B$ есть подмножество, равномощное $A$, т.е. если существует инъекция из $A$ в $B$. Отметим, что отношение $\preccurlyeq$ является предпорядком на классе всех множеств (оно рефлексивно и транзитивно). Можно также говорить, что множество $A$ менее мощное, чем $B$, если $(A \preccurlyeq B) \wedge (A \not\simeq B)$ (обозначение: $A \prec B$), переходя к строгому предпорядку.

В случае $A$ и $\mathscr{P}(A)$ очевидно неравенство $A \preccurlyeq \mathscr{P}(A)$, поскольку существует естественная инъекция (вложение) $f : A \to \mathscr{P}(A)$, определяемая по правилу $f(a) = \{a\}$ (как раз тот случай, когда $a \in f(a)$ для всех $a$). А учитывая теорему Кантора, заметим, что всякое множество $A$ менее мощное, чем $\mathscr{P}(A)$, т.е. $A \prec \mathscr{P}(A)$.

На самом деле отношение $\preccurlyeq$ согласовано с $\simeq$ так, что если бы мы могли рассматривать отношение $\preccurlyeq$ на кардинальностях (а не на множествах), то оно оказалось бы частичным порядком (рефлексивным, транзитивным и антисимметричным).

**Теорема D4.3** (Кантора-Бернштейна-Шрёдера)**.** *Если $A \preccurlyeq B$ и $B \preccurlyeq A$, то $A \simeq B$.*

*Доказательство.* По условию существуют инъекции $f : A \to B$ и $g : B \to A$, а нам необходимо предъявить биекцию $h : A \leftrightarrow B$. Определим следующую функцию на булеане $\mathscr{P}(A)$:

$$H(X) = A \setminus g[B \setminus f[X]], \quad X \in \mathscr{P}(A),$$

где квадратные скобки указывают на взятие *образа* множества относительно функции.

Предположим, что уравнение $H(X) = X$ разрешимо, т.е. такое множество $X$ существует. Тогда $f$ и $g^{-1}$ действуют на $X$ и $A \setminus X$ «параллельно», переводя их, соответственно, в $f[X]$ и $B \setminus f[X]$, т.е. функция

$$h(a) = \begin{cases} f(a), & a \in X, \\ g^{-1}(a), & a \in A \setminus X, \end{cases}$$

является искомой биекцией.

Как найти такое $X$? Для начала отметим свойство монотонности функции $H$: если $X \subseteq Y$, то $H(X) \subseteq H(Y)$, которое легко следует из определения $H$. Таким образом $H$ является монотонной функцией на решетке множеств $\mathscr{P}(A)$.

Далее, булеан является *полной решеткой*, т.е. такой решеткой, в которой всякое непустое подмножество имеет sup и inf ($\sup X = \bigcup X$, $\inf X = \bigcap X$). По теореме Кнастера-Тарского, если на полной решетке задана монотонная функция, то для этой функции множество неподвижных точек не пусто и, более того, существуют наименьшая и наибольшая неподвижные точки. Так что для нашего случая наличие корня уравнения $H(X) = X$ есть прямое следствие данной теоремы. □

**Лемма D4.1** (теорема Кнастера-Тарского)**.** *Пусть $\langle L, \leqslant \rangle$ — полная решетка и функция $f : L \to L$ монотонна, т.е. $f(x) \leqslant f(y)$ при $x \leqslant y$ для всех $x, y \in L$. Тогда множество неподвижных точек ($f(x) = x$) функции $f$ не пусто и его точные грани являются неподвижными точками.*

*Доказательство.* Рассмотрим подмножество $S = \{x \in L \mid x \leqslant f(x)\}$. Оно не пусто, т.к. $\min L \in S$. Пусть $x_0 = \sup S$ (его существование следует из полноты решетки). Необходимо показать, что $x_0 \in S$.

Для любого $s \in S$, во-первых, $s \leqslant f(s)$, во-вторых, поскольку $s \leqslant x_0$, то $f(s) \leqslant f(x_0)$ в силу монотонности $f$, следовательно, $s \leqslant f(x_0)$. Это значит, что $f(x_0)$ — верхняя грань $S$. Тогда по определению супремума $x_0 \leqslant f(x_0)$, откуда следует, что $x_0 \in S$, т.е. $x_0 = \max S$.

Если предположить, что $x_0 < f(x_0)$, то $f(x_0) \leqslant f(f(x_0))$, но тогда $f(x_0) \in S$ в противоречии с тем, что $x_0 = \max S$. Следовательно, $x_0 = f(x_0)$, т.е. это неподвижная точка $f$.

Кроме того, точка $x_0$ является наибольшей неподвижной точкой. Действительно, все неподвижные точки находятся в $S$, а $x_0 = \max S$.

Аналогично, рассматривая множество $S' = \{x \in L \mid x \geqslant f(x)\}$, по сути просто меняя во всех выкладках отношение на обратное, sup на inf и max на min, доказывается, что $x_1 = \min S'$ существует и является наименьшей неподвижной точкой функции $f$. □

Теорема Кантора-Бернштейна-Шрёдера позволяет относительно легко устанавливать некоторые равномощности. Например, легко построить инъекции из $\mathbb{N}$ в $\mathbb{Z}$ и в обратную сторону. Кроме того, теорему можно обобщить следующим образом: Если имеет место цикл $A_1 \preccurlyeq A_2 \preccurlyeq \ldots \preccurlyeq A_n \preccurlyeq A_1$, то все множества $A_1, \ldots, A_n$ попарно равномощны. Например, мы можем показать, что $\mathbb{Z} \preccurlyeq \mathbb{Q} \preccurlyeq \mathbb{Z} \times \mathbb{Z} \preccurlyeq \mathbb{Z}$, откуда следует, что все три множества равномощны.

Аналогично доказывается равномощность отрезка $[0;1]$ и квадрата $[0;1]^2$. Инъекция из отрезка в квадрат тривиальна, а чтобы построить инъекцию из квадрата в отрезок, можно воспользоваться «методом сплетения» десятичных записей: если $(a,b) \in [0;1]^2$, то $a = 0.a_0a_1a_2\ldots$, $b = 0.b_0b_1b_2\ldots$ (где $a_i, b_i$ — десятичные цифры), то по этим двум числам строится число $c = 0.a_0b_0a_1b_1a_2b_2\ldots$, которое принадлежит $[0;1]$.

Итерируя операцию взятия булеана произвольное число раз, мы можем придумать целую счетную последовательность бесконечных множеств с попарно различными кардинальностями:

$$\omega \prec \mathscr{P}(\omega) \prec \mathscr{P}(\mathscr{P}(\omega)) \prec \ldots \prec \mathscr{P}^n(\omega) \prec \ldots$$

Ясно, что все множества здесь, кроме первого, несчетны и неравномощны.

Отметим один важный момент: как бы нам ни хотелось написать, что множество $A$ бесконечно тогда и только тогда, когда $\omega \preccurlyeq A$, мы не можем этого утверждать в чистой теории ZF, поскольку не можем в ней доказать, что если $A$ бесконечно (неравномощно никакому $n \in \omega$), то существует инъекция из $\omega$ в $A$. Такая возможность у нас появится только с привлечением счетной аксиомы выбора $\mathrm{AC}_\omega$ (см. далее).

Кстати, множество $\mathscr{P}(\omega)$ равномощно вещественному отрезку $[0;1]$, поэтому $\mathrm{Card}(\mathscr{P}(\omega))$ называется **континуумом**. Специальный представитель класса $\mathrm{Card}(\mathscr{P}(\omega))$, обозначаемый $\mathfrak{c}$, за которым в дальнейшем будет закреплено понятие мощности континуума, также называется континуумом.

Георг Кантор безуспешно пытался отыскать множество промежуточной мощности — между счетным и континуальным, в результате чего построил множество красивых примеров очень «тонких» подмножеств $[0;1]$, но в итоге сформулировал свою знаменитую **континуум-гипотезу** CH: $\neg\exists A : \omega \prec A \prec \mathfrak{c}$.

Обобщенная континуум-гипотеза GCH: если $X$ бесконечно, то $\neg\exists A : X \prec A \prec \mathscr{P}(X)$ (в случае конечных множеств, как легко видеть, это не верно).

Как мы теперь знаем, CH и GCH не зависят от аксиом ZF, кроме того, CH не зависит от ZFC, а из GCH следует AC, причем GCH строго сильнее, чем AC.

### D4.2.2 Конечные множества

Сведя оценку мощности конечных и счетных множеств к конкретным объектам — множеству $\omega$ и его элементам, мы тем самым построили для них шкалу внутри теории ZF. Для измерения несчетных мощностей мы сможем продолжить эту шкалу за пределы $\omega$ только с помощью более сильной аксиомы, чем аксиома бесконечности, а именно, с помощью аксиомы выбора.

Но для начала нам нужно разобраться со структурой множества $\omega$ и некоторыми свойствами конечных множеств.

**Теорема D4.4.** *Множество $\omega$ (строго) вполне упорядочено отношением $\in$.*

*Доказательство.* Для начала вспомним обозначение $S(a) \overset{\text{def}}{\rightleftharpoons} a \cup \{a\}$ для последователя множества $a$.

**1)** Докажем, что на множестве $\omega$ работает принцип арифметической индукции в форме языка второпорядковой арифметики:

$$\forall A\ ((\varnothing \in A) \wedge (\forall x \in A : S(x) \in A) \to \omega \subseteq A). \tag{D4.6}$$

Действительно, всякое множество $A$, удовлетворяющее антецеденту данной импликации, является индуктивным, а значит, содержит в себе $\omega$ как минимальное индуктивное множество.

Отсюда также следует принцип индукции с произвольной формулой $\varphi$ языка ZF:

$$[\varphi(\varnothing) \wedge \forall x\ (\varphi(x) \to \varphi(S(x)))] \to \forall x \in \omega : \varphi(x).$$

Это легко вывести из предыдущего, полагая $A = \{x \mid (x \in \omega) \wedge \varphi(x)\}$.

**2)** Докажем предварительно несколько полезных лемм. Напомним определение: множество $a$ называется *транзитивным*, если $\forall x\ (x \in a) \to (x \subseteq a)$.

**Лемма D4.2** (о транзитивности)**.** *Множество $\omega$ и все его элементы транзитивны.*

*Доказательство.* Для доказательства транзитивности $\omega$ необходимо показать, что $\forall n\ (n \in \omega) \to (n \subseteq \omega)$. Рассмотрим множество $A = \{x \in \omega \mid x \subseteq \omega\}$.[6]

База индукции ($\varnothing \in A$): очевидно, т.к. $\varnothing \in \omega$ (в силу индуктивности $\omega$) и $\varnothing \subseteq \omega$.

Шаг индукции: введем гипотезу $(x \in \omega) \wedge (x \subseteq \omega)$. Тогда $S(x) \in \omega$ (в силу индуктивности $\omega$) и $S(x) = x \cup \{x\} \subseteq \omega$, т.к. $x \subseteq \omega$ в силу гипотезы, и $\{x\} \subseteq \omega$, т.к. $x \in \omega$ в силу гипотезы. Таким образом, если $x \in A$, то $S(x) \in A$, следовательно, $\omega \subseteq A$, т.е. $\forall x \in \omega : (x \in \omega) \wedge (x \subseteq \omega)$. Если теперь обозначить $\mathscr{A} \overset{\text{def}}{\rightleftharpoons} (x \in \omega)$ и $\mathscr{B} \overset{\text{def}}{\rightleftharpoons} (x \subseteq \omega)$, то в последней формуле под квантором стоит импликация $\mathscr{A} \to (\mathscr{A} \wedge \mathscr{B})$, из которой в логике высказываний выводится формула $\mathscr{A} \to \mathscr{B}$, которая соответствует нашей целевой формуле.

Докажем, что элементы $\omega$ также транзитивны, т.е. что для любого $n \in \omega$ имеет место $\forall y \in n : (y \subseteq n)$. Это доказательство также проводится индукцией по $n$.

База индукции ($n = \varnothing$): утверждение $\forall y \in \varnothing : (y \subseteq \varnothing)$ истинно вакуумно, так как в пустом множестве нет элементов.

Шаг индукции: предположим, что $n \in \omega$ является транзитивным множеством. Докажем, что $S(n)$ также транзитивен. Пусть $y \in S(n)$. Это означает, что $y \in n$ или $y = n$.

[6] Фактически это означает, что мы собираемся вести индукцию для формулы $(x \in \omega) \wedge (x \subseteq \omega)$, а вовсе не для исходной формулы.

Случай 1: $y \in n$. По индукционному предположению, $n$ транзитивно, поэтому $y \subseteq n$. Поскольку $n \subseteq S(n)$, то $y \subseteq S(n)$.

Случай 2: $y = n$. Нужно показать, что $n \subseteq S(n)$. Это следует непосредственно из определения $S(n)$. Таким образом, $S(n)$ является транзитивным множеством. Индукция завершена. □

Стоит отметить, что из транзитивности множества, вообще говоря, не следует транзитивность его элементов, даже если это множество индуктивно. Например, универсум фон Неймана $V_\omega$ транзитивен и индуктивен, но далеко не все его элементы транзитивны.

**Лемма D4.3.** *Для любого $n \in \omega$ если $(n \neq \varnothing)$, то $(\varnothing \in n)$.*

*Доказательство.* Доказываем индукцией. При $n = \varnothing$ утверждение истинно ввиду ложности антецедента. Далее пусть оно верно для $n$, т.е. $n = \varnothing \vee \varnothing \in n$, тогда $\varnothing \in S(n) = n \cup \{n\}$. Индукция завершена. □

**Лемма D4.4.** *Для любых $n, k \in \omega$ если $n \in k$, то $S(n) = k$ или $S(n) \in k$.*

*Доказательство.* Воспользуемся индукцией по $k$. База индукции ($k = \varnothing$): Посылка $n \in \varnothing$ всегда ложна, поэтому импликация истинна вакуумно.

Индукционный шаг: предположим, что лемма верна для $k$. Докажем, что она верна и для $S(k)$.

Пусть $n \in S(k)$. Это означает, что $n = k$ или $n \in k$. Рассмотрим оба случая:

Случай $n = k$: нужно доказать, что $S(k) = S(k)$ или $S(k) \in S(k)$. Первое утверждение — тавтология. Таким образом, для этого случая лемма выполняется.

Случай $n \in k$: Нам нужно доказать, что $S(n) = S(k)$ или $S(n) \in S(k)$.

По индукционному предположению, так как $n \in k$, то $S(n) = k$ или $S(n) \in k$. Если $S(n) = k$, то так как $k \in S(k)$, мы получаем $S(n) \in S(k)$. Если $S(n) \in k$, то так как $k \subseteq S(k)$, то $S(n) \in S(k)$.

В обоих подслучаях мы пришли к выводу $S(n) \in S(k)$, что доказывает лемму. □

**3)** Докажем, что $\in$ является строгим линейным порядком на $\omega$.

Транзитивность $\in$: если $x \in y$ и $y \in z$ (где $z \in \omega$), то, поскольку $z$ — транзитивное множество (лемма D4.2), из $y \in z$ следует $y \subseteq z$. А раз $x \in y$, то $x \in z$.

Антирефлексивность ($x \notin x$): Докажем индукцией, что $\forall n \in \omega : (n \notin n)$.

База ($n = \varnothing$): $\varnothing \notin \varnothing$ верно по определению пустого множества.

Шаг индукции: предположим $n \notin n$. Докажем $S(n) \notin S(n)$. Если бы $S(n) \in S(n) = n \cup \{n\}$, то $S(n) \in n$ или $S(n) = n$. $S(n) = n$ невозможно, так как $n \in S(n)$, но $n \notin n$. $S(n) \in n$ невозможно, так как $n$ транзитивно, и отсюда бы следовало $S(n) \subseteq n$, что также противоречит $n \notin n$. Следовательно, $n \notin n$ для всех $n \in \omega$.

Связность (закон трихотомии): докажем $\forall x, y \in \omega : (x = y \vee x \in y \vee y \in x)$ индукцией по $x$.

База индукции ($x = \varnothing$): Нужно доказать, что $\forall y \in \omega : (\varnothing = y \vee \varnothing \in y \vee y \in \varnothing)$. Так как $y \in \varnothing$ ложно, нужно доказать $\forall y \in \omega : (y = \varnothing \vee \varnothing \in y)$. А это в точности утверждение леммы D4.3.

Индукционный шаг: предположим, что для $n \in \omega$ выполняется формула $\forall y \in \omega : (n = y \vee n \in y \vee y \in n)$. Докажем это для $S(n)$. Пусть $y \in \omega$. По индукционному предположению для $y$ есть три варианта: **a)** $y = n$: тогда $y \in S(n)$, так как $n \in S(n)$; **b)**

$y \in n$: так как $n \subseteq S(n)$, то $y \in S(n)$; **c)** $n \in y$: тогда по лемме D4.4 либо $S(n) = y$, либо $S(n) \in y$.

Объединяя все случаи, мы видим, что для любой пары $S(n)$ и $y$ выполняется одно из условий: $y \in S(n)$, $y = S(n)$ или $S(n) \in y$. Индукция завершена.

Таким образом, отношение $\in$ является строгим линейным порядком на $\omega$.

**4)** Докажем, что $\omega$ вполне упорядочено отношением $\in$, т.е. что в любом непустом подмножестве $\omega$ существует $\in$-минимальный элемент.

Здесь мы пойдем путем, аналогичным тому, что мы проделали при установлении эквивалентности разных видов индукции в арифметике Пеано (раздел D3.2), а именно, покажем сначала второпорядковый вариант полной индукции на $\omega$.

**Лемма D4.5.** *Для любого множества $A$*

$$[\forall n \in \omega : (n \subseteq A) \to (n \in A)] \to (\omega \subseteq A). \tag{D4.7}$$

*Доказательство.* Возьмем произвольное множество $A$ и предположим, что для него верна посылка (D4.7) (Гипотеза 1). Пусть далее

$$A' = \{x \in \omega \mid S(x) \subseteq A\}.$$

Проверим, что для этого множества выполняется посылка индукции (D4.6).

База индукции: $\varnothing \in A'$, т.к. $\varnothing \in \omega$ (в силу индуктивности $\omega$ по определению) и $\varnothing \in A$ в силу Гипотезы 1, откуда $S(\varnothing) = \{\varnothing\} \subseteq A$.

Индуктивный шаг: пусть $x \in A'$, тогда $x \in \omega$ и $S(x) \subseteq A$. Но так как $S(x) \in \omega$ (в силу индуктивности $\omega$), то в силу Гипотезы 1 $S(x) \in A$, откуда следует, что $S(S(x)) = S(x) \cup \{S(x)\} \subseteq A$.

Таким образом, $A'$ удовлетворяет (D4.6), откуда $\omega \subseteq A'$, следовательно, $\forall n \in \omega : S(n) \subseteq A$, откуда $\forall n \in \omega : n \in A$ (поскольку $n \in S(n)$). Таким образом, $\omega \subseteq A$, и формула (D4.7) доказана. □

Далее, формула (D4.7) в чистом исчислении предикатов равносильна формуле

$$(B \neq \varnothing) \to \exists n \in \omega : (n \in B) \wedge (n \cap B = \varnothing), \tag{D4.8}$$

где $B = \omega \setminus A$. То есть во всяком непустом множестве $B \subseteq \omega$ найдется элемент $n$ такой, что в $B$ нет элементов, меньших его по отношению $\in$ (нет таких $x \in B$, что $x \in n$). А это и означает фундированность порядка $\in$ на множестве $\omega$.

Вместе с доказанной в пункте **3)** линейностью получаем, что $\in$ вполне упорядочивает множество $\omega$. □

Доказательство можно было бы сделать покороче, если воспользоваться аксиомой регулярности, но мы стараемся не привлекать эту аксиому без особой надобности, чтобы показать максимально возможную общность теорем для разных аксиоматик теории множеств. Заметим также, что регулярность выполняется для всех элементов $\omega$ как раз в силу его $\in$-фундированности, даже если мы не включаем аксиому регулярности в список аксиом теории множеств.

Ввиду доказанной теоремы отношение $\in$ для элементов $\omega$ будем обозначать более привычным знаком $<$.

**Лемма D4.6.** *Для любых $n, k \in \omega$ существует инъекция $f : n \to k$ тогда и только тогда, когда $n \leqslant k$.*

*Доказательство.* Справа налево очевидно, поскольку $n \leqslant k$ означает, что $n \subseteq k$ (по лемме о транзитивности D4.2). В этом случае тождественное отображение $f(x) = x$ является искомой инъекцией.

Докажем обратное утверждение $\forall k\ ((f : n \to k \text{ является инъекцией}) \to (n \leqslant k))$ индукцией по $n$.

База индукции: $n = \varnothing$. Утверждение верно, так как $\varnothing \leqslant k$ для любого $k$ по лемме D4.3.

Шаг индукции: Предположим, что утверждение верно для $n$, и докажем его для $S(n)$. Пусть имеется инъекция $f : S(n) \to m$. Нам нужно показать, что $S(n) \leqslant m$. Поскольку $S(n)$ непусто, то и $m$ непусто, следовательно $m > 0$ и существует его предшественник $m - 1 = \cup m$.

Наша цель — построить инъекцию из $n$ в $m - 1$, чтобы применить предположение индукции для $k = m - 1$. Рассмотрим ограничение $f$ на $n$, то есть $f \restriction n$. Это инъекция из $n$ в $m$. Область ее значений — $f[n] = \{f(x) \mid x \in n\}$.

Рассмотрим два случая:

Случай 1: $m - 1 \notin f[n]$. В этом случае вся область значений $f \restriction n$ является подмножеством $m - 1$. Таким образом, $f \restriction n$ — это инъекция из $n$ в $m - 1$. По предположению индукции отсюда следует, что $n \leqslant m - 1$.

Случай 2: $m - 1 \in f[n]$. Это означает, что существует некоторый элемент $s \in n$ такой, что $f(s) = m - 1$. Поскольку $f$ — инъекция и $s \in n$, то $s \neq n$, и, следовательно, $f(s) \neq f(n)$. Это значит, $f(n) \neq m - 1$. Так как $f(n) \in m$ и $f(n) \neq m - 1$, то $f(n) \in m - 1$. Обозначим $y_n = f(n)$.

Теперь построим новую функцию $g : n \to m - 1$ следующим образом:

$$g(x) = \begin{cases} y_n, & x = s, \\ f(x), & x \in n \text{ и } x \neq s. \end{cases}$$

Эта функция $g$ является инъекцией. Действительно, ее область значений — это $(f[n] \setminus \{m - 1\}) \cup \{y_n\}$, что является подмножеством $m - 1$. Инъективность $g$ следует из инъективности $f$ на $n \setminus \{s\}$ и того факта, что $y_n = f(n)$ не может быть значением $f$ на $n \setminus \{s\}$.

В обоих случаях мы построили инъекцию из $n$ в $m-1$. По предположению индукции, это означает, что $n \leqslant m - 1$. Из $n \leqslant m - 1$ следует, что $S(n) \leqslant m$ (если $n < m - 1$, то $S(n) \leqslant m - 1 < m$; если $n = m - 1$, то $S(n) = m$). Индукционный переход доказан. □

Из этой леммы следует, что мощность конечного множества определяется однозначно. Действительно, если $|X| = n$ и $|X| = k$, то существуют биекции $f : X \leftrightarrow n$ и $g : X \leftrightarrow k$, но тогда композиция $f \circ g^{-1}$ будет биекцией между $k$ и $n$, откуда по лемме следует, что $k \leqslant n$ и $n \leqslant k$, т.е. $n = k$.

**Теорема D4.5** (принцип Дирихле)**.** *Пусть множества $X$ и $Y$ непустые, конечные и $|Y| < |X|$, тогда:*

D1 *не существует инъекции из $X$ в $Y$;*

D2 *не существует сюръекции из $Y$ в $X$.*

*Доказательство.* Пусть $|X| = n$ и $|Y| = k$. Тогда $k < n$ по условию леммы. Если существует инъекция из $X$ в $Y$, то существует инъекция из $n$ в $k$ (он получается композицией

исходной инъекции с двумя биекциями между $X$ и $n$ и между $Y$ и $k$). Тогда по лемме D4.6 $n \leqslant k$, тогда не верно $n > k$ в силу доказанного ранее линейного упорядочения $\omega$.

Докажем, что D1→D2. Предположим, что существует сюръекция из $Y$ в $X$, тогда существует сюръекция $g : k \to n$, где $0 < k < n$ ($k = 0$ исключается, т.к. не существует сюръекции из пустого множества в непустое). Тогда определим функцию $f : n \to k$ по правилу

$$f(x) = \min\{y \in k \mid g(y) = x\}.$$

Это определение корректно в силу сюръективности $g$ и принципа фундированности $\omega$. Очевидно, что $f : n \to k$ является инъекцией, что противоречит D1. Следовательно, сюръекции из $Y$ в $X$ не существует. □

Принцип Дирихле в форме D1 можно переформулировать иначе:[7] если множества $X, Y$ конечные, $f : X \to Y$ и $|Y| < |X|$, то найдутся два *различных* элемента $x_1, x_2 \in X$ такие, что $f(x_1) = f(x_2)$. Принцип Дирихле является одним из мощнейших инструментов решения задач в конечной математике. Кроме того, в слабых арифметиках он оказывается равносильным принципу индукции, что лишний раз подчеркивает силу и значимость этого принципа.

Из принципа Дирихле следует такое свойство

**Следствие D4.1.** *Если множество $X$ конечно и $Y \subseteq X$, то $Y$ конечно и $|Y| \leqslant |X|$.*

*Доказательство.* Пусть $|X| = n$. Очевидно, что биекция между $X$ и $n$ подмножество $Y$ переносит в равномощное ему подмножество $n$. В таком случае, нам достаточно показать, что любое подмножество $Y \subseteq n$ конечно и имеет мощность $k \leqslant n$. Докажем это индукцией по $n$.

При $n = 0$ утверждение верно тривиально, т.к. $Y = n = \varnothing$.

Шаг индукции: предполагаем, что это верно для $n$, и доказываем для $S(n)$. Пусть $Y \subseteq S(n)$. Тут есть два варианта: $n \notin Y$ или $n \in Y$. В первом случае $Y \subseteq n$, и по предположению индукции мощность $Y$ существует и равна $k \leqslant n$, т.е. $k \leqslant S(n)$. Во втором случае рассмотрим множество $Y' = Y \setminus \{n\}$, тогда $Y' \subseteq n$ и тоже имеет мощность $k \leqslant n$, т.е. Существует биекция $f : Y' \leftrightarrow k$. Тогда построим функцию

$$g(x) = \begin{cases} f(x), & x \in Y', \\ k, & x = n. \end{cases}$$

Легко видеть, что $g : Y \leftrightarrow S(k)$. Но так как $k \leqslant n$, то $S(k) \leqslant S(n)$, и, следовательно, во втором случае также получаем, что $Y$ имеет мощность не больше, чем $S(n)$. Индукция завершена. □

**Следствие D4.2.** *Если $X$ конечное и $Y \subsetneq X$, то $|Y| < |X|$.*

*Доказательство.* Пусть $|X| = n$. Так как $Y \subsetneq X$, то по предыдущему следствию $|Y| = k \leqslant n$. Если $k = n$, то существует биекция $f : Y \leftrightarrow n$, тогда построим функцию

$$g(x) = \begin{cases} f(x), & x \in Y, \\ n, & x \in X \setminus Y, \end{cases}$$

[7] Если кроликов больше, чем корзин, и все кролики рассажены по корзинам, то в какой-то корзине обязательно будет не менее двух кроликов.

которая будет сюръекцией $n$ на $S(n)$, но это невозможно по принципу Дирихле D2, т.к. $n < S(n)$. Следовательно, $k < n$. □

Как видим, у конечного множества есть отличительный признак — оно неравномощно никакому своему собственному подмножеству. В то же время если мы возьмем, например, множество $\omega$, то оно равномощно, например, множеству $\omega \setminus \{\varnothing\}$, т.к. функция $S(n)$ на $\omega$ является биекцией между этими множествами.

Поэтому существует подход к определению конечных и бесконечных множеств, не связанный с понятием мощности и с натуральными числами. Множество $A$ называется **бесконечным по Дедекинду**, если оно равномощно своему собственному подмножеству. В противном случае оно называется **конечным по Дедекинду**.

**Следствие D4.3.** *Если $X$ конечно, то оно конечно по Дедекинду.*

*Доказательство.* Пусть $|X| = n$, где $n \in \omega$. Если бы $X$ было бесконечным по Дедекинду, то нашлась бы биекция $f : X' \leftrightarrow X$, где $X' \subsetneq X$. Но это невозможно по предыдущему следствию. Значит, $X$ конечно по Дедекинду. □

Отсюда также следует, что если множество бесконечно по Дедекинду, то оно бесконечно. Например, $\omega$ равномощно своему собственному подмножеству, следовательно, оно бесконечно по Дедекинду и (просто) бесконечно.

Однако на этом сходство определений в рамках теории ZF заканчивается. Дело в том, что если мы хотим доказать их эквивалентность, а точнее, показать, что всякое конечное по Дедекинду множество конечно, то нам придется использовать одну из слабых форм аксиомы выбора: $\mathrm{AC}_\omega$ (см. далее теорему D4.11).

## D4.3. Ординалы и кардиналы

Рассмотрим теперь еще один мощный теоретико-множественный инструмент, а именно, шкалу ординалов и связанные с нею теоремы. В частности, нашей целью является обоснование метода трансфинитных определений (рекурсий) и сопутствующего метода доказательства — трансфинитной индукции. Все необходимые определения уже были введены в разделе C1.3. Повторим лишь, что под **ординалом** мы понимаем транзитивное множество, *строго* вполне упорядоченное отношением принадлежности.[8] Класс всех ординалов принято обозначать Ord, а запись $\mathrm{Ord}(x)$ означает формулу, которая выражает свойство множества $x$ быть ординалом.

Из теоремы D4.4 и леммы D4.2 следует, что $\omega$ и все его элементы (натуральные числа фон Неймана) являются ординалами.

В разделе C1.3 мы также договорились, что будем обозначать ординалы греческими буквами и даже определили для них собственные кванторы, чтобы проще было записывать утверждения об ординалах. Кроме того, как и в случае $\omega$, договоримся наряду с записью $x \in \alpha$ использовать предикат $x < \alpha$, учитывая, что $\in$ является порядком на ординале. Такая двойственность записи принадлежности позволяет лучше понимать текст доказательств про ординалы.

[8] Такой выбор определения мотивирован тем, что он в точности обобщает свойства натуральных чисел фон Неймана ($n \in \omega$), которые, как было показано, обладают именно этими характеристиками. Кроме того, требование строгой вполне упорядоченности по $\in$ само по себе исключает циклы вида $x \in \cdots \in x$, что позволяет нам не апеллировать на данном этапе к аксиоме регулярности.

Ординалы разбиваются на три класса: к одному относится нулевой ординал $\varnothing$, к другому — все **последователи**, т.е. ординалы вида $S(\alpha)$, к третьему — все остальные, которые называются **предельными** ординалами. Класс всех предельных ординалов принято обозначать Lim, класс всех последователей — Succ. Обычно последователей обозначают греческими буквами из начала алфавита, а предельные ординалы как правило обозначаются $\lambda$ (с индексами или без таковых). Кроме того, обозначения натуральных чисел сохраняются и за обозначениями конечных ординалов, в частности, ординал $\varnothing$ обозначается как 0.

### D4.3.1 Рекурсия и индукция

**Теорема D4.6.** *В* ZF *доказуемы следующие теоремы:*

1° *элемент ординала есть ординал;*

2° *для любых ординалов $\alpha, \beta$: $\alpha \in \beta \leftrightarrow (\alpha \subsetneq \beta)$;*

3° *для любых ординалов $\alpha, \beta$: $\alpha \leqslant \beta$ или $\beta \leqslant \alpha$;*

4° *объединение и пересечение любого множества ординалов есть ординал;*

5° *класс всех ординалов вполне упорядочен отношением $\in$ и является собственно классом;*

6° *для любого ординала $\alpha$: $S(\alpha)$ есть ординал;*

7° *натуральные числа фон Неймана и $\omega$ являются ординалами;*

8° *индукция [$\varphi$]: $[\forall \alpha : (\forall x \in \alpha : \varphi(x, \vec{p})) \to \varphi(\alpha, \vec{p})] \to \forall \alpha : \varphi(\alpha, \vec{p})$;*

9° *рекурсивное определение [$\varphi$]: пусть $\varphi(g, b, \vec{p})$ определяет отображение типа $g \mapsto b$, т.е. $\forall x \exists! y : \ \varphi(x, y, \vec{p})$, тогда для любого ординала $\alpha$ существует функция $f$, определенная на $\alpha$ и такая, что для любого $\beta < \alpha$:*

$$\varphi(f \restriction \beta, f(\beta), \vec{p}). \tag{D4.9}$$

10° *как последователи, так и предельные ординалы образуют собственно классы.*

*Доказательство.* **1)** Пусть $\alpha$ — ординал и $x \in \alpha$. В силу транзитивности ординала $x \subseteq \alpha$, а значит, наследует строгую вполне упорядоченность из $\alpha$. Остается показать, что $x$ транзитивен. Пусть $y \in x$, тогда поскольку $x \subseteq \alpha$, имеем также, что $y \in \alpha$. Возьмем любой $z \in y$, тогда аналогично получаем, что $z \in \alpha$. В итоге имеем: $x, y, z \in \alpha$ и $z \in y \in x$, откуда в силу транзитивности отношения $\in$ на ординале $\alpha$ заключаем, что $z \in x$, т.е. $y \subseteq x$, т.е. $x$ транзитивен. Таким образом любой $x \in \alpha$ есть ординал.

**2)** Прямая импликация верна в силу транзитивности ординалов: $\alpha \in \beta \to \alpha \subsetneq \beta$ (равенство исключается в виду антирефлексивности $\in$ на ординале $\beta$). Пусть $\alpha \subsetneq \beta$. Тогда существует $\gamma = \min \beta \setminus \alpha$ (т.к. $\beta \setminus \alpha \neq \varnothing$). Пусть $x \in \gamma$, тогда $x \in \beta$ и $x \notin \beta \setminus \alpha$, т.к. $x < \min \beta \setminus \alpha$, откуда $x \in \alpha$. Обратно, если $x \in \alpha$, то $x \in \beta$ и $x \notin \beta \setminus \alpha$, т.е. $x < \gamma$, т.е. $x \in \gamma$. Следовательно, $\alpha = \gamma$, откуда $\alpha \in \beta$.

**3)** Очевидно, что $\gamma = \alpha \cap \beta$ есть ординал (транзитивность и вполне упорядоченность наследуются от $\alpha$ и $\beta$). По предыдущему пункту $\gamma \leqslant \alpha$ и $\gamma \leqslant \beta$. Если $\gamma < \alpha$ и $\gamma < \beta$, то

$S(\gamma) \subseteq \alpha \cap \beta$, т.е. $S(\gamma) \subseteq \gamma$, что невозможно, т.к. иначе было бы $\gamma \in \gamma$. Следовательно, $\gamma = \alpha$ или $\gamma = \beta$. Тогда вместе с предыдущим получаем, что $\alpha \leqslant \beta$ или $\beta \leqslant \alpha$.

**4)** Пусть $A$ — множество ординалов. Если $A = \varnothing$, то по определению $\bigcap A = \varnothing$, а это ординал. Если $A \neq \varnothing$, то так же, как в случае пересечения двух ординалов, свойство быть ординалом для множества $\bigcap A$ наследуется сразу ото всех элементов $A$. Кроме того, $\bigcap A = \min A$, если $A \neq \varnothing$, т.к. $\bigcap A \leqslant a$ для всех $a \in A$ (см. пункт 2).

По аксиоме объединения существует множество $a = \bigcup A$. Это множество транзитивно, т.к. если $x \in a$, то существует $\alpha \in A$ такой, что $x \in \alpha$, откуда по транзитивности ординала $\alpha$ имеем $x \subseteq \alpha$ и, следовательно, $x \subseteq a$. Более того, $a$ есть множество ординалов (применяем свойство 1 к $x \in \alpha$).

Пусть $x, y, z \in a$. Во-первых, заметим, что $\neg(x < x)$, т.к. существует $\alpha \in A$ такой, что $x \in \alpha$, а в ординале $\alpha$ принадлежность антирефлексивна. Во-вторых, пусть $x < y < z$, тогда существует ординал $\alpha \in A$ такой, что $z \in \alpha$, откуда по транзитивности $y \in \alpha$, откуда снова по транзитивности $x \in \alpha$, т.е. $x, y, z \in \alpha$, но тогда $x < z$ в силу свойств ординала $\alpha$. В-третьих, для произвольных $x, y \in a$ существуют $\alpha, \beta \in A$ такие, что $x \in \alpha$, $y \in \beta$. По пункту 3 $\alpha \leqslant \beta$ или $\beta \leqslant \alpha$. В первом случае получаем, что $x, y \in \beta$, а там они связаны отношением принадлежности, т.е. $(x < y) \vee (x = y) \vee (y < x)$, во втором случае аналогично. Таким образом, множество $a$ линейно упорядочено отношением $\in$.

Пусть $X \subseteq a$ и $X \neq \varnothing$. Так как $X$ — множество ординалов, то по уже доказанному $\bigcap X = \min X$. Следовательно, $a$ вполне упорядочено отношением $\in$. Таким образом, $a = \bigcup A$ есть ординал.

Кроме того, нетрудно видеть, что $a = \sup A$ в классе ординалов, т.к., с одной стороны, $x \leqslant a$ для любого $x \in A$, с другой стороны, если $x \leqslant \beta$ для всех $x \in A$ (т.е. $\beta$ есть верхняя грань $A$), то $a \leqslant \beta$.

**5)** Антирефлексивность, транзитивность и связность отношения $\in$ для любых ординалов следует из вышедоказанных пунктов. Далее, если $\mathscr{K}$ — некоторый непустой подкласс класса ординалов, то возьмем любой его элемент $\alpha \in \mathscr{K}$, тогда $\min \mathscr{K} = \min \mathscr{K} \cap S(\alpha)$, а последний существует, т.к. $\mathscr{K} \cap S(\alpha)$ — множество ординалов.

Иначе говоря, класс Ord можно рассматривать как самый большой ординал, включающий в себя все ординалы в качестве начальных отрезков. При этом сам класс Ord хоть и удовлетворяет формально определению ординала, однако таковым не является, потому что это собственно класс, т.е. он не является множеством. И это следует из следующего пункта.

**6)** $S(\alpha) = \alpha \cup \{\alpha\}$. Во-первых, $S(\alpha)$ транзитивен: действительно, если $x \in S(\alpha)$, то либо $x \in \alpha$, либо $x = \alpha$. В первом случае $x \subseteq \alpha \subseteq S(\alpha)$, т.к. $\alpha$ — ординал, во втором случае, очевидно, $\alpha \subseteq S(\alpha)$. Во-вторых, для доказательства того, что $S(\alpha)$ вполне упорядочен отношением $\in$, достаточно заметить, что множество $\alpha$ уже вполне упорядочено, а $S(\alpha)$ получается добавлением одного максимального элемента $\alpha$. Очевидно, что любое непустое подмножество $A \subseteq S(\alpha)$ будет иметь минимальный элемент: если $A \cap \alpha \neq \varnothing$, то это $\min(A \cap \alpha)$; если же $A \cap \alpha = \varnothing$, то $A = \{\alpha\}$ и $\min A = \alpha$.

Таким образом, если бы Ord был множеством, т.е. ординалом, то $S(\mathrm{Ord})$ тоже бы существовал как множество и был бы больше любого ординала, в том числе самого себя, что невозможно в силу антирефлексивности порядка на ординалах. Следовательно, Ord есть собственно класс. Это доказывает вторую часть утверждения пункта 5.

**7)** Как уже отмечалось, из теоремы D4.4 и леммы D4.2 следует, что $\omega$ и все его элементы (натуральные числа фон Неймана) являются ординалами.

**8)** Пусть для формулы $\varphi$ верна посылка

$$\forall \alpha : (\forall x < \alpha : \varphi(x)) \to \varphi(\alpha).$$

Допустим, что вывод не верен, т.е. $\exists \alpha : \neg\varphi(\alpha)$. Пусть тогда $\alpha$ — наименьший из таких ординалов, тогда $\forall x < \alpha : \varphi(x)$, откуда из посылки заключаем, что $\varphi(\alpha)$ в противоречии с предположением. Тем самым принцип трансфинитной индукции установлен.

**9)** Для доказательства теоремы о рекурсии переформулируем ее в более удобном виде, следуя обозначениям, введенным в разделе C1.3. Именно, пусть $\Phi_{\vec{p}}$ есть отображение-класс, определенное формулой $\varphi(g, b, \vec{p})$. Тогда существует отображение-класс $F$, определенное на классе ординалов и такое, что

$$F(\alpha) = \Phi_{\vec{p}}(F \restriction \alpha).$$

Доказательство поведем индукцией по $\alpha$, доказывая следующую формулу:

$$\psi(\alpha) \overset{\text{def}}{\leftrightarrow} \exists! f : S(\alpha) \to \mathfrak{V} : \forall \gamma \leqslant \alpha : f(\gamma) = \Phi_{\vec{p}}(f \restriction \gamma), \tag{D4.10}$$

после чего докажем согласованность всех таких функций $f$, что и даст нам тотальное на классе ординалов отображение $F$.

Шаг индукции: предположим, что $\psi(\beta)$ для всех $\beta < \alpha$. Требуется доказать $\psi(\alpha)$.

Как обычно при работе с ординалами требуется рассмотреть три случая в соответствии с классовой принадлежностью ординала. Пусть $\alpha = 0$. Тогда $\psi(0)$ означает, что существует функция $f : S(0) \to \mathfrak{V}$, определенная в нуле, и ее значение задается равенством $f(0) = \Phi_{\vec{p}}(f \restriction \varnothing) = \Phi_{\vec{p}}(\varnothing)$. По сути это и есть база рекурсии для функции-класса $F$.

Пусть $\alpha = S(\beta)$, тогда по индукционному предположению истинно $\psi(\beta)$, т.е. существует единственная функция $f : S(\beta) \to \mathfrak{V}$ такая, что $\forall \gamma \leqslant \beta : f(\gamma) = \Phi_{\vec{p}}(f \restriction \gamma)$, в том числе, $f(\beta) = \Phi_{\vec{p}}(f \restriction \beta)$. Задача состоит в том, чтобы продолжить эту функцию на точку $\{\alpha\}$. Определим функцию $f' : S(\alpha) \to \mathfrak{V}$ строго по нужной формуле:

$$f'(\gamma) \overset{\text{def}}{=\!=} \begin{cases} \Phi_{\vec{p}}(f), & \gamma = \alpha, \\ f(\gamma), & \gamma \leqslant \beta, \end{cases}$$

где мы воспользовались тем, что $f' \restriction \alpha = f \restriction S(\beta) = f$.

Наконец, пусть $\alpha \in \mathrm{Lim}$, и по предположению индукции для всех $\beta < \alpha$ существуют единственные функции $f_\beta : S(\beta) \to \mathfrak{V}$ такие, что $\forall \gamma \leqslant \beta : f_\beta(\gamma) = \Phi_{\vec{p}}(f_\beta \restriction \gamma)$. Тогда по аксиоме подстановки существует множество $\{f\beta \mid \beta < \alpha\}$ всех таких функций. Положим

$$f \overset{\text{def}}{=\!=} \bigcup \{f_\beta \mid \beta < \alpha\}.$$

Во-первых, нужно проверить, что $f$ — функция, определенная на $\alpha$. Пусть $\langle \gamma, a\rangle, \langle \gamma, b\rangle \in f$. Это значит, что существуют $\beta_1, \beta_2 < \alpha$ такие, что $f_{\beta_1}(\gamma) = a$ и $f_{\beta_2}(\gamma) = b$. Допустим, что $a \neq b$, и тогда в качестве $\gamma$ выберем наименьший такой ординал, что $f_{\beta_1}(\gamma) \neq f_{\beta_2}(\gamma)$. Это значит, что $f_{\beta_1}(\delta) = f_{\beta_2}(\delta)$ для всех $\delta < \gamma$, т.е. $f_{\beta_1} \restriction \gamma = f_{\beta_2} \restriction \gamma$. Но так как $f_{\beta_1}$ и $f_{\beta_2}$ удовлетворяют рекурсивной формуле, т.е. выполнено $\psi(\beta_1)$ и $\psi(\beta_2)$, то

$$f_{\beta_1}(\gamma) = \Phi_{\vec{p}}(f_{\beta_1} \restriction \gamma) = \Phi_{\vec{p}}(f_{\beta_2} \restriction \gamma) = f_{\beta_2}(\gamma).$$

Следовательно, предположение $a \neq b$ не верно, а значит, $f$ функционально. Нетрудно видеть также, что $f$ всюду на $\alpha$ определено, т.е. $f$ есть функция, определенная на $\alpha$.

Во-вторых, $f$ удовлетворяет рекурсивному тождеству, т.е. для любого $\beta < \alpha$: $f(\beta) = \Phi_{\vec{p}}(f \restriction \beta)$, поскольку $f \restriction S(\beta) = f_\beta$ является продолжением $f \restriction \beta$.

Наконец, расширим $f$ на точку $\{\alpha\}$ так же, как мы это делали в предыдущем случае, и получим функцию $f' : S(\alpha) \to \mathfrak{V}$, удовлетворяющую рекурсивному тождеству.

Нетрудно видеть, что $f'$ в обоих случаях определяется единственным способом. Таким образом, мы доказали $\psi(\alpha)$.

Отсюда по индукции мы приходим к тому, что $\psi(\alpha)$ истинно для всех $\alpha$.

Наконец, мы можем определить отображение-класс $F$, используя формулу:

$$d = F(\alpha) \overset{\text{def}}{\leftrightarrow} \exists! f : S(\alpha) \to \mathfrak{V} : ((f(\alpha) = d) \wedge \forall \gamma \leqslant \alpha : f(\gamma) = \Phi_{\vec{p}}(f \restriction \gamma)).$$

По сути отображение $F$ есть объединение всех функций $f$, существование и единственность которых гарантирует формула $\psi(\alpha)$, откуда легко понять, что $F$ всюду определено на классе Ord и функционально, т.е. если $a = F(\alpha)$ и $b = F(\alpha)$, то $a = b$ для любых ординалов $\alpha$ и любых множеств $a, b$.

На этом обоснование трансфинитного рекурсивного определения завершено.

Использование рекурсивных определений мы подробно обсуждали в разделе C1.3, в частности, тот факт, что как правило генератор рекурсии $\Psi_{\vec{p}}$ определяется отдельно для последователей и для предельных ординалов. Кроме того, не всегда требуется тотальное определение рекурсии на всем классе Ord, поэтому оно дается для нужного фрагмента этого класса, а для остальных ординалов предполагается какое-то дефолтное значение, не мешающее определению. Все эти мелочи достаточно обсудить один раз, чтобы потом пользоваться трансфинитной рекурсией относительно свободно.

**10)** Если бы класс Succ был множеством, то существовал бы последователь $S(\sup \mathrm{Succ})$, который не был бы элементом Succ. Следовательно, класс Succ является собственно классом ординалов. Чуть сложнее дело обстоит с классом Lim. Предположим, что это множество, тогда пусть $\lambda = \sup \mathrm{Lim}$. Предположим, что $\lambda \in \mathrm{Lim}$, т.е. $\lambda = \max \mathrm{Lim}$. Однако для любого ординала мы можем рекурсивно построить превосходящий его предельный ординал. Построим функцию $F$ с помощью доказанного выше свойства 9. Рассмотрим генератор

$$\Phi_\lambda(g) = \begin{cases} \lambda, & g = \varnothing; \\ S(\sup(\mathrm{ran}(g))), & g \neq \varnothing, \end{cases} \qquad F(\alpha) = \Phi_\lambda(F \restriction \alpha).$$

Положим $\lambda_\alpha \overset{\text{def}}{\rightleftharpoons} F(\alpha)$. Посмотрим, как ведет себя последовательность $\lambda$: $\lambda_0 = \Phi_\lambda(\varnothing) = \lambda$, $\lambda_1 = \Phi_\lambda(F \restriction 1) = S(\sup\{\lambda\}) = S(\lambda)$, $\lambda_2 = \Phi_\lambda(F \restriction 2) = S(\sup\{\lambda, S(\lambda)\}) = S(S(\lambda))$, и т.д., $\lambda_n = \Phi_\lambda(F \restriction n) = \underbrace{S \ldots S}_{n}(\lambda)$. Дальнейшие значения последовательности нам не интересны, поэтому на самом деле мы могли бы рассматривать рекурсивное определение только на начальном участке класса ориналов — ординале $\omega$, и определить генератор $\Phi_\lambda(x)$ не тотально, а только для конечных подмножеств $\omega$. Но так как мы впервые применяем эту теорему, мы постарались строго следовать ее условиям.

Итак, рассмотрим сужение последовательности $\lambda_\alpha$ на ординал $\omega$. По аксиоме подстановки область значений этого сужения есть множество ординалов вида $\underbrace{S \ldots S}_{n}(\lambda)$. Тогда ее предел $\Lambda = \sup\{\lambda_n \mid n < \omega\}$ является предельным ординалом (если бы он был последователем, у него был бы непосредственный предшественник. Однако $\Lambda$ как супремум

последовательности без максимального элемента не имеет непосредственного предшественника). $\Lambda$ больше, чем $\lambda$, т.е. $\Lambda > \max \mathrm{Lim}$ и $\Lambda \in \mathrm{Lim}$. Противоречие. Следовательно, класс Lim является собственно классом ординалов. □

Легко видеть, что $\alpha = S(\sup \alpha)$ тогда и только тогда, когда $\alpha$ — последователь. Предельные ординалы удовлетворяют тождеству $\lambda = \sup \lambda$.[9]

Метод доказательства с помощью (трансфинитной) индукции, которая идет в теореме под номером $8^o$, требует разбора случаев для трех типов ординала $\alpha$. Действительно, в посылке индукции требуется проверить переход

$$\forall \alpha : (\forall x \in \alpha : \varphi(x, \vec{p})) \to \varphi(\alpha, \vec{p}),$$

который удобнее делать разбором случаев для $\alpha = 0$, $\alpha \in \mathrm{Succ}$ и $\alpha \in \mathrm{Lim}$. При $\alpha = 0$ вакуумная истинность антецедента импликации требует от нас прямой проверки $\varphi(0)$, чтобы подтвердить истинность импликации, т.е. в точности как в обычной арифметической индукции. При $\alpha = S(\beta)$ антецедент предполагает истинность $\varphi(x)$ для всех $x \leqslant \beta$, но на самом деле как правило (хотя и не всегда) достаточно знать, что $\varphi(\beta)$, чтобы вывести $\varphi(\alpha)$, т.е. воспроизвести шаг локальной индукции, как в арифметике. Если же $\alpha \in \mathrm{Lim}$, то здесь начинают работать методы, связанные с порядковой топологией ординалов, поскольку нам по сути нужно доказать, что переходя к пределу $\alpha = \sup\{x \mid x < \alpha\}$, мы сохраняем истинность формулы $\varphi$. Это напоминает определение непрерывности функции из математического анализа:

$$\lim_{x \to \alpha - 0} \varphi(x) = \varphi(\alpha).$$

Так что в предельном случае мы так или иначе задействуем всю гипотезу индукционного шага, но для ординала, который сам задается как предел меньших (супремум).

Такое принципиальное отличие доказательства индукционного шага для трех видов ординалов почти всегда уместно и используется в доказательствах.

Еще одним вариантом индукции является отправление не с нуля, а с какого-то заданного ординала $\alpha_0$, когда м доказываем формулу вида $\forall \alpha \geqslant \alpha_0 : \varphi(\alpha, \vec{p})$. В этом случае у нас как бы появляется еще один, «вакуумный» тип ординалов, а именно ординалы $\alpha < \alpha_0$, т.к. для них проверка формулы индукционной посылки тривиальна. Поэтому обычно этот случай опускается, а оставшиеся случаи — это: $\alpha = \alpha_0$, $\alpha \in \mathrm{Succ} \wedge \alpha \geqslant \alpha_0$, $\alpha \in \mathrm{Lim} \wedge \alpha \geqslant \alpha_0$, что, безусловно, удобно. Так что при использовании индукции в дальнейшем мы не будем специально объяснять, почему мы пользуемся таким разбором случаев при доказательстве индукционного шага.

И еще один вариант индукции — доказательство в пределах какого-то ординала, а не на всем классе Ord.

Те же соображения относятся и к рекурсии: чаще всего генератор рекурсии определяется тремя разными формулами для трех видов ординалов, а также сама рекурсия может стартовать не обязательно с нуля, а с любого другого ординала. Вообще, индукция и рекурсия — это две стороны одной медали. Индукция — это метод доказательства, опирающийся на рекурсивную структуру объектов, а рекурсия — это метод

[9] Чисто формально $\sup \varnothing = 0$, т.к. любой ординал является верхней гранью пустого множества, поэтому некоторые авторы относят 0 к классу предельных ординалов. Однако заигрывание с пустым множеством приводит к тому, что его нижней гранью тоже является любой ординал, а в качестве $\inf \varnothing$ можно рассматривать класс Ord и, более того, для всякой верхней грани найдется превосходящая ее нижняя грань пустого множества, что звучит абсурдно, поэтому $\varnothing$ лучше рассматривать как особый объект и не применять к нему понятия граней, точных граней, max / min.

определения таких объектов. Соответственно, если мы определяем какую-то рекурсию, то большинство ее свойств будем доказывать индукцией.

### D4.3.2 Иерархия фон Неймана и ранг

Теперь, имея в распоряжении мощный аппарат трансфинитной рекурсии, мы можем формально построить иерархию универсумов, о которой шла речь в разделе C1.3.

Иерархия универсумов фон Неймана определяется рекурсивно по ординалам:

$$V_0 = \varnothing, \quad V_{\alpha+1} = \mathscr{P}(V_\alpha), \quad V_\lambda = \bigcup_{\beta<\lambda} V_\beta, \tag{D4.11}$$

где $\lambda$ — предельный ординал. Класс $\bigcup_{\alpha\in\mathrm{Ord}} V_\alpha$ называется **универсумом фон Неймана**. Ранее в разделе C1.3 мы показали, что отображение $V_\alpha$ строго монотонно, т.е. если $\alpha < \beta$, то $V_\alpha \subsetneq V_\beta$.

**Рангом** множества $A$ называется минимальный такой ординал, что $A \subseteq V_\alpha$.

Аксиома регулярности гарантирует, что любое множество принадлежит универсуму фон Неймана, т.е. имеет ранг.

**Теорема D4.7** (о ранге)**.** *Всякое множество является элементом и, следовательно, подмножеством некоторого универсума иерархии фон Неймана. Иначе говоря,* $\mathfrak{V} = \bigcup_{\alpha\in\mathrm{Ord}} V_\alpha$.

*Доказательство.* Предположим, что существует хотя бы одно множество, не имеющее ранга, обозначим его $A$. Построим его *транзитивное замыкание* $TC(A)$, которое определяется рекурсивно:

$$A_0 = A, \quad A_{n+1} = \bigcup A_n, \quad TC(A) = \bigcup\{A_n \mid n \in \omega\}.$$

Его существование в ZF гарантируется аксиомами объединения и подстановки, а также теоремой о рекурсивном определении. Легко видеть, что $TC(A)$ транзитивно. Действительно, если $x \in TC(A)$, то существует $n$ такой, что $x \in A_n$, тогда $x \subseteq A_{n+1}$, значит, $x \subseteq TC(A)$.

Рассмотрим множество $S = TC(A) \cup \{A\}$. Оно тоже транзитивно, т.к. $A \subseteq S$. Выделим из $S$ подмножество $B$, состоящее из всех элементов $S$, которые не имеют ранга:

$$B \stackrel{\text{def}}{=\!=} \{x \in S \mid \forall\alpha\ \neg(x \subseteq V_\alpha)\}.$$

По нашему начальному предположению, множество $A$ не имеет ранга, и так как $A \in S$, то $A \in B$. Следовательно, множество $B$ непусто.

Поскольку $B$ непустое множество, по аксиоме регулярности в нем существует $\in$-минимальный элемент. Назовем его $x_0$. Это означает, что:

1. $x_0 \in B$ (т.е. $\mathrm{rank}(x_0)$ не определен).
2. $x_0 \cap B = \varnothing$.

Так как $x_0 \in S$ и $S$ транзитивно, то все элементы $x_0$ также находятся в $S$. Но при этом элементы $x_0$ не принадлежат $B$ в силу минимальности $x_0$, значит, для всех элементов $x_0$ определен ранг. Пусть $\Lambda = \{\mathrm{rank}(y) \mid y \in x_0\}$. Это множество по аксиоме подстановки, а значит, это множество ординалов, и у него есть супремум (объединение), который мы обозначим за $\lambda$.

Теперь, поскольку $\forall y \in x_0 : \mathrm{rank}(y) \leqslant \lambda$, то в силу монотонности последовательности универсумов $\forall y \in x_0 : y \subseteq V_\lambda$, откуда следует, что $x \subseteq V_{\lambda+1}$, а это значит, что $x_0$ имеет ранг в противоречии с выбором $x_0 \in B$. □

### D4.3.3 Арифметика ординалов

**Лемма D4.7** (о порядковом типе)**.** *Если $\langle X, \prec\rangle$ — строго вполне упорядоченное множество, то существует единственный ординал $\alpha$ такой, что $\langle X, \prec\rangle \cong \langle \alpha, \in\rangle$.*

*Доказательство.* Иначе говоря, нужно показать, что существует единственный ординал $\alpha$, порядково изоморфный $X$. Дадим рекурсивное определение:

$$F(\alpha) = \begin{cases} \min\{x \in X \mid F[\alpha] \prec x\}, & \exists x \in X : F[\alpha] \prec x, \\ X, & \text{иначе,} \end{cases}$$

где $f[\alpha] \prec x$ означает, что $\forall \gamma < \alpha : f(\gamma) \prec x$. Иначе говоря, генератор рекурсии выбирает наименьшую *строгую* верхнюю грань подаваемого на вход множества, а если такой грани нет, то возвращает все множество $X$.

Второй случай нам на самом деле не интересен, т.к. он срабатывает, когда уже весь изоморфизм построен. Важно показать, что при каком-то ординале $\alpha$ это случится. Допустим, что это не так, т.е. что при любом $\alpha$ образ $F[\alpha]$ имеет строгую верхнюю грань. Это значит, что для всех ординалов $F(\alpha) = \min\{x \in X \mid F[\alpha] \prec x\}$. Отсюда легко видеть что при $\alpha < \beta$ имеем $F(\alpha) \prec F(\beta)$, т.е. $F$ представляет собой (монотонную) инъекцию. В таком случае возьмем полный образ $F[\mathrm{Ord}] \subseteq X$ и рассмотрим обратное отображение: $F^{-1} : F[\mathrm{Ord}] \leftrightarrow \mathrm{Ord}$, которое будет биекцией. Но поскольку $F[\mathrm{Ord}]$ является определяемой частью множества $X$, т.е. является множеством по аксиоме выделения, то в силу аксиомы подстановки Ord тоже будет множеством, а это, как мы ранее показали, не верно.

Следовательно, при каком-то $\alpha$ мы получим, что у образа $F[\alpha]$ нет строгой верхней грани в $X$. Обозначим за $\alpha_0$ наименьший из таких ординалов. Тогда, очевидно, $F[\alpha_0] \subseteq X$, причем $F$ строго монотонна на $\alpha_0$.

Предположим, что $F[\alpha_0] \subsetneq X$, т.е. найдется $y \in X \setminus F[\alpha_0]$. Пусть $y_0$ — наименьший из таких $y$. Далее возьмем начальный сегмент $Y = \{x \in X \mid x \prec y_0\}$. Ясно, что для любого $x \in Y$ найдется $\delta < \alpha_0$ такой, что $F(\delta) = x$. Боле того, прообраз $F^{-1}[Y]$ является ординалом (транзитивность следует из того, что если $\lambda < \delta \in F^{-1}[Y]$, то $\lambda \in F^{-1}[Y]$). Обозначим этот ординал за $\gamma$, тогда $F(\gamma) = \min\{x \in X \mid F[\gamma] \prec x\} = \min\{x \in X \mid Y \prec x\} = y_0$. Мы пришли в противоречие с тем, что $y_0$ не является значением $F$. Следовательно, $F[\alpha_0] = X$.

Итак, мы нашли ординал $\alpha_0$, изоморфный множеству $X$.

Единственность: предположим, что $\alpha_0 \cong \langle X, \prec\rangle \cong \alpha_1$, тогда $\alpha_0 \cong \alpha_1$, т.е. существует биекция $f : \alpha_0 \leftrightarrow \alpha_1$, сохраняющая порядок.

Покажем, что $f(\beta) \geqslant \beta$ для всех $\beta < \alpha_0$. Действительно, если это не так, то в качестве $\beta$ возьмем наименьший такой, что $f(\beta) < \beta$. Пусть $\gamma = f(\beta)$. Так как $f$ сохраняет порядок, то $f(\gamma) < f(\beta) = \gamma$. Стало быть, мы нашли ординал $\gamma < \beta$, для которого тоже выполнено $f(\gamma) < \gamma$ в противоречии с выбором $\beta$. Следовательно, $f(\beta) \geqslant \beta$ для всех $\beta < \alpha_0$.

Далее заметим, что $f^{-1}$ также является изоморфизмом, а значит, $f^{-1}(\beta) \geqslant \beta$ для всех $\beta < \alpha_1$, т.е. $f(\beta) \leqslant \beta$. Тогда, учитывая оба неравенства, получаем, что $f = \mathrm{id}_{\alpha_0}$, откуда следует, что $\alpha_0 = \alpha_1$. Единственность доказана. □

Операции на ординалах определяются следующим образом:

$$\begin{array}{lll} \alpha + 0 = \alpha, & \alpha \cdot 0 = 0, & \alpha^0 = 1, \\ \alpha + S(\beta) = S(\alpha + \beta), & \alpha \cdot S(\beta) = \alpha \cdot \beta + \alpha, & \alpha^{S(\beta)} = \alpha^\beta \cdot \alpha, \\ \alpha + \lambda = \sup\{\alpha + \gamma \mid \gamma < \lambda\}, & \alpha \cdot \lambda = \sup\{\alpha \cdot \gamma \mid \gamma < \lambda\}, & \alpha^\lambda = \sup\{\alpha^\gamma \mid 0 < \gamma < \lambda\}, \end{array}$$

где $\lambda \in \mathrm{Lim}$. Это — рекурсивное определение, которое обобщает аналогичное определение арифметических операций в PA. Заметим, что в определении $\alpha^\lambda$ добавлено ограничение $\gamma > 0$. Это связано с тем, что при $\alpha = 0$ получаем $0^{S(\beta)} = 0^\beta \cdot 0 = 0$, и поэтому $0^\gamma = 0$ при всех $\gamma > 0$, однако если допустить $\gamma = 0$, то получится $0^0 = 1$, и указанный в определении $\alpha^\lambda$ супремум уже будет равен 1, что приведет к рассогласованности определений.

У этих операций есть и другое, теоретико-множественное определение.

Пусть заданы два вполне упорядоченных множества $X, Y$ с отношениями порядка, соответственно, $<_X, <_Y$. Под их *упорядоченной суммой* мы будем понимать следующую конструкцию: носителем структуры будет множество $(X \times \{0\}) \cup (Y \times \{1\})$, которое для краткости будем обозначать как $X \sqcup Y$. Домножение на точки $\{0\}$ и $\{1\}$ защищает нас от возможных наложений $X$ и $Y$ друг на друга, т.к. $(X \times \{0\}) \cap (Y \times \{1\}) = \varnothing$. На множестве $X \sqcup Y$ определяется отношение $\prec$ по следующему правилу:

$$(a, b) \prec (c, d) \overset{\text{def}}{\leftrightarrow} (b = 0 \wedge d = 1) \vee (b = d = 0 \wedge a <_X c) \vee (b = d = 1 \wedge a <_Y c), \quad \text{(D4.12)}$$

т.е. все элементы $X$ меньше всех элементов $Y$, а внутри каждого из этих множеств работает исходное сравнение. Несложно показать, что $\prec$ будет вполне упорядочением: все свойства порядка наследуются из $X$ и $Y$. Оказывается, что в таком случае сложение ординалов удовлетворяет тождеству

$$ot(X \sqcup Y, \prec) = ot(X, <_X) + ot(Y, <_Y). \quad \text{(D4.13)}$$

Отметим, что если поменять местами $X$ и $Y$, то порядок $\prec$ будет, вообще говоря, другой.

Заменяя $X$ на ординал $\alpha$ (по лемме о порядковом типе) и $Y$ — на ординал $\beta$, докажем (D4.13) в виде $ot(\alpha \sqcup \beta) = \alpha + \beta$ индукцией по $\beta$.

Предположим, что формула верна для всех $\beta < \gamma$ и докажем ее для $\gamma$. Разбор случаев по типу ординала $\gamma$: $\gamma = 0$, $\gamma \in \mathrm{Succ}$, $\gamma \in \mathrm{Lim}$.

a) $\gamma = 0$, тогда $\alpha + 0 = \alpha$ и $ot(\alpha \sqcup \varnothing) = \alpha$, тождество выполняется.

b) Пусть $\gamma = S(\beta)$. По индукционному предположению $ot(\alpha \sqcup \beta) = \alpha + \beta$. Это значит, что имеется единственный порядковый изоморфизм $f : \alpha \sqcup \beta \leftrightarrow \alpha + \beta$. В то же время

$$\alpha \sqcup \gamma = \alpha \times \{0\} \cup \gamma \times \{1\} = \alpha \times \{0\} \cup (\beta \cup \{\beta\}) \times \{1\} = \\ (\alpha \times \{0\} \cup \beta \times \{1\}) \cup \{\langle \beta, 1 \rangle\} = (\alpha \sqcup \beta) \cup \{\langle \beta, 1 \rangle\}$$

и по рекурсивному определению сложения

$$\alpha + \gamma = \alpha + S(\beta) = S(\alpha + \beta) = (\alpha + \beta) \cup \{\alpha + \beta\}.$$

При этом $\alpha + \beta = \max_\in(\alpha + \gamma)$ и $\langle \beta, 1 \rangle = \max_\prec \alpha \sqcup \gamma$. Тогда определим функцию $g$:

$$g(x) = \begin{cases} f(x), & x \in \alpha \times \{0\} \cup \beta \times \{1\}, \\ \alpha + \beta, & x = \langle \beta, 1 \rangle, \end{cases}$$

иначе говоря, доопределим $f$ парой $\langle\langle\beta, 1\rangle, \alpha + \beta\rangle$ максимумов соответствующих множеств. Очевидно, что $g$ является порядковым изоморфизмом между $\alpha \sqcup \gamma$ и $\alpha + \gamma$. Отсюда следует, что $ot(\alpha \sqcup \gamma) = \alpha + \gamma$.

c) Самый сложный кейс: $\gamma \in \mathrm{Lim}$. По индукционному предположению $ot(\alpha \sqcup \beta) = \alpha + \beta$ для всех $\beta < \gamma$. Это значит, что для каждого $\beta < \gamma$ существует единственный порядковый изоморфизм $f_\beta : \alpha \sqcup \beta \leftrightarrow \alpha + \beta$. Эти изоморфизмы образуют цепь по вложению: если $\beta_1 \leqslant \beta_2$, то $f_{\beta_1} \subseteq f_{\beta_2}$. Действительно, рассмотрим сужение $g = f_{\beta_2} \restriction \alpha \sqcup \beta_1$. Это — строго монотонное отображение в ординал $\alpha + \beta_2$, обладающее свойством: $\mathrm{ran}(g)$ есть ординал, поскольку $\mathrm{ran}(g)$ является начальным сегментом ординала $\alpha + \beta_2$, а любой начальный сегмент ординала сам является ординалом. Поскольку $g$ — порядковый изоморфизм между $\alpha \sqcup \beta_1$ и $\mathrm{ran}(g)$, то $ot(\alpha \sqcup \beta_1) = \mathrm{ran}(g)$. По индукционному предположению, $ot(\alpha \sqcup \beta_1) = \alpha + \beta_1$. В силу единственности порядкового типа, $\mathrm{ran}(g) = \alpha + \beta_1$. А в силу единственности изоморфизма между двумя вполне упорядоченными множествами, $g$ должен совпадать с $f_{\beta_1}$. Следовательно, $f_{\beta_1} = f_{\beta_2} \restriction \alpha \sqcup \beta_1$.

Отсюда легко видеть, что $f = \bigcup\{f_\beta \mid \beta < \gamma\}$ является, во-первых, функцией, определенной на $\alpha \sqcup \gamma$, во-вторых, это строго монотонная функция из $\alpha \sqcup \gamma$ в $\alpha + \gamma$ (так как для любого $\beta < \gamma$ имеем $\alpha + \beta < \alpha + \gamma$ в силу определения сложения).

Нетрудно также видеть, что $f$ является сюръекцией, поскольку $\forall y \in \alpha + \gamma : \exists \beta < \gamma : y \in \alpha + \beta$ по определению сложения для предельного ординала. Тогда $\exists x \in \alpha \sqcup \beta : f(x) = f_\beta(x) = y$. Следовательно, $f$ есть порядковый изоморфизм между $\alpha \sqcup \gamma$ и $\alpha + \gamma$, т.е. $ot(\alpha \sqcup \gamma) = \alpha + \gamma$. Индукция завершена.

**Замечание**: из построения изоморфизма $f : \alpha \times \{0\} \cup \beta \times \{1\}$ в индукционном переходе вытекает одно его важное свойство: он оставляет первый компонент суммы на месте в том смысле, что $\mathrm{ran}(f \restriction \alpha \times \{0\}) = \alpha$.

Теперь проделаем то же самое с умножением. Пусть заданы два вполне упорядоченных множества $X, Y$ с отношениями порядка, соответственно, $<_X, <_Y$. Под их *антилексикографическим произведением* мы будем понимать следующую конструкцию: носителем структуры будет множество $X \times Y$, на котором определяется отношение $\prec$ по следующему правилу:

$$\langle a, b\rangle \prec \langle c, d\rangle \overset{\text{def}}{\leftrightarrow} (b <_Y d) \vee (b = d \wedge a <_X c), \tag{D4.14}$$

т.е. сравнение в $Y$ приоритетнее, чем в $X$: это можно понимать так, что мы в каждую точку $Y$ вставили клон $X$ и результат сравниваем сначала крупномасштабно (по точкам $Y$), а затем уже внутри каждого клона $X$.

Несложно показать, что отношение $\prec$ является вполне упорядочением. Действительно, его антирефлексивность наследуется из $<_X$ и $<_Y$. Для доказательства транзитивности предположим, что $\langle a, b\rangle \prec \langle c, d\rangle \prec \langle e, f\rangle$. Далее нужно рассмотреть все возможные варианты выполнения этих неравенств. Если все пары относятся к одной копии $X$, т.е. $b = d = f$, то включается сравнение внутри $X$, а оно транзитивно. Если $b <_Y d = f$ или $b = d <_Y f$ или $b <_Y d <_Y f$, то включается сравнение в $Y$, которое также транзитивно. Других вариантов в силу определения (D4.14) нет. Связность: для любых двух пар $\langle a, b\rangle$ и $\langle c, d\rangle$ сначала смотрим на $b$ и $d$: если $b <_Y d$ или $d <_Y b$, то сравнение для пар имеет место. Если же $b = d$, то либо $a <_X c$, либо $a = c$, либо $c <_X a$. В любом случае связность исходных порядков гарантирует связность порядка произведения.[10]

[10] Кстати говоря, таким же способом определяется линейное упорядочение на прямом произведении, например, так можно линейно упорядочить плоскость $\mathbb{C}$, правда, этот порядок не будет согласован с алгебраическими операциями на комплексных числах.

Наконец, пусть $A \subseteq X \times Y$ и $A \neq \varnothing$. Как найти его минимум? Для этого мы сначала спроецируем его на $Y$: рассмотрим множество $A_Y = \{y \mid \exists x \langle x, y\rangle \in A\}$. Это множество не пусто, пусть $y_0 = \min A_Y$. Далее слой множества $A$, соответствующий $y_0$, спроецируем на $X$, т.е. рассмотрим множество $B = \{x \mid \langle x, y_0\rangle \in A\}$. Пусть $x_0 = \min B$. Тогда, как легко видеть, $\langle x_0, y_0\rangle = \min A$.

Оказывается, что и в этом случае имеет место равенство:

$$ot(X \times Y, \prec) = ot(X, <_X) \cdot ot(Y, <_Y). \tag{D4.15}$$

Отметим, что если поменять местами $X$ и $Y$, то порядок $\prec$ будет, вообще говоря, другой.

Заменяя $X$ на ординал $\alpha$ (по лемме о порядковом типе) и $Y$ — на ординал $\beta$, докажем (D4.15) в виде $ot(\alpha \times \beta) = \alpha \cdot \beta$ индукцией по $\beta$.

Предположим, что формула верна для всех $\beta < \gamma$ и докажем ее для $\gamma$. Разбор случаев по типу ординала $\gamma$: $\gamma = 0$, $\gamma \in \mathrm{Succ}$, $\gamma \in \mathrm{Lim}$.

a) $\gamma = 0$, тогда $\alpha \times \gamma = \varnothing$ и $\alpha \cdot \gamma = \alpha \cdot 0 = 0$, тождество $ot(\alpha \times \varnothing) = \alpha \cdot 0$ выполняется.

b) Пусть $\gamma = S(\beta)$. По индукционному предположению $ot(\alpha \times \beta) = \alpha \cdot \beta$. В то же время

$$\alpha \times \gamma = \alpha \times S(\beta) = \alpha \times (\beta \cup \{\beta\}) = (\alpha \times \beta) \cup (\alpha \times \{\beta\})$$

и по определению умножения

$$\alpha \cdot \gamma = \alpha \cdot S(\beta) = \alpha \cdot \beta + \alpha.$$

При этом все элементы $\alpha \times \{\beta\}$ строго больше в смысле $\prec$, чем все элементы $\alpha \times \beta$, и упорядочены так же, как ординал $\alpha$. Тогда множество $(\alpha \times \beta) \cup \alpha \times \{\beta\}$ можно рассматривать как упорядоченную сумму $(\alpha \times \beta) \sqcup \alpha \times \{\beta\}$, а значит, по доказанному для упорядоченной суммы имеет место равенство

$$ot((\alpha \times \beta) \sqcup (\alpha \times \{\beta\})) = ot(\alpha \times \beta) + ot(\alpha \times \{\beta\}) = \alpha \cdot \beta + \alpha = \alpha \cdot \gamma,$$

что и требовалось.

c) Пусть $\gamma \in \mathrm{Lim}$. По индукционному предположению $ot(\alpha \times \beta) = \alpha \cdot \beta$ для всех $\beta < \gamma$. Это значит, что для каждого $\beta < \gamma$ существует единственный порядковый изоморфизм $f_\beta : \alpha \times \beta \leftrightarrow \alpha \cdot \beta$. Эти изоморфизмы образуют цепь по вложению: если $\beta_1 \leqslant \beta_2$, то $f_{\beta_1} \subseteq f_{\beta_2}$, т.к. сужение $f_{\beta_2} \restriction \alpha \times \beta_1$ совпадает с $f_{\beta_1}$ (здесь можно использовать те же рассуждения, что и в пункте c) доказательства для сложения).

Отсюда легко видеть, что $f = \bigcup\{f_\beta \mid \beta < \gamma\}$ является, во-первых, функцией, определенной на $\alpha \times \gamma$, во-вторых, это строго монотонная функция из $\alpha \times \gamma$ в $\alpha \cdot \gamma$ (так как для любого $\beta < \gamma$ имеем $\alpha \cdot \beta < \alpha \cdot \gamma$ в силу определения умножения). Сюръективность $f$ доказывается аналогично доказательству для сложения. Следовательно, $f$ есть порядковый изоморфизм между $\alpha \times \gamma$ и $\alpha \cdot \gamma$, т.е. $ot(\alpha \times \gamma) = \alpha \cdot \gamma$. Индукция завершена.

Эквивалентное определение возведения в степень также существует, хотя и является более сложным. Оно связано с упорядочением множества функций с *конечным носителем*. Пусть заданы два вполне упорядоченных множества $X, Y$ с отношениями порядка, соответственно, $<_X, <_Y$. Носителем структуры, определяющей степень ординалов является множество всех функций из $Y$ в $X$ с конечным носителем, т.е. $F^{fin}(Y, X) = \{f : Y \to X \mid |\operatorname{supp}(f)| < \omega\}$, где $\operatorname{supp}(f) = \{y \in Y \mid f(y) \neq 0\}$ — носитель функции $f$, где 0 обозначает $\min Y$.

*Антилексикографический порядок* $\prec$ на этом множестве определяется так: для $f, g \in F^{fin}(Y, X)$, $f \neq g$, положим $\delta = \max\{y \in Y \mid f(y) \neq g(y)\}$ (максимальная точка расхождения функций, она существует в силу конечности носителей обеих функций). Тогда

$$f \prec g \overset{\text{def}}{\leftrightarrow} f(\delta) <_X g(\delta). \tag{D4.16}$$

Докажем, что отношение $\prec$ на $F^{fin}(Y, X)$ является отношением строгого вполне упорядочения.

*Линейность порядка*. Пусть $f, g \in F^{fin}(Y, X)$ и $f \neq g$. Множество $D = \{y \in Y \mid f(y) \neq g(y)\}$ не пусто и является подмножеством конечного множества $\operatorname{supp}(f) \cup \operatorname{supp}(g)$, следовательно, $D$ конечно и имеет максимальный элемент $\delta = \max D$. Поскольку $<_X$ является линейным порядком, то либо $f(\delta) <_X g(\delta)$, либо $g(\delta) <_X f(\delta)$. В первом случае $f \prec g$, во втором $g \prec f$. Транзитивность доказывается разбором случаев для положений максимумов, аналогично доказательству для антилексикографического произведения.

*Фундированность*. Мы докажем фундированность конструктивно, построив для любого непустого подмножества $F^{fin}(Y, X)$ его минимальный элемент. Алгоритм заключается в итеративном отсеивании «больших» функций. Не умаляя общности, можно считать, что $X$ и $Y$ — ординалы, это позволяет использовать более простые обозначения.

Пусть $A \subseteq F^{fin}(Y, X)$ — непустое множество функций. Необходимо найти его минимум. Определим убывающую последовательность множеств $A_k \subseteq A$ рекурсивно.

1) База рекурсии: $A_0 = A$. Пусть, кроме того, $y_0 = Y$.

2) Шаг рекурсии: пусть заданы $A_k$ и $y_k$, тогда положим

$$\begin{aligned} y_{k+1} &= \min\{\max \operatorname{supp}(f \restriction y_k) \mid f \in A_k\}, \\ B &= \{f \in A_k \mid \max \operatorname{supp}(f \restriction y_k) = y_{k+1}\}, \\ z &= \min\{f(y_{k+1}) \mid f \in B\}, \\ A_{k+1} &= \{f \in B \mid f(y_{k+1}) = z\}, \end{aligned}$$

где $f \restriction y_k \overset{\text{def}}{=\!=} f \restriction \{y \in Y \mid y < y_k\}$, т.е. на каждом шаге рекурсии мы сначала выбираем функции, у которых носители, лежащие ниже $y_k$, максимально близки к нулю (максимум носителя минимальный), это множество $B$, затем смотрим, какие значения в точке $y_{k+1}$ принимают все эти функции, и оставляем только те функции, которые принимают там минимальное значение, собираем их в множество $A_{k+1}$.

При этом, очевидно, имеют место неравенства: $A_{k+1} \subseteq A_k$, причем в $A_k$ нет элементов, строго меньших, чем все элементы $A_{k+1}$, т.е. $A_{k+1}$ содержит минимум $A_k$, если только он есть.

Заметим, что у нас получается строго убывающая последовательность $\langle y_k \rangle$ во вполне упорядоченном множестве $Y$, а значит, она конечная, т.е. при каком-то $k$ у нас отсутствует возможность построить $y_{k+1}$ и $A_{k+1}$.

Почему это может произойти? Из построения видно, что это возможно только в том случае, когда $\operatorname{supp}(f \restriction y_k) = \varnothing$ для всех $f \in A_k$. Это означает, что все носители функций $f \in A_k$ содержат только точки $\geqslant y_k$.

Но в $A_k$ мы собирали только функции, у которых одинаковые значения в точке $y_k$, а также во всех предыдущих точках $y_j$, $0 < j \leqslant k$, т.е. в $A_k$ находится единственная функция, и она является минимумом $A$.

Таким образом, фундированность доказана.

Поскольку $F^{fin}(Y,X)$ вполне упорядочено отношением $\prec$, существует единственный ординал, являющийся его порядковым типом. Можно доказать, что

$$ot(F^{fin}(Y,X),\prec) = ot(X,<_X)^{ot(Y,<_Y)}. \tag{D4.17}$$

Снова для удобства будем доказывать это равенство для ординалов, т.е. $ot(F^{fin}(\beta,\alpha)) = \alpha^\beta$. Доказываем индукцией по $\beta$.

1) База индукции: $\beta = 0$, тогда $F^{fin}(\varnothing,\alpha) = \{\varnothing\}$, т.е. в этом множестве есть единственная функция — пустая. Откуда очевидно, что $ot(F^{fin}(\varnothing,\alpha)) = 1$, что соответствует рекурсивному определению $\alpha^0 = 1$.

2) Шаг индукции: предполагаем, что $ot(F^{fin}(\beta,\alpha)) = \alpha^\gamma$ для всех $\gamma < \beta$.

2.1) Индуктивный переход для последователя: $\beta = S(\gamma)$. Множество $F^{fin}(\beta,\beta)$ состоит из функций $f : S(\gamma) \to \alpha$ с конечным носителем. Каждой такой функции взаимно однозначно соответствует пара $\langle f',\delta\rangle$, где $f' = f \restriction \gamma$ и $\delta = f(\gamma)$. Иначе говоря, мы сводим функцию на $S(\gamma)$ к двум компонентам — сужению ее на ординал $\gamma$ и ее значению в точке $\gamma$. При этом $f' \in F^{fin}(\gamma,\alpha)$, $\delta \in \alpha$, так что указанное соответствие есть биекция $h : F^{fin}(\beta,\alpha) \leftrightarrow F^{fin}(\gamma,\alpha) \times \alpha$.

Теперь введем на множестве $F^{fin}(\gamma,\alpha) \times \alpha$ антилексикографический порядок $\prec_1$ по формуле (D4.14), а на множествах $F^{fin}(\beta,\alpha)$ и $F^{fin}(\gamma,\alpha)$ — порядки $\prec$ и $\prec'$ по формуле (D4.16). Докажем, что для любых $f,g \in F^{fin}(\beta,\alpha)$ имеет место формула

$$(f \prec g) \leftrightarrow (h(f) \prec_1 h(g)).$$

Действительно, пусть $\delta$ — решающая точка для $f$ и $g$, тогда $(f \prec g) \leftrightarrow (f(\delta) < g(\delta))$. При этом $\delta \in S(\gamma)$, т.е. либо $\delta < \gamma$, либо $\delta = \gamma$.

При $\delta < \gamma$ имеем, во-первых, что $(f \prec g) \leftrightarrow (f' \prec' g')$, а во-вторых, что $f(\gamma) = g(\gamma) = x$ (по определению решающей точки), что равносильно $h(f) = \langle f',x\rangle$ и $h(g) = \langle g',x\rangle$. Таким образом при $\delta < \gamma$ по определению порядка $\prec_1$ будем иметь:

$$(h(f) \prec_1 h(g)) \leftrightarrow (f' \prec' g') \leftrightarrow (f \prec g).$$

При $\delta = \gamma$ получаем, что $(f \prec g) \leftrightarrow f(\gamma) < g(\gamma)$, а это равносильно отношению $\langle f',f(\gamma)\rangle \prec_1 \langle g',g(\gamma)\rangle$ по определению порядка $\prec_1$.

Итак, $h$ — не просто биекция, но еще и порядковый изоморфизм между структурами $\langle F^{fin}(\beta,\alpha),\prec\rangle$ и $\langle F^{fin}(\gamma,\alpha)\times\alpha,\prec_1\rangle$, т.е. они имеют один и тот же порядковый тип и, следовательно, верны равенства:

$$ot(F^{fin}(\beta,\alpha)) = ot(F^{fin}(\gamma,\alpha)\times\alpha) = ot(F^{fin}(\gamma,\alpha))\cdot\alpha = \alpha^\gamma\cdot\alpha = \alpha^\beta,$$

где второе равенство получено из (D4.15), третье — по предположению индукции, а четвертое — по рекурсивному определению степени ординалов.

2.2) Индуктивный переход для предельного ординала $\beta \in \mathrm{Lim}$. Здесь заметим, что все функции из $F^{fin}(\beta,\alpha)$ можно рассматривать как функции из множеств $F^{fin}(\gamma,\alpha)$, $\gamma < \beta$, переходя к их сужениям $f \mapsto f'$, что сразу дает намек на доказательство.

Поэтому, взяв произвольный ординал $\gamma < \beta$, мы можем построить изоморфное вложение $F^{fin}(\gamma,\alpha)$ в $F^{fin}(\beta,\alpha)$ по следующему правилу: функции $f' \in F^{fin}(\gamma,\alpha)$ ставится в соответствие функция $f$, которая продлевает $f'$ на весь ординал $\beta$ нулевыми значениями. Это соответствие будет собственным, поскольку в его область значений не попадут функции, носитель которых имеет точки не ниже $\gamma$). Такое вложение означает, что

$$ot(F^{fin}(\gamma,\alpha)) < ot(F^{fin}(\beta,\alpha)),$$

поэтому, пользуясь предположением индукции, заключаем, что $ot(F^{fin}(\beta,\alpha)) > \alpha^\gamma$ для всех $\gamma < \beta$, откуда

$$ot(F^{fin}(\beta,\alpha)) \geqslant \alpha^\beta,$$

где мы воспользовались рекурсивным определением $\alpha^\beta = \sup\{\alpha^\gamma \mid \gamma < \beta\}$.

Чтобы доказать обратное неравенство, покажем, что порядковый тип любого начального отрезка множества $(F^{fin}(\beta,\gamma), \prec)$ не превышает $\alpha^\beta$. Возьмем произвольную функцию $f \in F^{fin}(\beta,\alpha)$ и рассмотрим начальный отрезок, определяемый ею: $I_f = \{g \in F^{fin}(\beta,\alpha) \mid g \preccurlyeq f\}$. Поскольку носитель $f$, $\mathrm{supp}(f)$, является конечным подмножеством предельного ординала $\beta$, он ограничен сверху и, более того, $\gamma = S(\max \mathrm{supp}(f)) < \beta$.

Докажем, что для любой функции $g \prec f$ ее носитель $\mathrm{supp}(g)$ также является подмножеством $\gamma$. Предположим противное: пусть существует $g \prec f$ такая, что $\max(\mathrm{supp}(g)) \geqslant \gamma$. Пусть $\delta_{max} = \max(\mathrm{supp}(g))$. Тогда $\delta_{max} \geqslant \gamma > \max \mathrm{supp}(f)$. В точке $\delta_{max}$ имеем $g(\delta_{max}) > 0$, в то время как $f(\delta_{max}) = 0$, поскольку $\delta_{max}$ не принадлежит носителю $f$. «Решающая» точка для сравнения $f$ и $g$ — это $\max\{y \mid f(y) \neq g(y)\}$. Поскольку функции отличаются в точке $\delta_{max}$, а выше нее $g$ может быть не равна нулю, в то время как $f$ равна нулю, то «решающая» точка будет не меньше $\delta_{max}$. Но в этой точке $f = 0$, а $g > 0$, что означало бы $f \prec g$. Это противоречит нашему предположению, что $g \prec f$. Следовательно, для любой функции $g \prec f$ выполняется $\mathrm{supp}(g) \subseteq \gamma$.

Это означает, что весь начальный отрезок $I_f$ является подмножеством множества функций с носителем в $\gamma$. Это множество, в свою очередь, изоморфно $F^{fin}(\gamma,\alpha)$ (через сопоставление $f \mapsto f \restriction \gamma$). Таким образом, мы имеем вложение, сохраняющее порядок, из $I_f$ в $F^{fin}(\gamma,\alpha)$. Отсюда следует, что порядковый тип $I_f$ не может превышать порядковый тип $F^{fin}(\gamma,\alpha)$:

$$ot(I_f) \leqslant ot(F^{fin}(\gamma,\alpha)).$$

По индукционному предположению, $ot(F^{fin}(\gamma,\alpha)) = \alpha^\gamma$. Итак, для любой функции $f \in F^{fin}(\beta,\alpha)$, порядковый тип множества ее предшественников не превышает $\alpha^\gamma$ для некоторого $\gamma < \beta$.

Порядковый тип всего множества $F^{fin}(\beta,\alpha)$ равен супремуму порядковых типов всех его собственных начальных отрезков.

$$ot(F^{fin}(\beta,\alpha)) = \sup\{ot(I_f) \mid f \in F^{fin}(\beta,\alpha)\}.$$

А поскольку для каждого $f$ мы нашли $\gamma < \beta$ такой, что $ot(I_f) \leqslant \alpha^\gamma$, то

$$ot(F^{fin}(\beta,\alpha)) \leqslant \sup\{\alpha^\gamma \mid \gamma < \beta\}.$$

Правая часть по рекурсивному определению степени равна $\alpha^\beta$. Таким образом, $ot(F^{fin}(\beta,\alpha)) \leqslant \alpha^\beta$.

Объединяя оба неравенства, получаем $ot(F^{fin}(\beta,\alpha)) = \alpha^\beta$. На этом индукция завершена.[11]

Тем самым мы доказали следующее утверждение.

**Лемма D4.8** (об эквивалентности определений)**.** *Определения суммы, произведения и степени ординалов через рекурсивные определения и по формулам* (D4.12)*,* (D4.14)*,* (D4.16) *эквивалентны.*

[11] Мы использовали здесь прямой путь доказательства, хотя если бы мы чуть ранее изложили здесь теорию упорядоченных множеств, то доказательство этой части было бы намного короче: мы бы просто сказали, что $ot(F^{fin}(\beta,\alpha)) = \sup\{ot(F^{fin}(\gamma,\alpha)) \mid \gamma < \beta\}$.

Это весьма полезная лемма, которая позволяет в ряде случаев сильно упростить доказательство алгебраических свойств ординалов.

**Теорема D4.8.** *Алгебраические свойства ординалов:*

1° $S(\alpha) = \alpha + 1$, $0 + \alpha = \alpha$, $0 \cdot \alpha = 0$, $\alpha \cdot 1 = \alpha = 1 \cdot \alpha$.

2° *Некоммутативность:* $\omega + 2 \neq 2 + \omega$, $\omega \cdot 2 \neq 2 \cdot \omega$.

3° *Правая дистрибутивность нарушается:* $(1+1)\cdot\omega = 2\cdot\omega = \omega$. *Но* $(1\cdot\omega)+(1\cdot\omega) = \omega + \omega$.

4° *Ассоциативность:* $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$, $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$.

5° *Левая дистрибутивность:* $\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$.

6° *Правая строгая монотонность сложения:* $\beta < \gamma \Leftrightarrow \alpha + \beta < \alpha + \gamma$.

7° *Правая строгая монотонность умножения: если* $\alpha > 0$, *то* $\beta < \gamma \Leftrightarrow \alpha \cdot \beta < \alpha \cdot \gamma$.

8° *Левая нестрогая монотонность: если* $\alpha < \beta$, *то* $\alpha + \gamma \leqslant \beta + \gamma$ *и* $\alpha \cdot \gamma \leqslant \beta \cdot \gamma$.

9° *Отсутствие делителей нуля: если* $\alpha \cdot \beta = 0$, *то* $\alpha = 0$ *или* $\beta = 0$.

10° *Единственность вычитания: если* $\beta \leqslant \alpha$, *то существует единственный ординал* $\gamma$ *такой, что* $\beta + \gamma = \alpha$.

11° *Возможность деления с остатком: для любых* $\alpha$ *и* $\beta > 0$ *существует единственная пара* $\gamma, \delta$ *таких, что* $\alpha = \beta \cdot \gamma + \delta$, *где* $\delta < \beta$.

12° *Свойства степени:* $1^\alpha = 1$; $\alpha^1 = \alpha$;

13° *Дистрибутивность по показателю степени:* $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$;

14° *Монотонность степени: если* $\alpha > 1$ *и* $\beta < \gamma$, *то* $\alpha^\beta < \alpha^\gamma$;

15° *Мультипликативность степени:* $(\alpha^\beta)^\gamma = \alpha^{\beta\cdot\gamma}$.

16° *Нарушение дистрибутивности по основанию степени: например,* $(2\cdot 2)^\omega = 4^\omega = \omega$, *но* $2^\omega \cdot 2^\omega = \omega \cdot \omega = \omega^2 > \omega$.

*Доказательство.* **1)** Напомним, что первые ординалы мы обозначаем как натуральные числа, т.е. $0 = \varnothing$, $1 = S(\varnothing)$, $2 = S(1)$, и т.д. Тогда из определения сложения ординалов легко видеть, что $\alpha + 1 = \alpha + S(0) = S(\alpha + 0) = S(\alpha)$. Заметим, что $0 + \alpha = \alpha$ уже приходится доказывать тансфинитной индукцией: $0+0 = 0$ по определению, $0+S(\alpha) = S(0+\alpha) = S(\alpha)$, $0 + \lambda = \sup\{0 + \beta \mid \beta < \lambda\} = \lambda$, где мы пользуемся индукционной гипотезой и рассматриваем два разных случая шага индукции: для последователя и для предельного ординала $\lambda$.

Аналогично доказываем, что $0\cdot\alpha = 0$: $0\cdot 0 = 0$ по определению, $0\cdot S(\alpha) = 0\cdot\alpha + 0 = 0$, $0 \cdot \lambda = \sup\{0 \cdot \beta \mid \beta < \alpha\} = 0$.

По определению $\alpha \cdot 1 = \alpha \cdot S(0) = \alpha \cdot 0 + \alpha = \alpha$. Индукцией доказываем $1\cdot\alpha$: $1\cdot 0 = 0$, $1 \cdot S(\alpha) = 1 \cdot \alpha + 1 = \alpha + 1 = S(\alpha)$, $1 \cdot \lambda = \sup\{1 \cdot \beta \mid \beta < \lambda\} = \lambda$.

**2)** $2 + \omega = \sup\{2 + n \mid n < \omega\} = \omega$, но $\omega + 2 = S(S(\omega)) > \omega$. $\omega \cdot 2 = \omega \cdot S(1) = \omega \cdot 1 + \omega = \omega + \omega > \omega$, но $2 \cdot \omega = \sup\{2n \mid n < \omega\} = \omega$.

**3)** Значение $(1 + 1) \cdot \omega$ проще представить, пользуясь вторым определением умножения: вместо каждого натурального числа вставляется пара — это то же самое, что

взять сначала все четные числа, а потом к ним в паре поставить следующие нечетные, итоговый порядковый тип так и останется $\omega$. С другой стороны, сумма $(1 \cdot \omega) + (1 \cdot \omega)$ явно содержит «в середине предельную точку» и никак не может быть равна $\omega$.

**4)** Ассоциативность тоже проще доказывать через второе определение операций.

Сложение: рассматриваем множества $(\alpha \times \{0\} \cup \beta \times \{1\}) \times \{0\} \cup \gamma \times \{1\}$ и $\alpha \times \{0\} \cup (\beta \times \{0\} \cup \gamma \times \{1\}) \times \{1\}$. Между ними существует естественный изоморфизм, сохраняющий порядок: $\langle\langle a, 0\rangle, 0\rangle \mapsto \langle a, 0\rangle$, $\langle\langle b, 1\rangle, 0\rangle \mapsto \langle\langle b, 0\rangle, 1\rangle$, $\langle c, 1\rangle \mapsto \langle\langle c, 1\rangle, 1\rangle$, где $a \in \alpha, b \in \beta, c \in \gamma$.

Проще всего понять это, если оба множества свести к более простому $\alpha \times \{0\} \cup \beta \times \{1\} \cup \gamma \times \{2\}$, в котором сравнение пар сначала осуществляется по второму аргументу $(0 < 1 < 2)$, а затем, если они совпали, — по первому. У такого множества ассоциативность присутствует естественным образом, т.к. она наследуется от ассоциативности операции $\cup$.

Умножение: рассматриваем множества $(\alpha \times \beta) \times \gamma$ и $\alpha \times (\beta \times \gamma)$. Между ними существует естественный изоморфизм, сохраняющий порядок: $\langle\langle a, b\rangle, c\rangle \mapsto \langle a, \langle b, c\rangle\rangle$. Действительно, пусть $\langle\langle a, b\rangle, c\rangle \prec \langle\langle x, y\rangle, z\rangle$, тогда есть два варианта:[12]

1) $c < z$, тогда $\langle b, c\rangle \prec \langle y, z\rangle$, а тогда и $\langle a, \langle b, c\rangle\rangle \prec \langle x, \langle y, z\rangle\rangle$;

2) $c = z$, тогда $\langle a, b\rangle \prec \langle x, y\rangle$, а здесь снова есть два случая:

2.1) $b < y$, тогда $\langle b, c\rangle \prec \langle y, z\rangle$, откуда $\langle a, \langle b, c\rangle\rangle \prec \langle x, \langle y, z\rangle\rangle$;

2.2) $b = y$, тогда $a < x$, откуда $\langle a, \langle b, c\rangle\rangle \prec \langle x, \langle y, z\rangle\rangle$.

**5)** Чтобы показать, что $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$, снова используем второе определение операций: достаточно показать, что $\alpha \times (\beta \sqcup \gamma)$ изоморфно $(\alpha \times \beta) \sqcup (\alpha \times \gamma)$. Это делается по аналогии с предыдущим и почти очевидно, поскольку $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

**6)** Формулу $(\beta < \gamma) \leftrightarrow (\alpha + \beta) < (\alpha + \gamma)$ докажем с помощью второго определения операций, но отчасти с использованием рекурсивного определения $(S(\alpha + \beta) = \alpha + S(\beta))$.

Если $\beta < \gamma$, то $S(\beta) \leqslant \gamma$ и существует естественное строго монотонное вложение $\mathrm{id} : \alpha \sqcup S(\beta) \to \alpha \sqcup \gamma$. Поскольку $ot(\alpha \sqcup S(\beta)) = \alpha + S(\beta)$ и $ot(\alpha \sqcup \gamma) = \alpha + \gamma$, имеется строго монотонное вложение $f : S(\alpha + \beta) \to \alpha + \gamma$, а как мы уже отмечали ранее (см. доказательство леммы о порядковом типе), $f(x) \geqslant x$, следовательно, $f(\alpha + \beta) \geqslant \alpha + \beta$, в то же время $f(\alpha + \beta) < \alpha + \gamma$, откуда получаем, что $\alpha + \beta < \alpha + \gamma$.

Обратно, пусть $\alpha + \beta < \alpha + \gamma$. Допустим, что $\neg(\beta < \gamma)$, тогда $\beta \geqslant \gamma$, тогда по предыдущему $\alpha + \beta \geqslant \alpha + \gamma$. Противоречие.

Попутно мы доказали еще один полезный факт: если имеется монотонное вложение $\alpha$ в $\beta$, то $\alpha \leqslant \beta$, т.е. строго монотонные вложения «несжимаемы».

**7)** Пусть $\alpha > 0$ и $\beta < \gamma$. Докажем формулу $\alpha \cdot \beta < \alpha \cdot \gamma$ индукцией по $\gamma > \beta$, предполагая, что для ординалов меньше $\gamma$ она верна. Разбор случаев для $\gamma$: $\gamma = S(\beta)$ (нет меньших ординалов), $S(\beta) < \gamma \in \mathrm{Succ}$, $\beta < \gamma \in \mathrm{Lim}$.

1) $\gamma = S(\beta)$, тогда $\alpha \cdot \gamma = \alpha \cdot \beta + \alpha > \alpha \cdot \beta$, т.к. $\alpha > 0$.

2) $\gamma = S(\delta)$, где $\delta > \beta$, тогда $\alpha \cdot \gamma = \alpha \cdot \delta + \alpha > \alpha \cdot \beta$, т.к. $\alpha \cdot \delta > \alpha \cdot \beta$ по предположению индукции.

3) $\gamma \in \mathrm{Lim}$, тогда $\alpha \cdot \gamma = \sup\{\alpha \cdot \delta \mid \delta < \gamma\} = \sup\{\alpha \cdot S(\delta) \mid \delta < \gamma\}$, откуда следует, что $\alpha \cdot S(\beta) \leqslant \alpha \cdot \gamma$, а так как $\alpha \cdot S(\beta) = \alpha \cdot \beta + \alpha > \alpha \cdot \beta$ (т.к. $\alpha > 0$), то $\alpha \cdot \beta < \alpha \cdot \gamma$. Индукция завершена.

Обратно, пусть $\alpha \cdot \beta < \alpha \cdot \gamma$. Предполагая, что $\beta \geqslant \gamma$, придем к неравенству $\alpha \cdot \beta \geqslant \alpha \cdot \gamma$ по только что доказанному. Противоречие. Значит, $\beta < \gamma$.

[12] Мы не используем разные обозначения для сравнений на упорядоченных суммах, т.к. это слишком громоздко, различаем только сравнение в ординалах и в множествах.

**8)** Левая нестрогая монотонность доказывается аналогично. Но в доказательстве нельзя будет прибегнуть к помощи $S(\delta)$, чтобы получить строгое неравенство, т.к. у нас нет рекурсивного правила для левой компоненты сложения и умножения. Поэтому мнонотонность оказывается нестрогой.

Более того, можно легко привести пример, когда строгая монотонность нарушается: сравните $1 < 2$, но $1 + \omega = 2 + \omega = \omega$, а также $1 \cdot \omega = 2 \cdot \omega = \omega$.

**9)** Если $\alpha, \beta > 0$, то $\alpha \geqslant 1$ и $\beta \geqslant 1$, откуда по предыдущим свойствам получаем, что $\alpha \cdot \beta \geqslant 1 \cdot 1 = 1 > 0$. Так что если $\alpha \cdot \beta = 0$, то $(\alpha = 0) \vee (\beta = 0)$.

**10)** Пусть $\alpha \geqslant \beta$, тогда положим $\alpha \div \beta = ot(\alpha \setminus \beta)$. Нетрудно видеть, что $\alpha = \beta \sqcup (\alpha \setminus \beta)$ (тут даже не нужно домножать на 0 и 1), так что по второму определению сложения имеем $\alpha = \beta + ot(\alpha \setminus \beta)$, т.е. $\gamma = a \div \beta$ есть искомый ординал. Если бы существовало два ординала, обеспечивающих данное равенство $\gamma_1 < \gamma_2$, то свойству 6 мы бы получили $\beta + \gamma_1 < \beta + \gamma_2$, т.е. $\alpha < \alpha$, что невозможно для ординалов.

**11)** Переходим к теореме о делении с остатком. Пусть $\beta > 0$ и $\alpha$ — произвольный ординал. Положим $\gamma' = \min\{\delta \mid \beta \cdot \delta > \alpha\}$. Это множество не пусто, т.к. $\beta \cdot (\alpha + 1) > \alpha$, так что указанный $\gamma'$ существует. Покажем, что $\gamma' \in \mathrm{Succ}$. Во-первых, заметим, что $\gamma' > 0$. Во-вторых, допустим, что $\gamma' \in \mathrm{Lim}$. Тогда для любого $\delta < \gamma'$ имеем $\beta \cdot \delta' \leqslant \alpha$ и по определению умножения $\beta \cdot \gamma' = \sup\{\beta \cdot \delta \mid \delta < \gamma'\} \leqslant \alpha$, а это противоречит выбору $\gamma'$. Следовательно, $\gamma' = \gamma + 1$ при некотором $\gamma$. Кроме того, в силу выбора $\gamma'$ получаем, что $\alpha \geqslant \beta \cdot \gamma$.

Пусть далее $\delta = \alpha \div (\beta \cdot \gamma)$. Тогда по предыдущему свойству $\alpha = \beta \cdot \gamma + \delta$.

Предположим, что $\alpha = \beta \cdot \gamma_1 + \delta_1 = \beta \cdot \gamma_2 + \delta_2$, где $\delta_1, \delta_2 < \beta$. Пусть $\gamma_1 < \gamma_2$. Тогда $\gamma_1 + 1 \leqslant \gamma_2$, тогда $\alpha \geqslant \beta \cdot \gamma_2 \geqslant \beta \cdot (\gamma_1 + 1) = \beta \cdot \gamma_1 + \beta > \beta \cdot \gamma_1 + \delta_1 = \alpha$. Противоречие. Аналогично, не может быть $\gamma_1 > \gamma_2$, так что $\gamma_1 = \gamma_2$. Отсюда уже по свойству 10 получаем, что и $\delta_1 = \delta_2$, так что пара $\gamma, \delta$ определяется однозначно.

**12)** Перейдем к доказательству свойств степеней ординалов.

$1^\alpha = 1$ доказываем индукцией по $\alpha$: $1^0 = 1$ по определению, далее $1^{S(\alpha)} = 1^\alpha \cdot 1 = 1$ и $1^\lambda = \sup\{1^\gamma \mid \gamma < \lambda\} = 1$, где $\lambda \in \mathrm{Lim}$.

Далее, $\alpha^1 = \alpha^{S(0)} = \alpha^0 \cdot \alpha = 1 \cdot \alpha = \alpha$.

**13)** Тождество $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$ можно доказать, используя теоретико-множественные определения операций на ординалах. Именно, нам требуется доказать, что

$$\langle F^{fin}(\beta \sqcup \gamma, \alpha), \prec \rangle \cong \langle F^{fin}(\beta, \alpha) \times F^{fin}(\gamma, \alpha), \prec \rangle.$$

Слева у нас функции с конечным носителем в $\beta \sqcup \gamma$. Ясно, что каждую такую функцию $f$ можно представить как объединение $f' \cup f''$, где $f' = f \restriction \beta \times \{0\}$, $f'' = f \restriction \gamma \times \{1\}$. Соответствие $f \mapsto \langle f', f'' \rangle$ является взаимно однозначным. Справа у нас функции $g$ и $h$ с конечным носителем из двух ординалов $\beta$ и $\gamma$, которые мы рассматриваем независимо. Из этих функций легко получить наши $f'$ и $f''$ по следующему правилу:

$$f'(x, 0) = g(x), \quad f''(x, 1) = h(x),$$

и это соответствие также взаимно однозначное. Следовательно, между базовыми множествами $F^{fin}(\alpha, \beta \sqcup \gamma)$ и $F^{fin}(\alpha, \beta) \times F^{fin}(\alpha, \gamma)$ у нас есть биекция.

Остается проверить, что это порядковый изоморфизм. Не умаляя общности, мы можем вместо исходных функций $g, h$ рассматривать соответствующие им $f', f''$, т.е. вместо базового множества $F^{fin}(\alpha, \beta) \times F^{fin}(\alpha, \gamma)$ рассмотрим сразу множество $F^{fin}(\alpha, \beta \times \{0\}) \times F^{fin}(\alpha, \gamma \times \{1\})$.

Пусть $f, g \in F^{fin}(\alpha, \beta \sqcup \gamma)$. Пусть также $\delta = \max\{x \mid f(x) \neq g(x)\}$ — «решающая» точка. Для нее существует две возможности: $\delta \in \beta \times \{0\}$ или $\delta \in \gamma \times \{1\}$. Рассмотрим первый кейс, тогда $\delta$ будет решающей точкой для $f'$ и $g'$, причем $(f \prec g) \leftrightarrow (f' \prec g')$, и, кроме того, $f'' = g''$, таким образом, в первом случае $(f \prec g) \leftrightarrow \langle f', f'' \rangle \prec \langle g', g'' \rangle$, где символом $\prec$ мы обозначаем разные упорядочения на соответствующих множествах, определенные по формулам (D4.14) и (D4.16). Во втором случае имеем $f'' \prec g''$, так что в прямом произведении сравнение происходит по второй компоненте, и снова возникает эквиваленция $(f \prec g) \leftrightarrow \langle f', f'' \rangle \prec \langle f'', g'' \rangle$.

Таким образом, указанное соответствие $f \mapsto \langle f', f'' \rangle$ является порядковым изоморфизмом. Отсюда следует, что $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$.

**14)** Докажем теперь монотонность степени: если $\alpha > 1$ и $\beta < \gamma$, то $\alpha^\beta < \alpha^\gamma$. Это свойство легче тоже получить из теоретико-множественного определения степени. Слева в неравенстве у нас стоит базовое множество, состоящее из функций $f : \beta \to \alpha$ с конечным носителем, а справа — из функций $g : \gamma \to \alpha$ с конечным носителем. Отсюда сразу видно, почему требуется $\alpha > 1$: если $\alpha = 1 = \{0\}$, то все функции превращаются в тождественно равные нулю, т.е. базовые множества состоят из единственной точки, и мы получаем $\alpha^\beta = \alpha^\gamma$, а если $\alpha = 0$, то неравенство и вовсе не верно, т.к. $0^0 > 0^1$.

Пусть $\alpha > 1$, т.е. в $\alpha$ есть хотя бы два элемента. Тогда рассмотрим функцию $g : \gamma \to \alpha$, заданную правилом $g(\beta) = 1$ и $g(x) = 0$ при $x \neq \beta$. Такая функция окажется строго больше, чем любая функция $f$ (чтобы их корректно сравнивать, нужно все $f$ продлить нулями на $\gamma$). Таким образом, в порядке, заданном на $F^{fin}(\alpha, \gamma)$ найдется хотя бы одна точка больше всех точек из $F^{fin}(\alpha, \beta)$. Отсюда следует, что $\alpha^\beta < \alpha^\gamma$.

**15)** Тождество $\alpha^{\beta\cdot\gamma} = (\alpha^\beta)^\gamma$ для разнообразия докажем индукцией по $\gamma$.

База: $\alpha^{\beta\cdot 0} = \alpha^0 = 1$ и $(\alpha^\beta)^0 = 1$.

Шаг индукции для последователя: $\alpha^{\beta\cdot(\gamma+1)} = \alpha^{\beta\cdot\gamma+\beta} = \alpha^{\beta\cdot\gamma}\cdot\alpha^\beta = (\alpha^\beta)^\gamma\cdot(\alpha^\beta)^1 = (\alpha^\beta)^{\gamma+1}$, где мы воспользовались предыдущим свойством.

Шаг индукции для предельного ординала: сначала заметим, что если $\lambda \in \mathrm{Lim}$, то $\beta \cdot \lambda \in \mathrm{Lim}$, если $\beta > 0$. Поэтому сначала проверим тождество при $\beta = 0$: $\alpha^{0\cdot\lambda} = \alpha^0 = 1$ и $(\alpha^0)^\gamma = 1^\gamma = 1$.

Далее пусть $\beta > 0$. Так как $\beta \cdot \lambda \in \mathrm{Lim}$, то $\alpha^{\beta\cdot\lambda} = \sup\{\alpha^\delta \mid \delta < \beta \cdot \lambda\}$, а для каждого $\delta < \beta \cdot \lambda$ можно найти $\xi < \lambda$ такой, что $\delta < \beta \cdot \xi$. Как это сделать? Поделим $\delta$ с остатком на $\beta$, тогда $\delta = \beta \cdot \sigma + \rho$, где $\rho < \beta$, а также $\sigma < \lambda$ (иначе бы получилось $\delta \geqslant \beta \cdot \lambda$), тогда $\sigma + 1 < \lambda$ (в силу предельности $\lambda$), откуда $\beta \cdot (\sigma + 1) > \delta$ и $\beta \cdot (\sigma + 1) < \beta \cdot \lambda$, так что искомый $\xi = \sigma + 1$.

В силу монотонности степени получаем, что:

$$\sup\{\alpha^\delta \mid \delta < \beta \cdot \lambda\} = \sup\{\alpha^{\beta\cdot\xi} \mid \xi < \lambda\},$$

т.к., с одной стороны, каждый $\delta < \beta \cdot \lambda$ можно оценить сверху $\beta \cdot \xi < \beta \cdot \lambda$, где $\xi < \lambda$, а с другой стороны, каждый $\beta \cdot \xi$ можно оценить сверху некоторым $\delta < \beta \cdot \lambda$ (например, полагая $\delta = \beta \cdot \xi$).[13]

Пользуясь предположением индукции, заменяем $\alpha^{\beta\cdot\xi}$ на $(\alpha^\beta)^\xi$, откуда получаем, что

$$\alpha^{\beta\cdot\lambda} = \sup\{(\alpha^\beta)^\xi \mid \xi < \lambda\} = (\alpha^\beta)^\lambda,$$

что и требовалось. □

[13] В этом случае говорят, что множество $\{\beta \cdot \xi \mid \xi < \lambda\}$ конфинально ординалу $\beta \cdot \lambda$.

Итак, класс всех ординалов Ord ведет себя в теории ZF в некотором смысле так же, как $\omega$ ведет себя в HF, где аксиома бесконечности ложна: это вполне упорядоченная шкала, задающая своего рода бесконечность в соответствующем универсуме множеств. Эта шкала, кроме того, имеет свою арифметику с неплохими свойствами вроде деления с остатком (эвклидовость) и отсутствием делителей нуля. Но есть и отличие от натуральных чисел: операции сложения и умножения некоммутативны в бесконечной области, а также есть много равномощных ординалов. Например, $\omega + \omega \simeq \omega$.

Ситуацию можно попытаться подправить, если среди ординалов выделить спецпредставителей, отвечающих за уникальность мощности. Так появляется определение кардинальных чисел.

### D4.3.4 Арифметика кардиналов

В отличие от ординалов, которые служат эталонами для всех вполне упорядоченных множеств, кардиналы призваны измерять «размер» или «мощность» произвольных множеств.

Ординал, неравномощный никакому своему элементу, называется **кардиналом** (или *кардинальным числом*).

Эквивалентное определение: кардинал — это начальный ординал, то есть ординал, являющийся наименьшим среди всех ординалов данной мощности. Иначе говоря, кардинал реализует самый «сжатый» порядок на множестве.

Ранее мы вводили понятие кардинальности для произвольного множества, как класса равномощных множеств. Проблема с этими классами заключается в том, что, во-первых, это не объекты теории ZF, а ее формулы, и, соответственно, мы не можем формализовать такие высказывания как «для любой мощности», «существует мощность», поскольку это означало бы квантование по формулам, а во-вторых, без аксиомы выбора их нельзя линейно упорядочить, т.е. не любые два класса кардинальностей можно сравнить.

Вводя кардиналы как подкласс шкалы ординалов, мы сразу же решаем эти две проблемы автоматически. Кардиналы — это легальные множества ZF, по ним можно квантовать (навешивать квантор) и любые два кардинала можно сравнить. Расплатой за это приобретение является то, что не для всякого множества можно доказать наличие равномощного кардинала, опять же, в отсутствие аксиомы выбора. При добавлении аксиомы выбора в теорию кардиналы становятся универсальными измерителями мощностей множеств.

Если какое-то множество $X$ равномощно некоторому кардиналу $\tau$, то говорят, что $\tau$ есть **мощность множества** $X$, что обозначается: $|X| = \tau$. В частности, все натуральные числа и ординал $\omega$ являются кардинальными числами.

Поскольку любое вполне упорядоченное множество имеет единственный порядковый тип, оно также имеет и мощность. Действительно, если $ot(X) = \alpha$, то мощностью $X$ будет кардинал $\tau = \min\{\beta \mid (\beta \leqslant \alpha) \wedge (\beta \simeq \alpha)\}$.

Говоря об арифметике кардинальных чисел, обычно подразумевают бесконечные кардиналы, поскольку в конечной области она совпадает с обычной арифметикой, а взаимодействие конечных кардинальных чисел с бесконечными, в отличие от шкалы ординалов, богатством свойств не отличается.

Операции задаются следующим образом, как правило, сразу для произвольных множеств. Пусть $|A| = \tau$ и $|B| = \chi$, тогда *суммой кардиналов* $\tau + \chi$ называется мощность

$|A \sqcup B|$, *произведением кардиналов* $\tau \cdot \chi$ называется мощность $|A \times B|$, степенью кардиналов $\tau^\chi$ называется мощность $|A^B|$, если таковая существует.[14]

**Замечание**: операции на ординалах и кардиналах обозначаются одинаково, а учитывая, что кардиналы являются ординалами, легко перепутать, какая операция к ним применяется, особенно если это не очевидно из обозначения. Поэтому нужно всегда следить по контексту, какие операции используются. В том случае, когда к кардиналам требуется применить именно ординальные операции, вводятся различные обозначения для этих операций, например, $+^o$ v.s. $+^c$. Это тонкий вопрос конвенций, имеющий прямое отношение к математическому языку. Попытка сделать язык удобнее для восприятия неминуемо приводит к тому, что каждый конкретный текст имеет некие семантические условности и предопределенные конвенции.

Если $\tau$ — кардинал, то через $\tau^+$ обозначается минимальный кардинал, больший, чем $\tau$. Кардинал $\tau^+$ называется *последователем*. Если кардинал не является последователем и не равен нулю, то он называется (*слабо*) *предельным кардиналом*. Здесь начинаются первые проблемы с кардиналами. В ZF невозможно доказать, что $\tau^+$ существует для любого $\tau$, т.к. мы не можем гарантировать существование вполне упорядочения множества $\mathscr{P}(\tau)$. Это значит, что мы не можем доказать, что кардиналы образуют собственно класс, а также не можем доказать, что они образуют множество. Эти утверждения являются независимыми от ZF. При добавлении аксиомы выбора при помощи теоремы Цермело мы уже можем гарантировать вполне упорядочение у любого множества, а значит, гарантировать наличие мощности у этого множества, а также наличие сколь угодно большой мощности. Так что в теории ZFC кардиналы образуют собственно класс.

Кардиналы обычно обозначаются греческими буквами из конца алфавита, а также с помощью специальной нумерации «алефов».

**Теорема D4.9.** *Пусть $\mathscr{K}$ — собственно класс, вполне упорядоченный некоторым отношением-классом. Тогда существует единственное отображение-класс $F : \mathrm{Ord} \leftrightarrow \mathscr{K}$, являющееся порядковым изоморфизмом.*

Эта теорема является обобщением леммы о порядковом типе на случай собственных классов, и ее доказательство принципиально ничем не отличается.

В частности, мы можем занумеровать бесконечные кардиналы, используя эту теорему, следующим образом: $\aleph_0 = \omega$, $\aleph_{\alpha+1} = \aleph_\alpha^+$, $\aleph_\lambda = \sup\{\aleph_\alpha \mid \alpha < \lambda\}$, где $\lambda \in \mathrm{Lim}$.

Отсюда мы видим, что предельные кардиналы имеют номера, являющиеся предельными одиналами, а последовательные кардиналы имеют номера, являющиеся последовательными ординалами. И только предельный кардинал $\omega$ имеет номер 0.

Имея нумерацию класса (или даже множества) ординалами, мы можем запускать индукцию по этому классу. Например, мы можем доказывать какое-то свойство $\varphi(\tau)$ только для кардиналов $\tau$, проверяя индуктивный переход, как обычно, для трех типов ординальных индексов: 0, Succ и Lim. В случае с алефами это значит, что мы будем рассматривать индуктивный переход в трех случаях: когда $\tau = \omega$, когда $\tau = \chi^+$ и когда $\tau$ является предельным кардиналом.

В отличие от ординальной, арифметика для бесконечных кардиналов оказывается гораздо проще, что и делает ее удобной для измерения «размеров» множеств.

[14] Вполне упорядочение $A \sqcup B$ и $A \times B$ определяется в ZF по оформулам (D4.12) и (D4.14). Это гарантирует существование мощностей суммы и произведения кардиналов. Ситуация для степени принципиально иная, поскольку для степени кардиналов используется множество *всех* функций из $B$ в $A$, в то время как для степени ординалов — только функций с конечным носителем. А вполне упорядчоение $A^B$ в общем случае в ZF построить невозможно, требуется более сильная система аксиом.

**Теорема D4.10.** *Алгебраические свойства кардиналов:*

1° $\kappa + 0 = \kappa$; $\kappa \cdot 1 = \kappa$; $\kappa \cdot 0 = 0$;

2° *сложение и умножение кардиналов ассоциативны, коммутативны, дистрибутивны;*

3° *нет делителей нуля;*

4° *сложение и умножение нестрого монотонны;*

5° $\tau^0 = 1$, *в частности,* $0^0 = 1$; $0^\tau = 0$, *если* $\tau > 0$;

6° $1^\tau = 1$;

7° $\tau^{\kappa+\chi} = \tau^\kappa \cdot \tau^\chi$; $(\tau^{\kappa\cdot\chi}) = (\tau^\kappa)^\chi$; $(\tau \cdot \kappa)^\chi = \tau^\chi \cdot \kappa^\chi$;

8° *экспонента монотонна по обоим аргументам;*

9° $\kappa^2 = \kappa$, *если* $\kappa \geqslant \omega$ *(Теорема Гессенберга);*

10° *если* $\max\{\tau, \chi\} \geqslant \omega$ *и* $\tau, \chi > 0$, *то* $\tau + \chi = \tau \cdot \chi = \max\{\tau, \chi\}$;

11° $|\mathscr{P}(X)| = 2^{|X|}$ *(если существует);*

12° $\tau < 2^\tau$ *(Теорема Кантора).*

*Доказательство.* Большинство свойств (1-8, 11-12) являются прямыми следствиями определений операций над мощностями через дизъюнктное объединение, декартово произведение и множество отображений. Их доказательства сводятся к построению соответствующих биекций и аналогичны доказательствам для конечных множеств.

Ключевые свойства (9, 10), специфичные для бесконечных кардиналов, требуют более детального рассмотрения. Центральным результатом здесь является **теорема Гессенберга**, утверждающая, что $\kappa^2 = \kappa$ для любого бесконечного кардинала $\kappa$.

*Доказательство теоремы Гессенберга.* Утверждение эквивалентно тому, что для любого ординала $\alpha$ справедливо $\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$. Доказательство ведётся трансфинитной индукцией по $\alpha$. База индукции ($\alpha = 0$) — это равенство $\aleph_0 \cdot \aleph_0 = \aleph_0$, которое следует из существования биекции между $\omega \times \omega$ и $\omega$.

Для индуктивного перехода предположим, что для всех $\beta < \alpha$ верно $\aleph_\beta \cdot \aleph_\beta = \aleph_\beta$. Докажем, что $\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$. Для этого введем на множестве $\aleph_\alpha \times \aleph_\alpha$ отношение вполне упорядочения $\prec$ по правилу:

$$\langle \xi_1, \eta_1 \rangle \prec \langle \xi_2, \eta_2 \rangle \overset{\text{def}}{\leftrightarrow} \begin{cases} \max\{\xi_1, \eta_1\} < \max\{\xi_2, \eta_2\}, & \text{или} \\ \max\{\xi_1, \eta_1\} = \max\{\xi_2, \eta_2\} \text{ и } \xi_1 < \xi_2, & \text{или} \\ \max\{\xi_1, \eta_1\} = \max\{\xi_2, \eta_2\}, \xi_1 = \xi_2 \text{ и } \eta_1 < \eta_2. \end{cases}$$

Это упорядочение «фреймами» можно представлять себе на примере множества $\omega \times \omega$, где, в отличие от канторовской диагональной нумерации, происходит нумерация по верхней и правой кромке квадратов $n \times n$. Легко проверить, что это действительно вполне упорядочение. Антирефлексивность очевидна, поскольку в определении используются строгие неравенства, транзитивность наследуется из исходного порядка внутри $\aleph_\beta$, связность следует из того, что если две точки лежат на разных «фреймах», то они

сравниваются по номеру этого «фрейма», который равен $\max\{\xi,\eta\}$, а если они принадлежат одному «фрейму», то включается сравнение по координатам внутри $\aleph_\beta$. Минимум непустого подмножества $A$ также нетрудно найти: сначала ищутся точки $\langle\xi,\eta\rangle$ с минимальным значением $\max\{\xi,\eta\}$, затем среди них — с минимальным значением $\xi$, наконец, среди оставшихся — с минимальным значением $\eta$.

Пусть $\delta = ot(\aleph_\alpha \times \aleph_\alpha, \prec)$. Тогда $|\aleph_\alpha \times \aleph_\alpha| = |\delta|$. Докажем, что $|\delta| = \aleph_\alpha$. Оценка $|\delta| \geqslant \aleph_\alpha$ очевидна. Для обратной оценки $|\delta| \leqslant \aleph_\alpha$ рассмотрим произвольную пару $\langle\xi,\eta\rangle \in \aleph_\alpha \times \aleph_\alpha$ и множество ее предшественников $P(\xi,\eta)$.

Пусть $\mu = \max\{\xi,\eta\}$. Так как $\xi,\eta < \aleph_\alpha$, то и $\mu < \aleph_\alpha$. Из определения $\prec$ следует, что $P(\xi,\eta) \subseteq (\mu+1)\times(\mu+1)$. Следовательно, $|P(\xi,\eta)| \leqslant |\mu+1|^2$. Поскольку $\mu+1 < \aleph_\alpha$, то $|\mu+1| = \aleph_\beta$ для некоторого $\beta < \alpha$. По индукционному предположению, $|\mu+1|^2 = \aleph_\beta \cdot \aleph_\beta = \aleph_\beta < \aleph_\alpha$. Таким образом, каждый начальный отрезок множества $(\aleph_\alpha \times \aleph_\alpha, \prec)$ имеет мощность меньше $\aleph_\alpha$. Это означает, что его порядковый тип $\delta$ не может превышать $\aleph_\alpha$, т.е. $\delta \leqslant \aleph_\alpha$. Из двух оценок следует $|\delta| = \aleph_\alpha$, откуда $\aleph_\alpha^2 = \aleph_\alpha$, что и доказывает теорему Гессенберга.

*Следствие.* Теперь свойство 10 выводится немедленно. Пусть $\kappa \geqslant \chi$ и $\kappa \geqslant \omega$, а также $\chi > 0$ (это условие нужно для умножения). Тогда имеют место неравенства:

$$\kappa \leqslant \kappa + \chi \leqslant \kappa + \kappa = 2\cdot\kappa \leqslant \kappa\cdot\kappa = \kappa^2 = \kappa,$$

$$\kappa \leqslant \kappa\cdot\chi \leqslant \kappa\cdot\kappa = \kappa^2 = \kappa.$$

Откуда по теореме Кантора-Бернштейна-Шрёдера следует, что $\kappa + \chi = \kappa\cdot\chi = \kappa = \max\{\kappa,\chi\}$.

Из теоремы Гессенберга индукцией по $n \in \omega$ легко выводится более общее тождество: $\kappa^n = \kappa$, где $\kappa \geqslant \omega$ и $n > 0$. □

## D4.4. Аксиома выбора

Напомним формулировку (общей) аксиомы выбора:

$$\text{(AC)} \qquad (\varnothing \notin A) \to \exists f : A \to \bigcup A :\ (\forall x \in A : f(x) \in x),$$

а также ее счетного варианта:

$$\text{(AC}_\omega\text{)} \qquad (|A| = \omega) \wedge (\varnothing \notin A) \to \exists f : A \to \bigcup A :\ (\forall x \in A : f(x) \in x).$$

Существуют и другие формы аксиомы выбора. Во-первых, стоит упомянуть эквивалентную формулировку в форме (C1.1) для индексированных семейств множеств.

Во-вторых, можно накладывать ограничения на мощность не только самого множества $A$, но и на мощность его элементов. Так, например, аксиома выбора $\text{AC}_\omega^{fin}$ говорит о том, что для счетного семейства *конечных* множеств существует функция выбора. Обобщением является рассмотрение аксиомы выбора $\text{AC}_\kappa^\lambda$, которая утверждает, что для любого семейства мощности $\kappa$ множеств мощности меньше $\lambda$ существует функция выбора, где $\kappa,\lambda$ — бесконечные кардиналы.

### D4.4.1 Счетный выбор и его следствия

Посмотрим, как с помощью $\mathrm{AC}_\omega$ можно уравнять два определения конечных и бесконечных множеств (классическое и по Дедекинду), возвращаясь к дискуссии в конце раздела D4.2.2.

**Теорема D4.11.** *Из $\mathrm{AC}_\omega$ следует, что каждое бесконечное множество является бесконечным по Дедекинду.*

*Доказательство.* Пусть $A$ — бесконечное множество, т.е. оно неравномощно никакому $n \in \omega$. Докажем по индукции, что для любого $n \in \omega$ в $A$ найдется подмножество мощности $n$.

База: $n = 0$. Такое подмножество есть, $\varnothing \subseteq A$.

Пусть для $n$ существует подмножество $B \subseteq A$ такое, что $|B| = n$. Очевидно, что $A \setminus B \neq \varnothing$, т.к. в противном случае было бы $A = B$, т.е. $A$ оказалось бы конечным. Тогда существует $x \in A \setminus B$ и, следовательно, существует множество $B' = B \cup \{x\}$. Легко видеть, что $|B'| = n + 1$. Индукция завершена.

Теперь рассмотрим множества

$$S_n = \{B \in \mathscr{P}(A) \mid |B| = n\}, \quad n \in \omega.$$

Множество $S_n$ можно понимать как «слой» в булеане $\mathscr{P}(A)$, состоящий из конечных равномощных множеств. Каждое $S_n$ не пусто по доказанному.

Тогда $\{S_n\}$ — это проиндексированное множеством $\omega$ множество непустых множеств. Используя $\mathrm{AC}_\omega$, возьмем функцию выбора $f : \omega \to \mathscr{P}(A)$ такую, что $f(n) \in S_n$. Мы получим последовательность подмножеств $B_n = f(n)$, имеющих мощность $n$.

Полученная последовательность множеств еще не позволяет выбрать счетную последовательность элементов $A$, поскольку может случиться, что $B_n$ содержится в объединении всех предыдущих, что не позволяет выбрать новую точку. Поэтому из полученной последовательности мы сконструируем новую, дизъюнктную последовательность.

Положим $C_n \overset{\text{def}}{\leftrightarrow} B_{2^n}$. Таким образом, мы имеем последовательность множеств $C_0, C_1, C_2, \ldots$, где $|C_n| = 2^n$.

Теперь определим новую последовательность попарно непересекающихся множеств $D_n$ следующим образом:

$$D_0 = C_0; \quad D_{n+1} = C_{n+1} \setminus \bigcup_{k=0}^{n} C_k$$

Покажем, что все множества $D_n$ непусты. Для $D_0$ это очевидно, так как $|D_0| = |C_0| = 2^0 = 1$. Для $D_{n+1}$ оценим мощность объединения $\left|\bigcup_{k=0}^{n} C_k\right|$.

$$\left|\bigcup_{k=0}^{n} C_k\right| \leqslant \sum_{k=0}^{n} |C_k| = \sum_{k=0}^{n} 2^k = 2^{n+1} - 1.$$

Поскольку $|C_{n+1}| = 2^{n+1}$, мощность $|C_{n+1} \setminus \bigcup_{k=0}^{n} C_k|$ будет не менее 1.

Таким образом, все множества $D_n$ непусты. По построению они также попарно не пересекаются. Теперь мы имеем счетное семейство непустых, попарно непересекающихся множеств $\{D_n\}_{n\in\omega}$. По аксиоме счетного выбора ($\mathrm{AC}_\omega$) существует функция выбора $g$

для этого семейства, которая из каждого множества $D_n$ выбирает ровно один элемент. Положим $a_n = g(D_n)$. Так как все $D_n$ не пересекаются, все элементы $a_n$ попарно различны.

Таким образом, мы доказали, что произвольное бесконечное множество $A$ содержит счетное подмножество $S = \{a_0, a_1, a_2, \ldots\}$.

Теперь докажем, что $A$ бесконечно по Дедекинду. Для этого достаточно показать, что оно равномощно своему собственному подмножеству. Рассмотрим $A' = A \setminus \{a_0\}$, которое очевидно является собственным подмножеством $A$. Определим биекцию $h : A \to A'$ следующим образом:

$$h(x) = \begin{cases} x, & x \in A \setminus S, \\ a_{n+1}, & x = a_n \in S. \end{cases}$$

Эта функция отображает каждый элемент, не входящий в нашу последовательность $S$, в самого себя, а каждый элемент $a_n$ из последовательности — в следующий за ним элемент $a_{n+1}$. Очевидно, что $h : A \leftrightarrow A'$ (является биекцией), что по определению означает, что $A$ является бесконечным по Дедекинду. □

Из этой теоремы немедленно следует, что всякое конечное по Дедекинду множество является конечным (при принятии $\mathrm{AC}_\omega$).

**Следствие D4.4.** *В* $\mathrm{ZF} + \mathrm{AC}_\omega$ *доказуемо, что множество конечно тогда и только тогда, когда оно конечно по Дедекинду (эквивалентно: множество бесконечно тогда и только тогда, когда оно бесконечно по Дедекинду).*

В терминах сравнения кардинальностей это утверждение можно переписать и так: Из $\mathrm{AC}_\omega$ следует, что множество $A$ бесконечно тогда и только тогда, когда $\omega \preccurlyeq A$ (т.е. существует инъекция из $\omega$ в $A$).

**Лемма D4.9** (Эквивалентные определения счетности)**.** *Для непустого множества $A$ следующие утверждения равносильны в* ZF*:*

**(1)** *$A$ не более чем счетно (т.е. конечно или равномощно $\omega$).*

**(2)** *Существует сюръекция $g : \omega \to A$.*

**(3)** *Существует инъекция $f : A \to \omega$.*

*Доказательство.* Докажем эквивалентность по циклу (1) → (2) → (3) → (1).

**(1 → 2):** Пусть $A$ не более чем счетно. Если $A$ конечно, $|A| = n$, то существует биекция $h : n \to A$. Мы можем определить сюръекцию $g : \omega \to A$ так:

$$g(k) = \begin{cases} h(k), & k < n \\ h(0), & k \geqslant n, \end{cases}$$

где мы пользуемся условием $A \neq \varnothing$ (иначе $h(0)$ не существовало бы).

Если $A$ счетно, то существует биекция $h : \omega \to A$, которая по определению является и сюръекцией.

**(2 → 3):** Пусть существует сюръекция $g : \omega \to A$. Нам нужно построить инъекцию $f : A \to \omega$. Для любого элемента $a \in A$, его прообраз $g^{-1}[\{a\}] = \{k \in \omega \mid g(k) = a\}$ является непустым подмножеством $\omega$. Поскольку $\omega$ является вполне упорядоченным множеством (Теорема D4.4), любое его непустое подмножество имеет единственный

минимальный элемент. Это позволяет нам сделать канонический выбор без привлечения аксиомы выбора. Определим функцию $f : A \to \omega$ по правилу:

$$f(a) = \min(g^{-1}[\{a\}]).$$

Покажем, что $f$ является инъекцией. Пусть $f(a_1) = f(a_2)$. Это означает, что $\min(g^{-1}[\{a_1\}]) = \min(g^{-1}[\{a_2\}])$. Обозначим это минимальное число как $k_0$. По определению функции $f$, это означает, что $k_0 \in g^{-1}(\{a_1\})$ и $k_0 \in g^{-1}(\{a_2\})$. Тогда по определению прообраза $g(k_0) = a_1$ и $g(k_0) = a_2$. Следовательно, $a_1 = a_2$. Инъективность доказана.

**(3 → 1):** Пусть существует инъекция $f : A \to \omega$. Тогда $A$ равномощно своему образу $f[A]$, который является подмножеством $\omega$. В ZF доказуемо, что любое подмножество $\omega$ либо конечно, либо равномощно $\omega$ (по лемме о порядковом типе D4.7). Поскольку $A \simeq f[A]$, то $A$ также либо конечно, либо равномощно $\omega$. То есть, $A$ не более чем счетно. □

**Теорема D4.12.** *В* ZF + $\mathrm{AC}_\omega$ *доказуемо: объединение не более чем счетного семейства не более чем счетных множеств является не более чем счетным множеством.*

*Доказательство.* Пусть $\{A_n\}$ — не более чем счетное семейство не более чем счетных множеств. Если все $A_n$ пусты, то их объединение также пусто и потому не более чем счетно. Предположим, что среди $A_n$ есть непустые множества, тогда вместо $\{A_n\}$ рассмотрим подпоследовательность, в которой оставим все $A_n$, кроме пустых. Результат объединения при этом не изменится. Поэтому можно сразу считать, что все $A_n$ непусты. Наконец, если семейство $\{A_n\}$ конечно, то мы можем сделать его счетным, продолжив последовательность, например, множеством $A_0$. Таким образом, мы можем сразу предполагать, что $\{A_n\}$ есть счетная последовательность непустых не более чем счетных множеств. Пусть $A = \bigcup_{n<\omega} A_n$. Необходимо доказать, что существует сюръекция из $\omega$ на $A$.

Для каждого $n$ существует сюръекция $f_n : \omega \to A_n$, т.к. $A_n \neq \varnothing$ и не более чем счетно. Значит, для каждого $n$ множество всех сюръекций из $\omega$ в $A$ непусто. По $\mathrm{AC}_\omega$ мы можем выбрать по одной такой сюръекции для каждого $n$, получив последовательность $\langle f_n \mid n \in \omega\rangle$. Определим отображение $h : \omega \times \omega \to A$ по правилу $h(n,k) = f_n(k)$. Это отображение является сюръекцией из $\omega \times \omega$ на $A$. Поскольку существует биекция $p : \omega \leftrightarrow \omega \times \omega$ (канторовская нумерация), то композиция $h \circ p : \omega \to A$ является сюръекцией. По лемме D4.9, если существует сюръекция из $\omega$ на множество, то это множество не более чем счетно. □

**Замечание**: обратное к теореме утверждение — что из принципа счетного объединения следует полная аксиома $\mathrm{AC}_\omega$ — неверно, так как этот принцип объединения является строго более слабым. Оказывается, он эквивалентен более слабой форме аксиомы выбора: аксиоме счетного выбора для семейств счетных множеств. Сам принцип объединения также часто формулируют именно для семейств счетных множеств, поскольку в ZF эта версия эквивалентна той, что использована в теореме (для не более чем счетных множеств).

## D4.4.2 Аксиома выбора и ее эквиваленты

**Теорема D4.13** (эквиваленты аксиомы выбора)**.** *Следующие утверждения эквивалентны в теории* ZF*:*

(1) *аксиома выбора* AC*;*

(2) *теорема Цермело* ZT*: любое множество можно вполне упорядочить;*

(3) *лемма Цорна* ZL*: если в частично упорядоченном множестве любая цепь ограничена сверху, то в нем существует максимальный элемент;*

(4) *принцип максимума Хаусдорфа* HMP*: в любом частично упорядоченном множестве существует максимальная по вложению цепь;*

(5) *теорема о квадрате: любое бесконечное множество равномощно своему квадрату.*

*Доказательство.* **1)**. Покажем что из AC следует теорема Цермело. Пусть $X$ — непустое множество. Положим $f(0) = x \in X$, где 0 — наименьший ординал. Дальнейшая нумерация элементов $X$ строится следующим образом: выбрасываем из $X$ все ранее пронумерованные элементы, и в оставшемся множестве, если оно не пустое, снова выбираем один элемент и нумеруем его наименьшим из неиспользованных ординалов.

Точнее, пусть $c : \mathscr{P}(X) \to X$ есть функция выбора, и $c(\varnothing) = X$. Тогда построим трансфинитной рекурсей функцию

$$f(\alpha) = c(X \setminus \{f(\beta) \mid \beta < \alpha\}).$$

Нетрудно показать, что до некоторого ординала $\gamma$ эта функция является инъекцией, а на ординале $\gamma$ — биекцией в множество $X$. На следующих точках ординальной шкалы $f$ принимает значение $X$. Таким образом, $\gamma$ индуцирует вполне упорядочение на $X$.

**2)**. Покажем, что из теоремы Цермело следует лемма Цорна. Пусть $\langle X, < \rangle$ — непустое ч.у.м., в котором каждая цепь ограничена. Под **цепью** понимается подмножество $Y \subseteq X$, такое, что $\langle Y, < \rangle$ — л.у.м.

Введем на $X$ вполне упорядочение $\prec$ в соответствии с теоремой Цермело. Построим в $X$ цепь рекурсивно, выбирая на каждом шаге несобственную верхнюю грань уже построенного участка цепи с помощью порядка $\prec$.

$$f(\alpha) = \min_{\prec}\{a \in X \mid \forall \beta < \alpha : \ f(\beta) < a\},$$

если это множество непустое, и $f(\alpha) = X$ в противном случае. Так, $f(0) = \min\limits_{\prec} X$. Нетрудно показать, что до некоторого ординала $\gamma$ эта функция является инъекцией, а на ординале $\gamma$ — биекцией в некоторую цепь $C \subseteq X$. На следующих точках ординальной шкалы $f$ принимает значение $X$. Таким образом, в $X$ выстраивается цепь $C$, у которой нет несобственной верхней грани (такая цепь называется сквозной). А поскольку в $X$ все цепи ограничены, то существует $\max\limits_{\prec} C$, который и является максимальным элементом $X$.

**3)**. Покажем, что из леммы Цорна следует принцип максимума Хаусдорфа. Пусть $\langle X, < \rangle$ — непустое ч.у.м. Очевидно, в нем есть хотя бы одно одноточечное л.у.м. Тогда множество всех линейно упорядоченных подмножеств $X$ непусто. Обозначим его $L(X)$ и рассмотрим его как ч.у.м. с отношением вложения $\subseteq$.

Пусть $C$ — какая-нибудь цепь в $L(X)$. **Пределом** цепи (в случае отношения порядка $\subseteq$) называется $\bigcup C$. Легко проверить, что $\bigcup C$ также является линейно упорядоченным (по $<$) подмножеством $X$, т. е. $\bigcup C \in L(X)$. Кроме того, $\bigcup C$ ограничивает сверху цепь $C$.

Таким образом, в $L(X)$ любая цепь ограничена, а значит, по лемме Цорна, существует максимальный элемент $L \in L(X)$. А это и есть максимальное по вложению линейно упорядоченное подмножество $X$.

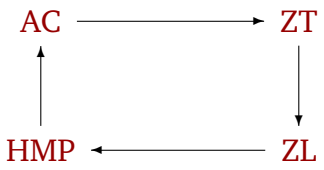
**4)**. Покажем, что из принципа максимума Хаусдорфа следует аксиома выбора. Пусть $X$ — непустое множество такое, что $\varnothing \notin X$. Пусть $y \in X$, тогда на множестве $\{y\} \subseteq X$ существует функция выбора $f_{\{y\}}$, которая ставит в соответствие точке $y$ какой-то его элемент.[15]

Таким образом, мы можем рассмотреть множество всех функций выбора, определенных на подмножествах $X$, и оно заведомо будет непустым. Обозначим его $F(X)$ и рассмотрим его как ч.у.м. с отношением вложения $\subseteq$. Вложение функций означает, что одна (бóльшая) продолжает вторую, а на пересечении их областей определения они совпадают.

Тогда из принципа максимума Хаусдорфа следует, что в $F(X)$ существует максимальное по вложению л.у.м. (линейный порядок тот же — вложение функций), которое мы обозначим $\mathscr{F}$. В этом множестве функций выбора каждая функция содержит в себе все меньшие ее, а значит, нетрудно показать, что предел цепи $\mathscr{F}$, который мы обозначим $f = \bigcup \mathscr{F}$, является а) функцией, б) функцией выбора на подмножестве $X$ и в) функцией выбора на всем $X$.

Последнее следует из того, что если бы $f$ не была определена в какой-то точке $X$, то можно было бы доопределить ее до более широкой (хотя бы на одну точку шире) функции выбора, а это противоречит максимальности $\mathscr{F}$.

Итак, мы показали следующие импликации:




Отсюда нетрудно понять, что первые четыре утверждения эквивалентны.

**5)** Эквивалентность AC и теоремы о квадрате.

**(2) → (5):** В силу теоремы Цермело мы можем вполне упорядочить любое множество $X$ и, тем самым, от множеств перейти к кардиналам, а для кардиналов у нас есть теорема Гессенберга (теорема D4.10).

**(5) → (2):** Пусть $X^2 \simeq X$ для любого бесконечного множества $X$. Наша цель — доказать теорему Цермело, т.е. что любое множество может быть вполне упорядочено. Ясно, что можно вести речь только о бесконечных множествах, т.к. конечные множества равномощны натуральным числам фон Неймана, которые вполне упорядочены.

Для удобства введем новый квантор $\forall^{inf}$, который означает квантование только по бесконечным множествам (его легализация в языке ZF аналогична легализации кванторов по ординалам).

**Лемма D4.10.** *Если* $\forall^{inf} x\ (x \times x) \simeq x$, *то* $\forall^{inf} x, y\ (x \times y) \simeq (x \sqcup y)$.

*Доказательство.* Для начала заметим, что из теоремы о квадрате следует и теорема об

[15] Заметим, что существование функции выбора для конечных множеств выводится из аксиом ZF, поскольку мы можем конечное число раз записать квантор существования для элемента непустого множества и, тем самым, явно вывести существование конечной функции выбора. Для бесконечных множеств конечной формулой, увы, не отделаешься.

удвоении: $\forall^{inf} x\ (x \sqcup x \simeq x)$, поскольку[16]

$$x \preccurlyeq (x \sqcup x) \preccurlyeq (x \times x) \simeq x,$$

откуда по теореме Кантора-Бернштейна-Шрёдера получаем равенство $x \simeq x \sqcup x$. Используя теорему о квадрате и теорему об удвоении, находим, что

$$(x \sqcup y) \simeq ((x \sqcup y) \times (x \sqcup y)) \simeq ((x \times x) \sqcup (x \times y) \sqcup (x \times y) \sqcup (y \times y)) \simeq (x \sqcup y \sqcup (x \times y)),$$

следовательно, $x \times y \preccurlyeq x \sqcup y$. Обратное вложение для бесконечных множеств очевидно: $x$ биективно отождествляется с $x \times \{y_0\}$, а $y$ биективно отождествляется с $(\{x_0\} \times (y \setminus \{y_0\})) \cup \{\langle x_1, y_1\rangle\}$, где $x_0 \neq x_1$ и $y_0 \neq y_1$ — произвольные точки множеств $x$ и $y$, соответственно (их можно найти в виду бесконечности обоих множеств).

Отсюда по теореме Кантора-Бернштейна-Шрёдера получаем $x \times y \simeq x \sqcup y$, что, кстати, соответствует пункту 10 теоремы D4.10. □

**Лемма D4.11.** *Если $\forall^{inf} x, y\ (x \times y) \simeq (x \sqcup y)$, то для любого множества $A$ и любого вполне упорядоченного множества $M$ имеет место альтернатива: $A \preccurlyeq M$ или $M \preccurlyeq A$. Иначе говоря, из теоремы о равенстве суммы и произведения следует, что любое множество сравнимо по мощности с любым вполне упорядоченным множеством.*

*Доказательство.* Сразу пропустим случай, когда хотя бы одно из множеств конечно, т.к. в этом случае лемма верна и без своего условия. Поэтому пусть $A$ и $M$ — бесконечные множества.

Пусть $<$ — вполне упорядочение на $M$. Рассмотрим прямое произведение $A \times M$. Так как существует биекция $f : A \sqcup M \leftrightarrow A \times M$, то положим $M' = f[M]$ (образ $M$). Так как $M' \subseteq A \times M$, то для $M'$ возможны два случая: либо проекция $M'$ на $A$ совпадает с $A$, либо нет.

В первом случае проекция на $A$, определяемая правилом $Pr_A(a, m) = a$, отображает $M'$ на $A$, т.е. сужение $Pr_A \restriction M'$ является сюръекцией на $A$. Поэтому из него можно построить обратную инъекцию $g : A \to M'$ по правилу

$$g(a) = \min_{<}(f^{-1} \circ \mathrm{pr}_A^{-1}(\{a\})), \quad a \in A,$$

которое корректно определено, поскольку множество $M' \cap \{a\} \times M$ не пусто в силу сюръективности проекции на $M'$.

Наличие инъекции из $A$ в $M$ автоматически означает $A \preccurlyeq M$.

Во втором случае, когда проекция $M'$ не совпадает с $A$, существует подмножество $\{a\} \times M$, целиком лежащее в дополнении к $M'$, а это дополнение равномощно $A$, т.к. оно совпадает с образом $f[A]$. Таким образом, у нас имеет тривиальная инъекция из $M$ в $A$, а значит, $M \preccurlyeq A$. □

Отметим, что здесь появилось важное ограничение — вполне упорядоченность одного из множеств. Вопрос — где его взять, если мы имеем по условию только одно бесконечное множество $A$?

Для этого существует понятие кардинального числа Хартогса. Положим

$$\hbar(A) \stackrel{\text{def}}{=\!=} \min\{\alpha \mid \neg(\alpha \preccurlyeq A)\},$$

[16] Мы не стали здесь описывать, как вложить $x \sqcup x$ в $x \times x$, т.к. yf cktle.otv ifut это сделано в более общем случае.

где предикат $(\alpha \preccurlyeq A)$ означает существование инъекции из $\alpha$ в $A$. Иначе говоря, **число Хартогса** — это минимальный ординал, который невозможно инъективно вложить в множество $A$.

Заметим, что $\mathfrak{h}(A)$ существует для любого $A$. Во-первых, класс ординалов, инъективно вкладываемых в $A$, не пуст, т.к. хотя бы 0 можно вложить в любое множество. Во-вторых, этот класс не может быть собственно классом ординалов. Действительно, пусть $WO(A)$ — множество всех вполне упорядочений подмножеств $A$ (как минимум, там существуют конечные вполне упорядоченные подмножества). Факторизуем его по отношению порядкового изоморфизма $\cong$, получив множество $W = WO(A)/_{\cong}$. Множество $W$ является определяемой частью множества $\mathscr{P}^2(A \times A)$ (при определении упорядоченной пары по Куратовскому). Каждый элемент $W$ взаимно однозначно сопоставляется с порядковым типом своих элементов, т.е. существует инъективное отображение из $W$ в класс Ord. Если бы мы могли вложить в $A$ любой ординал, то для него нашелся бы свой элемент в $W$, и тогда мы бы получили биекцию между $W$ и классом Ord, который является собственно классом. А это противоречит аксиоме подстановки. Следовательно, не все ординалы вкладываются в $A$, а значит, класс ординалов в определении числа Хартогса не пуст (на самом деле он представляет собой класс всех ординалов, не сопоставленных с элементами $W$), т.е. $\mathfrak{h}(A)$ всегда существует.

Кроме того, нетрудно видеть, что $\mathfrak{h}(A) = \sup\{ot(R)+1 \mid R \in WO(A)\}$,[17] а также, что число Хартогса есть кардинал, т.к. $WO(A)$ замкнуто относительно относительно равномощности порядков.

Итак, мы имеем бесконечное множество $A$ и кардинал $\mathfrak{h}(A)$, который вполне упорядочен отношением $\in$. Тогда в рамках теоремы о квадрате по двум предыдущим леммам получаем, что $A \preccurlyeq \mathfrak{h}(A)$ или $\mathfrak{h}(A) \preccurlyeq A$. Однако последнее невозможно по определению числа Хартогса, следовательно, $A \preccurlyeq \mathfrak{h}(A)$ (и, более того, $A \prec \mathfrak{h}(A)$).

Отсюда следует, что $A$ можно вполне упорядочить, перенеся порядок с $\mathfrak{h}(A)$.

Таким образом, мы показали, что из теоремы о квадрате следует теорема Цермело, а она, как показано выше, равносильна AC. Теорема доказана. □

## D4.5. О взаимосвязи формальных теорий

В качестве завершающего примера, иллюстрирующего глубокие связи между, на первый взгляд, различными областями математической логики, мы рассмотрим отношение между арифметикой Пеано (PA) и теорией наследственно конечных множеств (HF). Фундаментальный результат состоит в том, что эти две теории **взаимно интерпретируемы** и, более того, **би-интерпретируемы**, что означает не только возможность перевода теорем из одной теории в другую, но и доказуемость в каждой теории того факта, что последовательный перевод туда и обратно сохраняет исходные утверждения. Это устанавливает чрезвычайно тесную связь, показывая, что обе теории, по сути, говорят об одном и том же, но на разных языках.

**Интерпретация PA в HF.** Фактически, основную работу по интерпретации арифметики в теории множеств мы уже проделали, когда строили арифметику на базе ординалов фон Неймана. Мы определили натуральные числа и операции над ними, используя лишь базовые теоретико-множественные понятия. Важно подчеркнуть, что для определения множества натуральных чисел как класса конечных ординалов и для доказа-

[17] Добавка +1 здесь нужна только для случая конечного множества $A$.

тельства справедливости арифметических операций над ними (сложения, умножения) аксиома бесконечности не требуется. Все необходимые конструкции (понятия пустого множества, пары, объединения, транзитивного замыкания) доступны уже в HF.

Однако здесь есть методологический «подводный камень», касающийся схемы индукции. Когда мы утверждаем, что в HF доказуем перевод каждой аксиомы индукции из PA, мы должны понимать природу этого утверждения. PA содержит *схему* аксиом, по одной для каждой арифметической формулы. В HF мы доказываем каждую такую инстанцию отдельно. Доказательство того, что *все* переводы аксиом доказуемы, требует индукции по построению формулы в нашей *метатеории*. Таким образом, доказательство индукции, которую мы приписываем модели PA внутри HF, является в некотором смысле «внешним». Ситуация меняется, если рассматривать HF не как аксиоматическую систему, а семантически, как совокупность всех истинных предложений о стандартной модели наследственно конечных множеств $V_\omega$. В этой полной теории индукция, разумеется, верна.

**Интерпретация HF в PA.** Обратная интерпретация значительно более сложна и использует технику геделевой нумерации для кодирования конечных множеств и отношения принадлежности натуральными числами. Как было показано в разделе B2.3.2, мы можем установить взаимно-однозначное соответствие между наследственно-конечными множествами и натуральными числами (например, с помощью кодирования Аккермана, $\mathrm{Code}(S) = \sum_{s \in S} 2^{\mathrm{Code}(s)}$). Отношение принадлежности $a \in b$ переводится в арифметический предикат, проверяющий, что в двоичном разложении числа $\mathrm{Code}(b)$ на месте с номером $\mathrm{Code}(a)$ стоит единица. Этот предикат является $\Delta_0$-формулой (в предположении, что экспонента $2^x$ уже определена). Далее необходимо показать, что переводы всех аксиом HF являются доказуемыми утверждениями в PA. Это удается сделать для всех аксиом, включая аксиому степени и схему выделения, так как индукция в PA достаточно сильна, чтобы доказать существование кодов для результатов этих операций.

Эта взаимная интерпретируемость — не единичный случай. PA также биинтерпретируема с теорией Z-Inf (теория Цермело без аксиомы бесконечности). Это демонстрирует, что аксиомы Пеано с полной схемой индукции точно схватывают выразительную мощность, необходимую для формализации понятия конечного множества и базовых алгоритмических операций.

Взаимная интерпретируемость PA и HF — классический результат, демонстрирующий, что арифметика натуральных чисел с индукцией по своей выразительной силе эквивалентна базовой теории конечных множеств. Детальное изложение этих конструкций можно найти в [52] или [53].

Отметим, что упомянутая нами в разделе D3.1 арифметика Робинсона взаимно интерпретируема с так называемой слабой теорией конкатенаций $TC$, разработанной Гжегорчиком [49]. Эта теория по сути является конечной аксиоматизацией нашей модели скобочных записей из раздела B2.3.2, не содержащей аксиомы индукции.

Говоря о взаимосвязи теорий, нельзя не упомянуть и другие фундаментальные результаты, касающиеся уже самой теории множеств.

Во-первых, **ZF и ZFC также взаимно интерпретируемы**. Интерпретация ZFC в ZF — один из величайших триумфов Гёделя. Он показал, что если ZF непротиворечива, то её внутренняя «конструктивная вселенная» $L$ является моделью для ZFC. В обратную сторону интерпретация тривиальна, так как любая модель ZFC является и моделью ZF. Это означает, что аксиома выбора не может быть опровергнута в ZF, если сама ZF непротиворечива.

Во-вторых, существует еще более удивительный факт, связывающий непротиворечивость арифметики с существованием моделей для сильных теорий. Можно показать, что теория PA + Con(ZF), то есть PA с добавлением аксиомы, утверждающей непротиворечивость теории множеств Цермело–Френкеля, способна **интерпретировать теорию** ZFC + CH (т.е. с добавленной континуум-гипотезой) [48]. Это говорит о том, что непротиворечивость такой «простой» теории, как арифметика и способность ее кодировать в себе более сложные теории, является достаточно сильным предположением, из которого произрастают весьма нетривиальные следствия о структуре вселенной множеств.

Указанные пары взаимно интерпретируемых теорий лишний раз подчеркивают глубинную связь между базовыми математическими объектами, такими как: арифметика, алгоритмы, множества.

## D4.6. Упражнения

**Ex1.** Запишите двойственное утверждение для следующего тождества, справедливого в булевых алгебрах: $(a \vee b) \wedge (a \vee \neg b) = a$. Проверьте, верно ли двойственное утверждение.

**Ex2.** Пусть $X$ — бесконечное множество. Рассмотрим совокупность $\mathscr{A} \subset \mathscr{P}(X)$, определенную как:

$$\mathscr{A} = \{S \subseteq X \mid |S| < \omega \vee |X \setminus S| < \omega\}.$$

(Другими словами, $\mathscr{A}$ содержит все конечные подмножества $X$ и их дополнения).

1. Докажите, что $\mathscr{A}$ образует булеву подалгебру в $\mathscr{P}(X)$ (т.е. она содержит $\varnothing, X$ и замкнута относительно объединения, пересечения и дополнения).
2. Является ли $\mathscr{A}$ полной булевой алгеброй? (Напомним, что полнота требует, чтобы произвольные объединения $\bigcup S_i$ оставались в алгебре).
3. Элемент $a$ булевой алгебры называется *атомом*, если $a$ — ненулевой элемент (т.е. $a \neq \varnothing$), и для любого $b$ из алгебры условие $b \subseteq a$ влечет $b = \varnothing$ или $b = a$ (т.е. $a$ минимален среди непустых множеств). Опишите явно атомы алгебры $\mathscr{A}$. Содержит ли каждый непустой элемент $\mathscr{A}$ атом?

**Ex3.** В тексте мы показали, как превратить булеву алгебру в булево кольцо. Теперь рассмотрим обратное. Пусть $\mathscr{R} = \langle R, +, \cdot, 0, 1\rangle$ — коммутативное кольцо с единицей. Пусть $B = \{e \in R \mid e^2 = e\}$ — множество всех *идемпотентов* кольца. Определим операции на $B$:

$$x \wedge y \overset{\text{def}}{=} x \cdot y, \quad x \vee y \overset{\text{def}}{=} x + y - x \cdot y, \quad \neg x \overset{\text{def}}{=} 1 - x.$$

Докажите, что $\langle B, \vee, \wedge, \neg, 0, 1\rangle$ является булевой алгеброй. *Подсказка: Сначала проверьте, что операции замкнуты, т.е. результатом снова является идемпотент.*

**Ex4.** Напомним, что в алгебре Гейтинга импликация $a \to b$ определяется фундаментальным свойством сопряженности (адъюнкции):

$$\forall x \ (x \leqslant (a \to b) \iff x \wedge a \leqslant b).$$

1. Докажите, что это определение подразумевает, что $a \to b$ является наибольшим элементом множества $S = \{x \mid x \wedge a \leqslant b\}$.

2. Используя свойство сопряженности и определение супремума (объединения), докажите тождество:
$$(a \vee b) \to c = (a \to c) \wedge (b \to c).$$
*Подсказка: Чтобы доказать равенство $A = B$, покажите, что для любого тестового элемента $x$ условие $x \leqslant A$ логически эквивалентно $x \leqslant B$. Используйте универсальное свойство супремума: $u \vee v \leqslant w \iff (u \leqslant w \text{ и } v \leqslant w)$.*

**Ex5.** В булевых алгебрах отрицание удовлетворяет совершенной симметрии (двойственности). Однако в алгебрах Гейтинга эта симметрия нарушается.

1. Докажите аналитически, что первый закон Де Моргана выполняется: $\neg(x \vee y) = \neg x \wedge \neg y$.
2. Покажите, что второй закон $\neg(x \wedge y) = \neg x \vee \neg y$ выполняется **не** всегда. Используйте алгебру Гейтинга открытых множеств $\mathbb{R}$ (где $\neg U = \operatorname{Int}(\mathbb{R} \setminus U)$) и рассмотрите интервалы $U = (-\infty, 0)$ и $V = (0, +\infty)$ в качестве контрпримера.

**Ex6.** Докажите, что любая конечная булева алгебра $\mathscr{B}$ изоморфна алгебре подмножеств $\mathscr{P}(A)$ некоторого конечного множества $A$. *Конструктивные шаги:*

1. Пусть $A$ — множество всех атомов $\mathscr{B}$. Покажите, что для любого $x \in \mathscr{B}$ выполняется $x = \bigvee\{a \in A \mid a \leqslant x\}$. (Используйте тот факт, что в конечной алгебре каждый ненулевой элемент содержит атом).
2. Определите отображение $\varphi : \mathscr{B} \to \mathscr{P}(A)$ как $\varphi(x) = \{a \in A \mid a \leqslant x\}$. Докажите, что $\varphi$ — изоморфизм.

**Ex7.** Докажите, что множество точек на плоскости $\mathbb{R} \times \mathbb{R}$ имеет ту же мощность (кардинальное число), что и множество точек на прямой $\mathbb{R}$. *Подсказка: Используйте теорему Кантора-Бернштейна-Шрёдера.*

1. Постройте тривиальную инъекцию $\mathbb{R} \to \mathbb{R} \times \mathbb{R}$.
2. Постройте инъекцию $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$, используя десятичные разложения. (Предупреждение: Будьте осторожны с неединственностью десятичных представлений, например, $0.1999\ldots = 0.2000\ldots$. Как можно избежать этой проблемы?)

**Ex8.** Пусть $R$ — *конечное* коммутативное кольцо с единицей ($1 \neq 0$). Напомним, что элемент $a \neq 0$ называется делителем нуля, если существует $b \neq 0$, такой что $ab = 0$. $R$ называется областью целостности (integral domain), если в нем нет делителей нуля. Докажите, что конечная область целостности обязательно является полем (т.е. каждый ненулевой элемент имеет мультипликативный обратный). *Подсказка: Для фиксированного $a \neq 0$ рассмотрите отображение $f : R \to R$, заданное как $f(x) = ax$. Используйте Принцип Дирихле (а именно то, что инъекция на конечном множестве является сюръекцией).*

**Ex9.** Пусть $\omega^{<\omega}$ обозначает множество всех конечных последовательностей натуральных чисел (т.е. функций из некоторого $n \in \omega$ в $\omega$). Докажите, что $|\omega^{<\omega}| = \aleph_0$. *Подсказка: Представьте $\omega^{<\omega}$ как объединение $\bigcup_{n\in\omega} \omega^n$ и используйте тот факт, что конечное произведение счетных множеств счетно.*

**Ex10.** Вещественное число называется *алгебраическим*, если оно является корнем ненулевого многочлена с рациональными коэффициентами. В противном случае оно называется *трансцендентным*.

1. Используя теорему о счетном объединении счетных множеств (доказанную в тексте), покажите, что множество всех алгебраических чисел $\mathbb{A}$ счетно.
2. Выведите отсюда, что множество трансцендентных чисел несчетно.

**Ex11.** Используйте трансфинитную индукцию, чтобы доказать, что для любого ординала $\alpha$, если $\alpha \geqslant \omega$, то $1 + \alpha = \alpha$.

**Ex12.** Теорема о нормальной форме Кантора. Докажите, что для каждого ненулевого ординала $\alpha$ существуют уникальные натуральные числа $n \geqslant 1$, $k_1, \dots, k_n$ $(0 < k_i < \omega)$ и уникальные ординалы $\beta_1 > \beta_2 > \cdots > \beta_n$, такие что:

$$\alpha = \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \cdots + \omega^{\beta_n} \cdot k_n.$$

*Следуйте этим шагам:*

1. Лемма о росте: Докажите, что $\gamma \leqslant \omega^\gamma$ для всех ординалов $\gamma$.
2. Степень (Логарифм): Используя Лемму, покажите, что для любого $\alpha > 0$ множество $E = \{\gamma \mid \omega^\gamma \leqslant \alpha\}$ является множеством (а не собственным классом) и содержит максимальный элемент $\beta_1$ (или $\sup E = \beta_1$ удовлетворяет условию), такой что $\omega^{\beta_1} \leqslant \alpha < \omega^{\beta_1+1}$.
3. Основное доказательство: Используйте Теорему о делении, чтобы разделить $\alpha$ на $\omega^{\beta_1}$, и примените трансфинитную индукцию по $\alpha$ к остатку.

**Ex13.** Пусть $\alpha = \omega^\omega + \omega \cdot 2 + 1$ и $\beta = \omega^\omega + \omega$.

1. Вычислите $\alpha + \beta$ и $\beta + \alpha$ в нормальной форме Кантора.
2. Вычислите $\alpha \cdot 2$ и $\beta \cdot \omega$.

**Ex14.** Пусть $p_k$ обозначает $k$-е простое число $(p_1 = 2, p_2 = 3, p_3 = 5, \dots)$. Согласно Основной теореме арифметики, любое натуральное число $n > 1$ может быть однозначно представлено как $n = p_{k_m}^{a_m} \dots p_{k_1}^{a_1}$, где $k_m > \cdots > k_1 \geqslant 1$. Определим отображение $c : \mathbb{N} \setminus \{0\} \to \mathrm{Ord}$ так, что $c(1) = 0$, и для $n > 1$:

$$c(n) = \omega^{k_m - 1} \cdot a_m + \cdots + \omega^{k_1 - 1} \cdot a_1.$$

1. Вычислите ординальные значения $c(n)$ для следующих чисел (где $k, j, t \in \omega \setminus \{0\}$):

$$n_1 = 2^k, \quad n_2 = 3^k, \quad n_3 = 2^k 3^j 5^t.$$

2. Докажите, что образом этого отображения является в точности ординал $\omega^\omega$ и что отображение является порядковым изоморфизмом между $\langle \mathbb{N} \setminus \{0\}, \prec \rangle$ (где $n \prec m \iff c(n) < c(m)$) и $\omega^\omega$.

**Ex15.** Используя те же обозначения для разложения на простые множители ($n = p_{k_m}^{a_m} \dots p_{k_1}^{a_1}$), рассмотрим рекурсивно определенное отображение $o : \mathbb{N} \setminus \{0\} \to \mathrm{Ord}$:

$$o(1) = 0, \quad o(n) = \omega^{o(k_m)} \cdot a_m + \cdots + \omega^{o(k_1)} \cdot a_1.$$

1. Вычислите $o(n)$ для следующих чисел $(k, j, t \geqslant 1)$:

$$n_1 = 2^k, \quad n_2 = 3^k, \quad n_3 = 2^k 3^j 5^t.$$

2. Рассмотрим последовательность чисел, определенную рекурсивно: $h_0 = 1$ и $h_{n+1} = p_{h_n}$ ($h_n$-е простое число). Вычислите значения $h_0, h_1, h_2, h_3, h_4$.
3. Вычислите ординальные значения $o(h_n)$ для этих членов.
4. Докажите, что $\sup\{o(h_n) \mid n \in \omega\} = \varepsilon_0$.

**Ex16.** Упростите выражение $\aleph_1 + \aleph_0 \cdot \aleph_1$.

**Ex17.** Пусть $\kappa$ — бесконечный кардинал ($\kappa \geqslant \aleph_0$). Упростите следующие кардинальные выражения, используя свойства из D4.10:

1. $\kappa + \aleph_0$;
2. $3 \cdot \kappa$;
3. $(\kappa^2)^\kappa$.

**Ex18.** Напомним определение иерархии множеств: $V_0 = \varnothing$, $V_{\alpha+1} = \mathscr{P}(V_\alpha)$, и $V_\lambda = \bigcup_{\xi<\lambda} V_\xi$ для предельного $\lambda$.

1. Определите мощность множеств $V_0, V_1, V_2, V_3$.
2. Докажите, что для любого $\alpha$, $V_\alpha$ является транзитивным множеством.
3. Докажите, что если $x \in V_\alpha$, то $\operatorname{rank}(x) < \alpha$.

**Ex19.** В тексте ранг множества $x$ был определен через иерархию фон Неймана:

$$\operatorname{rank}(x) = \min\{\alpha \mid x \subseteq V_\alpha\}.$$

Дадим второе определение ранга рекурсивно:

$$\rho(x) = \sup\{\rho(y) + 1 \mid y \in x\}, \quad \rho(\varnothing) = 0.$$

Докажите, что эти два определения эквивалентны: для всех множеств $x$, $\operatorname{rank}(x) = \rho(x)$. *Подсказка: Докажите $\rho(x) \leqslant \operatorname{rank}(x)$ и $\operatorname{rank}(x) \leqslant \rho(x)$ по отдельности. Напомним, что $y \in V_\alpha \iff \operatorname{rank}(y) < \alpha$.*

**Ex20.** Мы определили трансфинитную рекурсию через сужение функции: $F(\alpha) = \Psi(F \restriction \alpha)$. Рассмотрим альтернативную схему, основанную на образе (множестве предыдущих значений): $G(\alpha) = \Phi(G[\alpha])$. Докажите, что эти две схемы эквивалентны по своей выразительной силе. То есть любую функцию, определенную по схеме сужения, можно получить (возможно, используя вспомогательное кодирование) с помощью схемы образа, и наоборот. *Подсказка:* Чтобы свести рекурсию по сужению к рекурсии по образу, рассмотрите вспомогательную функцию $G(\alpha) = \langle \alpha, F(\alpha) \rangle$.

**Ex21.** Рассмотрим множество рациональных чисел $\mathbb{Q}$ со стандартным порядком $<$.

1. Докажите, что структура $\langle \mathbb{Q}, < \rangle$ не изоморфна никакому ординальному числу.
2. [Теорема Кантора о плотных порядках] Докажите, что любые два счетных плотных линейных порядка без концевых точек изоморфны. (Линейный порядок называется *плотным*, если для любых $x$ и $y$, таких что $x < y$, существует $z$, такой что $x < z < y$. Он *без концевых точек*, если для любого $x$ существуют $y, z$, такие что $y < x < z$). Сделайте вывод, что любой такой порядок изоморфен $\langle \mathbb{Q}, < \rangle$.

*Подсказка к (b): Используйте метод «челнока» (back-and-forth method), чтобы построить изоморфизм шаг за шагом.*

## Рекомендуемая литература

Аксиоматическая теория множеств — это тот язык, на котором сегодня говорит почти вся современная математика. Это огромный и бурно развивающийся мир.

Для любого, кто хочет заниматься этой областью серьезно, существует одна книга, подобная «Властелину колец», — это монументальный труд Томаса Йеха «Теория множеств» [52]. В этом томе на более чем 700 страницах содержится практически все, что было создано в теории множеств за XX век, включая детальное изложение теории кардиналов, ординалов, больших кардиналов и доказательства независимости. Это не учебник для начинающих, а скорее библия специалиста и справочник, к которому возвращаются снова и снова.

Центральным техническим методом современной теории множеств является форсинг, позволивший доказать независимость континуум-гипотезы. Чтобы понять не только технику, но и дух этого открытия, стоит обратиться к первоисточнику — небольшой, но очень емкой книге его создателя Пола Коэна [58]. Это как читать записки гения в момент творения. Однако для систематического изучения метода форсинга большинство математиков предпочитают более гладкий и педагогически выверенный путь, проложенный в классическом учебнике Кеннета Кунена «Теория множеств: введение в доказательства независимости» [69]. Именно по этой книге целые поколения исследователей осваивали это непростое ремесло построения моделей теории множеств.

## Уровень A1

**Ex1.** Дерево разбора для формулы $x = \frac{-b+\sqrt{b^2-4ac}}{2a}$ состоит из следующей иерархии шаблонов:

- Верхний уровень: Равенство $x = \dots$
- Правая часть: Шаблон дроби $\frac{\square}{\square}$
- Числитель: Шаблон сложения $\square + \square$ (где первое слагаемое — унарный минус $-b$, второе — квадратный корень).
- Под корнем: Вычитание $\square - \square$.
- Внутри вычитания: Степень $b^2$ и Умножение $4ac$ (которое есть $4 \cdot a \cdot c$).
- Знаменатель: Умножение $2a$.

**Ex2.** 1) $(a \cdot b) + (c \cdot d)$; 2) $(x^2) + (2xy) + (y^2)$; 3) $(a/b)/c$; 4) $e^{(x^2+y)}$.

**Ex3.** Корень: =. Левый потомок: +, Правый потомок: 0. Потомки +: Левый — Степень ($e$ в степени $i\pi$), Правый — 1.

**Ex4.** Внешний: $\sqrt{\square}$. Внутри: Сложение $1 + \square$. Внутри: $\sqrt{\square}$. Внутри: $1 + \square$. Самый внутренний: $\sqrt{1+x}$.

**Ex5.** Объекты: $x, 3, x^3, 3x, 3x^2, 3$. Действия/Отношения: $\frac{d}{dx}$ (оператор), + (оператор), = (отношение).

**Ex6.** 1. $\exists x(Fr(x) \land Speak(x, \text{English}))$.

2. $\forall x(Fr(x) \to \neg Speak(x, \text{Chinese}))$.

3. $\exists x(Phys(x) \land Love(x, \text{Math}) \land \neg Love(x, \text{QM}))$.

4. $\forall x(Studies(x, \text{Logic}) \to Knows(x, \text{SetTheory}))$.

5. $\exists p(Phys(p) \land \exists t(Theory(t) \land Proposed(p,t) \land$
$\forall m(Math(m) \to Understands(m,t))))$.

6. $\forall x \exists y(Father(y,x) \land \forall z(Father(z,x) \to z = y))$.

7. $\exists x(Glitters(x) \land \neg Gold(x))$.

8. $\forall p(Phys(p) \land \neg Knows(p, \text{Math}) \to$
$\neg Understands(p, \text{GR}) \land \neg Understands(p, \text{QM}))$.

9. $\neg\exists t(Theory(t) \land \forall y(Explains(t,y)))$
или $\forall t(Theory(t) \to \exists y(\neg Explains(t,y)))$.

**Ex7.** 1. Если A содержится в B и B содержится в A, то A равно B.

2. Квадрат любого вещественного числа неотрицателен.

3. Для любого ненулевого целого числа $n$ и любого целого $m$, можно разделить $m$ на $n$ с частным $q$ и остатком $r$.

**Ex8.** 1. $(a+b)^2 = a^2 + b^2 + 2ab$.

2. $\forall x (x \cdot 0 = 0)$.

3. $\forall \varepsilon > 0 \; \exists \delta > 0$.

**Ex9.** 1. Корректно.

2. Некорректно (оператор + ожидает правый операнд, но находит другой оператор ·).

3. Некорректно (cos ожидает аргумент).

4. Корректно.

**Ex10.** 1. Связанная: $k$, Свободная: $n$.

2. Связанная: $x$, Свободная: $a$.

3. Связанная: $i$, Свободная: $I$.

**Ex11.** Внутренняя переменная $i$ затенила бы внешнюю переменную $i$. Диапазон внутренней суммы зависел бы от переменной, по которой она итерируется, создавая двусмысленность.

**Ex12.** 1. $3(a+b)$;

2. $(a+b)^2$;

3. $\sin(a+b)$.

**Ex13.** 1) $\pi$ и 2 (числовые константы). 2) $S$ и $r$ (переменные).

**Ex14.** $2^{(3^4)}$. Вычисление: $(2^3)^2 = 8^2 = 64$. $2^{(3^2)} = 2^9 = 512$.

**Ex15.** 1. Обратная функция (если $f$ — функция).

2. Мультипликативная инверсия (обратное число) $1/f(x)$ (если $f(x)$ — число).

**Ex16.** 1. Унарный (отрицание).

2. Бинарный (вычитание).

3. Унарный (факториал).

4. Бинарный (объединение).

## Уровень A2

**Ex1.** ▶ $2 + 2 = 5$: **Ложное высказывание**.

▶ $x + 1 = 5$: **Предикат** (зависит от $x$).

▶ Все простые числа нечетны: **Ложное высказывание** (контрпример: 2).

▶ $5 > 3$: **Истинное высказывание**.

**Ex2.** ▶ Некоторая кошка не черная.

▶ Ни один студент не любит математику (или: Все студенты не любят математику).

▶ Идет дождь, и земля не мокрая.

**Ex3.** ▶ **Истинно** (элементы $A$ — 1, 2, 3; все $< 4$).

▶ **Истинно** (элементы $B$ — 2, 3, 4; 2 и 4 четные).

▶ **Истинно** ($A \cap B = \{2, 3\}$; оба $\geqslant 2$).

**Ex4.** ▶ Делится на 6 → делится на 3: **Релевантная импликация**. Есть логическая связь и общая переменная $n$.

▶ Эйфелева башня → снег белый: **Материальная импликация**. Утверждение истинно только потому, что обе части истинны; между ними нет семантической связи.

▶ Бабушка → женщина: **Релевантная импликация**. Следствие семантически выводится из определения антецедента.

**Ex5.** **Обосновано**. Транзитивность включения: $S \subseteq R$ и $R \subseteq Q$ влечет $S \subseteq Q$.

**Ex6.** **a, b, c, d, e**. Так как Факси $\subseteq$ Кроло и Винда $\cap$ Кроло $= \varnothing$, множества Факси и Винда не пересекаются.

**Ex7.** **a, c**. Мы знаем, что есть $x \in$ Донас, такой что $x \notin$ Калси. Так как Донас $\subseteq$ Судр, этот $x$ также находится в Судр.

**Ex8.** **b, c, d**. Так как Тека $\subseteq$ Фато и Тека $\cap$ Арати $= \varnothing$, любой элемент Тека является Фато, который не является Арати.

**Ex9.** **b, c**. Мы знаем, что есть $z \in$ Турт, такой что $z \in$ Брон. Так как Брон $\subseteq$ Ханто, этот $z$ также находится в Ханто.

**Ex10.** 1. $A$ (Закон поглощения);

2. $A$ (Дистрибутивность: $A \cup (B \cap \overline{B}) = A \cup \varnothing = A$);

3. $A \cap B$ (Двойное дополнение относительно A);

4. $U$ (Универсум) или 1 (Выражение покрывает все возможные области).

**Ex11.** 1. Ложно. Левая часть равна $(A \setminus B) \cup (A \cap C)$, тогда как правая включает все $C$. Если есть элементы в $C \setminus A$, равенство нарушается.

2. Истинно. Пересечение дистрибутивно относительно симметрической разности.

**Ex12.** 1. Не рефлексивно, Не симметрично (если $y$ женщина, она сестра, а не брат), Транзитивно (брат брата — брат).

2. Рефлексивно, Симметрично, Не транзитивно (например, $0R0.9$ и $0.9R1.8$, но $\neg(0R1.8)$).

3. Строгий частичный порядок (Антирефлексивно, Асимметрично, Транзитивно).

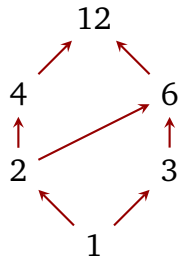
4. Частичный порядок (Рефлексивно, Антисимметрично, Транзитивно).

**Ex13.** 1. Рефлексивно, Не транзитивно: $\{(a, a), (b, b), (c, c), (a, b), (b, c)\}$ (отсутствует $(a, c)$).

2. Симметрично, Не рефлексивно: $\{(a, b), (b, a)\}$.

3. Строгий частичный порядок: $\{(a, b), (b, c), (a, c)\}$.

**Ex14.** Диаграмма Хассе ($D_{12}$):




**Ex15.** 1. Да. $x + y$ четно $\iff$ $x, y$ имеют одинаковую четность. Классы: Четные и Нечетные.

2. Да ($x = \pm y$). Классы суть $\{k, -k\}$.

3. Нет. Не симметрично ($1 \leqslant 2$, но $2 \not\leqslant 1$).

**Ex16.** 1. Да. Определено для всех $x \in A$, единственный $y$.

2. Нет. Не тотально (не определено для 3).

3. Нет. Не функционально (1 отображается и в 2, и в 3).

4. Да. (Константная функция).

**Ex17.** 1. A — Рыцарь, B — Лжец.

2. A — Рыцарь, B — Лжец.

**Ex18.** 1. Необосновано. (Ошибка утверждения следствия).

2. Обосновано. (Силлогизм / Modus Ponens).

3. Обосновано. (Modus Tollens / Контрапозиция).

**Ex19.** 1. Индуктивное.

2. Дедуктивное.

3. Дедуктивное.

**Ex20.** ▶ *Язык:* «Он умер и был похоронен» против «Он был похоронен и умер».

▶ *Программирование:* ‘if (x != 0) and (1/x > 1)‘ (Сначала проверяет безопасность) против ‘if (1/x > 1) and (x != 0)‘ (Вызывает ошибку Деления на ноль).

**Ex21.** 1. $\{0, 1, 2, 3, 4\}$.

2. Множество четных чисел $\{0, 2, 4, \dots\}$.

3. $\varnothing$ (Пустое множество).

4. $\mathbb{N}$ (Весь универсум, тавтология).

**Ex22.** 1. $\text{Дед}(x, y) \overset{\text{def}}{\leftrightarrow} \exists z(\text{Отец}(x, z) \wedge \text{Отец}(z, y))$.

2. $\text{Прадед}(x, y) \overset{\text{def}}{\leftrightarrow} \exists z(\text{Дед}(x, z) \wedge \text{Отец}(z, y))$.

3. $\text{ОбщийОтец}(x, y) \overset{\text{def}}{\leftrightarrow} \exists z(\text{Отец}(z, x) \wedge \text{Отец}(z, y))$.

Дед и Прадед антирефлексивны, несимметричны и нетранзитивны. ОбщийОтец — рефлексивное отношение (общий отец $x$ и $x$ — это отец $x$), симметричное и, поскольку отец у каждого единственный, транзитивное, то есть отношение эквивалентности.

## Уровень B1

**Ex1.** 1. Да. 2. Да. 3. Да. 4. Да (если $A$ и $B$ оба истинны, импликация выполняется; если ложны, выполняется).

**Ex2.** 1. $\mathscr{A} = 0, \mathscr{B} = 1$ ($1 \to 0$, ложно).

2. $\mathscr{A} = 0, \mathscr{B} = 1$ ($1 \to 0$, ложно).

3. $\mathscr{A} = 0, \mathscr{B} = 1, \mathscr{C} = 1$ ($1 \to 0$, ложно).

**Ex3.** 1. $\neg\mathscr{A} \wedge \mathscr{B}$;

2. $\mathscr{A} \wedge (\neg\mathscr{B} \vee \mathscr{C})$;

3. $\exists x \forall y (\varphi(x, y) \wedge \psi(x))$ (используя $\neg(\mathscr{A} \to \mathscr{B}) \equiv \mathscr{A} \wedge \neg\mathscr{B}$).

**Ex4.** 1. $\forall x (P(x) \to Q(a))$;

2. $(\forall x P(x)) \wedge Q(a)$;

3. $\exists z (a < z \to \forall x (x = z))$;

4. $\int_0^a x^2 dx$.

**Ex5.** 1. $\exists y\ (b < y)$;

2. $\exists y\ (S(b) < y)$;

3. Недопустимо, потому что $y$ связана в $\varphi$. Подстановка $a \to y$ захватила бы переменную («существует $y$ больше самого себя» вместо «больше $a$»).

**Ex6.** Используйте Теорему о дедукции и Modus Ponens дважды для $\mathscr{A}, \mathscr{A} \to \mathscr{B}, \mathscr{B} \to \mathscr{C}$.

**Ex7.** 1. $\mathscr{A} \to (\mathscr{A} \to \mathscr{B})$ (Гипотеза);

2. $\mathscr{A}$ (Гипотеза);

3. $\mathscr{A} \to \mathscr{B}$ (MP 1,2);

4. $\mathscr{B}$ (MP 3,2). Результат $\mathscr{B}$. По Теореме о дедукции: $(\mathscr{A} \to (\mathscr{A} \to \mathscr{B})) \vdash \mathscr{A} \to \mathscr{B}$.

**Ex8.** 1. $\forall x P(x)$ (Гипотеза).

2. $P(a)$ (Аксиома $\forall$).

3. $P(a) \to \exists x P(x)$ (Аксиома $\exists$).

4. $\exists x P(x)$ (MP).

**Ex9.** Если $P(a) \to \forall x P(x)$, то мы утверждаем «если свойство выполняется для конкретного $a$, оно выполняется для всех», что явно ложно (напр., $a = 2, P(x)$=«x четно»). Важно понимать отличие от правила обобщения: в нем, если мы вывели $P(a)$ без условий на $a$, то мы можем перейти к формуле $\forall x P(x)$.

**Ex10.** 1. $\exists x (P(x) \wedge \neg Q(x))$;

2. $\forall x \exists y (\neg R(x, y) \wedge \neg S(x))$;

3. $\exists x P(x) \wedge \exists y \neg Q(y)$.

**Ex11.** Если $x$ нет в $P$, то $P$ константно относительно $x$. «Для всех $x$, ($P$ истинно или $Q(x)$ истинно)» эквивалентно «$P$ истинно или (для всех $x$, $Q(x)$ истинно)».

**Ex12.** $P(x)$ означает «$x$ четно», а $Q(x)$ означает «$x$ нечетно» в Арифметике.

**Ex13.** 1. Универсум $\{1, 2\}$, $P(1) = T, P(2) = F$.

2. Универсум $\mathbb{N}, P(x, y) : x < y$.

3. $P$ четно, $Q$ нечетно.

**Ex14.** Да. Модель: $\{2, 3, 4, \dots\}$ с порядком, определенным делимостью (рефлексивно, транзитивно, нелинейно). Числа 0 и 1 исключены: 1 делит всё, а всё делит 0, поэтому несравнимого с ними элемента не нашлось бы.

**Ex15.** 1. $(a = b) \to (P(a) \leftrightarrow P(b))$;

2. $(a = b) \to ((a < c) \leftrightarrow (b < c))$.

**Ex16.** 1. $\exists x \exists y (x \neq y)$;

2. $\exists x \exists y \exists z (x \neq y \wedge y \neq z \wedge x \neq z)$.

**Ex17.** 1. $\exists x \forall y (y = x)$;

2. $\exists x \exists y (x \neq y \wedge \forall z (z = x \vee z = y))$.

**Ex18.** 1. $\forall x (x \in A \to (x \in B \vee x \in C))$;

2. $\neg \exists x (x \in A \wedge x \in B)$;

3. $\forall x ((x \in A \wedge x \notin B) \to x \in C)$.

**Ex19.** 1. Истинно. (Каждый карандаш либо Красный, либо Длинный. $p_1$: Красный (Т), $p_2$: Красный (Т), $p_3$: Длинный (Т)).

2. Истинно. (Свидетель: $p_1$ Красный и Не Длинный).

3. Ложно. (Контрпример: $p_2$ Длинный, но он Красный, поэтому $\neg R(p_2)$ Ложно).

4. Истинно. (Если $x$ Красный $(p_1, p_2)$, нам нужен Длинный карандаш $y \neq x$. Для $p_1$ возьмем $p_2$ или $p_3$. Для $p_2$ возьмем $p_3$).

**Ex20.** 1. Истинно. (Для каждого числа $x$ существует большее число $y$).

2. Истинно. (У каждого есть биологический родитель).

3. Ложно. (Не каждая фигура атакует что-то; например, ладья, зажатая пешками, может ничего не атаковать, или Король один на доске).

## Уровень B2

**Ex1.** $\forall x (x = 0 \vee \exists y (x = S(y)))$.

**Ex2.** $Sq(x) \overset{\text{def}}{\leftrightarrow} \exists y (x = y \cdot y)$.

**Ex3.** ▶ $Even(x) \overset{\text{def}}{\leftrightarrow} \exists k (x = k + k)$ (или $x = 2 \cdot k$, если 2 определено).

▶ $x \mid y \overset{\text{def}}{\leftrightarrow} \exists k (y = x \cdot k)$.

▶ $Prime(p) \overset{\text{def}}{\leftrightarrow} (1 < p) \wedge \forall x \ (x \mid p \to x = 1 \vee x = p)$.

▶ $\forall n \ (Even(n) \wedge 2 < n) \to \exists p, q \ (Prime(p) \wedge Prime(q) \wedge n = p + q))$.

**Ex4.** $Prime(p) \overset{\text{def}}{\leftrightarrow} \neg Inv(p) \wedge \forall d \ (d \mid p \to Inv(d) \vee (p \mid d))$. *Пояснение:* Простое число — это необратимый элемент (не равный 1), такой что любой его делитель $d$ является либо обратимым элементом (1), либо делится на $p$. В натуральных числах, если $d \mid p$

и $p \mid d$, то $d = p$. Таким образом, формула корректно утверждает, что единственными делителями $p$ являются 1 и само $p$.

**Ex5.** $\forall x \exists p(Prime(p) \wedge p > x \wedge Prime(S(S(p))))$.

**Ex6.** $\forall x \forall y \exists z(\exists k(z = x \cdot k) \wedge \exists m(z = y \cdot m))$.

**Ex7.** $G(a,b,d) \overset{\text{def}}{\leftrightarrow} (d \mid a) \wedge (d \mid b) \wedge \forall k((k \mid a \wedge k \mid b) \to k \leqslant d)$.

**Ex8.** Пусть $x \mid y$ и $y \mid z$. Тогда $\exists k(y = x \cdot k)$ и $\exists m(z = y \cdot m)$. Подставляя $y$: $z = (x \cdot k) \cdot m = x \cdot (k \cdot m)$ (по ассоциативности умножения). Так как $k \cdot m$ натуральное число, $x \mid z$.

**Ex9.** База $n = 0$: $0 = 0$. Шаг: $S_{n+1} = S_n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}$.

**Ex10.** База $n = 0$: 0 делится. Шаг: $(n+1)^3 - (n+1) = n^3 + 3n^2 + 3n + 1 - n - 1 = (n^3 - n) + 3(n^2 + n)$. Оба слагаемых делятся на 3.

**Ex11.** База $n = 0$: $1 \geqslant 1$. Шаг: $(1+x)^{k+1} = (1+x)^k(1+x) \geqslant (1+kx)(1+x) = 1 + (k+1)x + kx^2 \geqslant 1 + (k+1)x$.

**Ex12.** База $n = 1$: $1 = 1^2$. Шаг: $n^2 + (2(n+1) - 1) = n^2 + 2n + 1 = (n+1)^2$.

**Ex13.** Предположим верно для всех $k < n$. Если $n$ простое, готово. Если составное, $n = a \cdot b$. $a < n$, поэтому $a$ имеет простые множители.

**Ex14.** Если $a^2 = 2b^2$, то $a$ четно, $a = 2k$. $4k^2 = 2b^2 \implies 2k^2 = b^2$, значит $b$ четно. Мы получаем меньшее решение $(b, a/2)$, продолжая бесконечно.

**Ex15.** Корневой узел $\{\dots\}$ с тремя потомками: лист $\varnothing$, узел $\{\varnothing\}$ (потомок $\varnothing$), узел $\{\varnothing, \{\varnothing\}\}$ (потомки $\varnothing$ и $\{\varnothing\}$).

**Ex16.** $\operatorname{rank}(x) = \sup\{\operatorname{rank}(y) + 1 \mid y \in x\}$ (для конечных, max +1).

**Ex17.** $(x \in A/_\sim) \overset{\text{def}}{\leftrightarrow} (x \subseteq A) \wedge (x \neq \varnothing) \wedge \forall y, z \in A\ ((y \sim z) \wedge (y \in x) \to z \in x) \wedge \forall y, z \in x\ (y \sim z)$.

**Ex18.** Чтобы выразить, что $A$ есть упорядоченная пара $\langle x, y\rangle = \{\{x\}, \{x, y\}\}$ полностью формально (без использования фигурных скобок), мы должны явно утверждать существование составляющих множеств $\{x\}$ и $\{x, y\}$:

$$\exists u \exists v \Big( \underbrace{\forall t(t \in u \leftrightarrow t = x)}_{u=\{x\}} \wedge \underbrace{\forall s(s \in v \leftrightarrow (s = x \vee s = y))}_{v=\{x,y\}} \wedge \underbrace{\forall z(z \in A \leftrightarrow (z = u \vee z = v))}_{A=\{u,v\}} \Big).$$

**Ex19.** Если $a = a' + kn$ и $b = b' + mn$, то $(a+b) = (a'+b') + n(k+m)$, так что $a + b \equiv a' + b' \pmod n$.

**Ex20.** Если $a = a' + kn$ и $b = b' + mn$, то $ab - a'b' = a(b - b') + b'(a - a')$, так что $ab \equiv a'b' \pmod n$.

**Ex21.** $\operatorname{Code}(\varnothing) = 0$; $\operatorname{Code}(\{\varnothing\}) = 2^0 = 1$; $\operatorname{Code}(\{\{\varnothing\}\}) = 2^1 = 2$; $\operatorname{Code}(\{\varnothing, \{\varnothing\}\}) = 2^0 + 2^1 = 3$; $\langle \varnothing, \varnothing\rangle = \{\{\varnothing\}, \{\varnothing, \varnothing\}\} = \{\{\varnothing\}\}$, так что $\operatorname{Code}(\langle \varnothing, \varnothing\rangle) = 2$.

**Ex22.** a) $11 = 2^0 + 2^1 + 2^3$. Элементы имеют коды 0, 1, 3. Так как код 3 соответствует $\{\varnothing, \{\varnothing\}\}$, результат — $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$. (Это ординал 3). b)$15 = 2^0 + 2^1 + 2^2 + 2^3$. Элементы имеют коды 0, 1, 2, 3. Множество есть $\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}$.

# Уровень C1

**Ex1.** 1. $\forall x(x \in A \to x \in B)$; 2. $\neg\exists x(x \in A \wedge x \in B)$; 3. $\exists x\exists y(x \in A \wedge y \in A \wedge x \neq y \wedge \forall z(z \in A \to (z = x \vee z = y)))$; 4. $\forall x(x \in P \leftrightarrow x \subseteq A)$.

**Ex2. Теорема Кантора:**

$$\neg\exists f\ \big((f : A \to \mathscr{P}(A)) \wedge \forall Y \in \mathscr{P}(A)\ \exists x \in A\ (f(x) = Y)\big).$$

(Примечание: Вторая часть конъюнкции выражает, что $f$ сюръективна).

**Аксиома счетного выбора ($\mathrm{AC}_\omega$):**

$$\forall I \forall A\big(((I : \omega \to A) \wedge \forall n \in \omega :\ I(n) \neq \varnothing) \to \big(\exists f\ (f : \omega \to \bigcup A) \wedge \forall n \in \omega :\ f(n) \in I(n))\big).$$

(Здесь $I$ представляет семейство множеств, индексированных $\omega$).

**Определение фильтра $\mathscr{F}$ на $S$:**

$$\mathrm{Filter}(\mathscr{F}, S) \overset{\text{def}}{\leftrightarrow} (\mathscr{F} \subseteq \mathscr{P}(S)) \wedge (S \in \mathscr{F}) \wedge (\varnothing \notin \mathscr{F}) \wedge [\forall A, B \in \mathscr{F} : (A \cap B \in \mathscr{F})] \wedge [\forall C \in \mathscr{F} : \forall D \in \mathscr{P}(S) : (C \subseteq D \to D \in \mathscr{F})].$$

**Принцип максимума Хаусдорфа:** Определим вспомогательные предикаты для частичного порядка на $A$ и цепи в $A$:

$$\mathrm{Part}(A, R) \overset{\text{def}}{\leftrightarrow} \forall x, y, z \in A : \big(xRx \wedge (xRy \wedge yRz \to xRz) \wedge (xRy \wedge yRx \to x = y)\big);$$

$$\mathrm{Chain}(C, A, R) \overset{\text{def}}{\leftrightarrow} (C \subseteq A) \wedge \forall x, y \in C : (xRy \vee yRx).$$

(Примечание: Так как $R$ — частичный порядок на $A$, он уже транзитивен и антисимметричен на любом подмножестве $C$, так что для цепи нам нужно лишь постулировать связность).

Принцип:

$$\forall A, R\big(\mathrm{Part}(A, R) \to \forall C[\mathrm{Chain}(C, A, R) \to \exists M(\mathrm{Chain}(M, A, R) \wedge (C \subseteq M) \wedge \forall X(\mathrm{Chain}(X, A, R) \wedge (M \subseteq X) \to M = X))]\big).$$

**Ex3.** Проверьте 3 свойства фильтра. Пустого множества там нет (так как $S$ бесконечно). Пересечение множеств с конечными дополнениями имеет конечное дополнение. Надмножество множества с конечным дополнением имеет конечное дополнение.

**Ex4.** $R_1$: Рефлексивно, Симметрично, Антисимметрично, Транзитивно. $R_2$: Симметрично. $R_3$: Антисимметрично (обратных пар нет), Транзитивно.

**Ex5.** Функция отображает пару $\langle a, b\rangle$ в $N = 2^a(2b + 1) - 1$. Это эквивалентно $N + 1 = 2^a(2b + 1)$. По Основной теореме арифметики, каждое положительное целое $M$ (здесь $M = N + 1 \geqslant 1$) может быть однозначно представлено как произведение степени 2 и

нечетного числа. Пусть $M = 2^k \cdot m$, где $m$ нечетно. Так как $m$ нечетно, оно однозначно представимо как $2l + 1$ для некоторого $l \in \omega$. Таким образом, для каждого $N \in \omega$ существует уникальная пара экспоненты и нечетного множителя, соответствующая уникальной паре $\langle a, b\rangle$, такой что $N + 1 = 2^a(2b + 1)$. Это гарантирует как сюръективность (существование), так и инъективность (единственность).

**Ex6.** Так как $f$ сюръективна, множество прообразов $f^{-1}(\{y\})$ непусто для каждого $y$. По AC, мы можем выбрать один элемент $x_y$ из каждого прообраза. Положим $g(y) = x_y$. Тогда $f(g(y)) = f(x_y) = y$.

**Ex7.** Алгоритм: Мы действуем рекурсией по размеру множества. Пусть $i$ — счетчик, изначально 0. Пусть $A_{current} = A$.

▶ *Шаг:* Пока $A_{current} \neq \varnothing$:

1. Выбрать минимальный элемент $m$ в $A_{current}$ (существует, т.к. множество конечно).
2. Положить $f(m) = i$.
3. Удалить $m$: $A_{current} := A_{current} \setminus \{m\}$.
4. Увеличить $i$: $i := i + 1$.

Проверка: 1) *Биективность:* Так как мы удаляем ровно один элемент на каждом шаге и увеличиваем $i$, и процесс выполняется $n$ раз, $f$ отображает $A$ биективно на $\{0, \dots, n-1\}$. 2) *Линейность:* Порядок $\preccurlyeq$ изоморфен стандартному порядку на натуральных числах, который линеен. 3) *Продолжение:* Если $x < y$ в исходном частичном порядке, то $y$ не может быть минимальным, пока $x$ все еще в множестве. Таким образом, $x$ должен быть удален (получить значение) на более раннем шаге, чем $y$. Следовательно, $f(x) < f(y)$, что влечет $x \preccurlyeq y$.

**Ex8.** 1. Да ($3 = \{0, 1, 2\}$). 2. Нет (не транзитивно: пусть $x = \{\{\varnothing\}\}$, тогда $x \in B$, но $x \notin B$, потому что $\{\varnothing\} \in x$, но $\{\varnothing\} \notin B$). 3. Да ($\omega + 1$).

**Ex9.** 1: 0; 2: 1; 3: 2; 4: 2.

**Ex10.** 1. $\operatorname{rank}(\{a\}) = \alpha + 1$. $\operatorname{rank}(\{a, b\}) = \max(\alpha, \beta) + 1$.
$\operatorname{rank}(\langle a, b\rangle) = \operatorname{rank}(\{\{a\}, \{a, b\}\}) = \max(\alpha + 1, \max(\alpha, \beta) + 1) + 1 = = \max(\alpha, \beta) + 2$.

2. Целые числа $\mathbb{Z} \subseteq \mathscr{P}(\omega \times \omega)$. $\operatorname{rank}(n) < \omega$. $\operatorname{rank}(\langle n, m\rangle) < \omega$. $\operatorname{rank}(\omega \times \omega) = \omega$. Класс эквивалентности $z \in \mathbb{Z}$ есть множество пар, поэтому $\operatorname{rank}(z) = \omega$. Множество $\mathbb{Z}$ состоит из таких классов, поэтому $\operatorname{rank}(\mathbb{Z}) = \omega + 1$.

**Ex11.** 1. $V_1$. 2. $V_{\omega+1}$. 3. $V_{\omega+2}$.

**Ex12.** $F(\alpha) = \alpha$.

**Ex13.** Генератор Фибоначчи.

$$\Phi(g) = \begin{cases} 0, & \text{если } \operatorname{dom}(g) = \varnothing \text{ (шаг 0);} \\ 1, & \text{если } \operatorname{dom}(g) = \{\varnothing\} \text{ (шаг 1);} \\ g(n-1) + g(n-2), & \text{если } \operatorname{dom}(g) = n \geqslant 2. \end{cases}$$

Примечание: $g(n-1)$ — последний элемент предыстории, $g(n-2)$ — предпоследний.

**Ex14.** Шаг 1: $\mathbb{R} \leftrightarrow (0, 1)$. Стандартная функция $f(x) = \frac{1}{2} + \frac{1}{\pi}\arctan(x)$ отображает $\mathbb{R}$ биективно в открытый интервал $(0, 1)$.

Шаг 2: $(0,1) \leftrightarrow [0,1]$. Нам нужно «поглотить» две недостающие концевые точки $\{0,1\}$ в открытый интервал. Выберем счетную последовательность различных точек внутри $(0,1)$, например:

$$S = \left\{ \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots \right\} = \left\{ \frac{1}{n+2} \mid n \in \omega \right\}.$$

Построим биекцию $g : (0,1) \to [0,1]$. Мы отображаем множество $S$ в множество $S \cup \{0,1\}$ и оставляем остальную часть интервала без изменений. Определим $g(x)$ следующим образом:

$$g(x) = \begin{cases} 0, & \text{если } x = 1/2 \text{ (1-й элемент S)}, \\ 1, & \text{если } x = 1/3 \text{ (2-й элемент S)}, \\ \frac{1}{n}, & \text{если } x = \frac{1}{n+2} \text{ для } n \geqslant 2 \text{ (сдвигаем остальные)}, \\ x, & \text{если } x \notin S. \end{cases}$$

Эта $g$ является биекцией. Обратная $g^{-1}$ переводит $0 \to 1/2$, $1 \to 1/3$, и сдвигает последовательность обратно.

Результат: Композиция $g \circ f$ является искомой биекцией $\mathbb{R} \to [0,1]$.

**Ex15.** Пусть $A = (0,1)$ и $B = (0,1) \cup (2,3)$. Мы строим биекцию $F : B \to A$ в три шага.

Шаг 1: Сдвиг и Масштабирование. Отобразим два интервала из $B$ в один интервал с выколотой точкой $(0,1) \setminus \{1/2\}$. Определим $f : B \to (0,1) \setminus \{1/2\}$ как:

$$f(x) = \begin{cases} x/2, & \text{если } x \in (0,1) \quad \text{(отображает в } (0,1/2)), \\ x/2 - 1/2, & \text{если } x \in (2,3) \quad \text{(отображает в } (1/2,1)). \end{cases}$$

Эта функция является биекцией из $B$ в $Z = (0,1) \setminus \{1/2\}$.

Шаг 2: Заполнить пробел (Отель Гильберта). Нам нужна биекция $g : Z \to (0,1)$, которая «поглощает» недостающую точку $1/2$. Выберем счетную последовательность внутри $Z$: $S = \{1/3, 1/4, 1/5, \dots\} = \{1/n \mid n \geqslant 3\}$. Определим $g(y)$, сдвигая эту последовательность, чтобы включить $1/2$:

$$g(y) = \begin{cases} 1/(n-1), & \text{если } y = 1/n \text{ для } n \geqslant 3 \quad \text{(отображает } 1/3 \to 1/2, 1/4 \to 1/3, \dots), \\ y, & \text{если } y \notin S. \end{cases}$$

Эта $g$ отображает $Z$ на $(0,1)$ биективно.

Заключение: Композиция $F = g \circ f$ является искомой биекцией из $(0,1) \cup (2,3)$ в $(0,1)$.

**Ex16.** 1. Покомпонентный порядок ($\leqslant_{prod}$). Проверяем $x \leqslant_{prod} y$: $2 \leqslant 3$ Истинно, но $100 \leqslant 1$ Ложно. Значит $\neg(x \leqslant_{prod} y)$. Проверяем $y \leqslant_{prod} x$: $3 \leqslant 2$ Ложно. Значит $\neg(y \leqslant_{prod} x)$. *Заключение:* $x$ и $y$ несравнимы. *Свойства:* Так как существуют несравнимые элементы, $\leqslant_{prod}$ не является линейным порядком (это частичный порядок). Следовательно, это не вполне упорядочение (так как вполне упорядочение должно быть линейным).

2. Лексикографический порядок ($\leqslant_{lex}$). Сравниваем первые компоненты: $2 < 3$. Согласно определению, это немедленно влечет $x <_{lex} y$.

*Свойства:*

1. Для любых различных пар, либо первые компоненты отличаются (тогда порядок определяется ими), либо они равны (тогда порядок определяется вторыми компонентами). Таким образом, это **линейный порядок**.

2. Так как $\omega$ вполне упорядочено, лексикографическое произведение $\omega \times \omega$ также вполне упорядочено. (Любое непустое подмножество $S$ имеет минимум: возьмем множество первых координат элементов $S$, найдем его минимум $m_1$, затем найдем минимум $m_2$ вторых координат среди элементов $S$, начинающихся с $m_1$).

**Ex17.** Если $x = \{x\}$, то $x \in x$. Множество $\{x\}$ имеет только один элемент $x$, и $x \cap \{x\} = \{x\} \cap \{x\} = x \neq \varnothing$. Это противоречит Аксиоме регулярности.

**Ex18.** 1. $\omega$ (предельный). 2. $\omega + 1$ (последователь). 3. $\omega$. 4. $\omega + \omega$.

**Ex19.** $(1 + 1) \cdot \omega = 2 \cdot \omega = \omega$. $1 \cdot \omega + 1 \cdot \omega = \omega + \omega = \omega \cdot 2$. Так как $\omega \neq \omega \cdot 2$, правая дистрибутивность нарушается.

**Ex20.** $\omega + x = \omega \cdot 2$. Так как $\omega \cdot 2 = \omega + \omega$, решение $x = \omega$. (Примечание: $x = n < \omega$ дает $\omega + n < \omega \cdot 2$, а $x = \omega + 1$ дает $\omega + (\omega + 1) = \omega \cdot 2 + 1 > \omega \cdot 2$).

**Ex21.** $\beta$ меньше. В арифметике ординалов младшие члены справа не влияют на сравнение по старшей степени, но здесь коэффициенты при $\omega$ важны. $3 > 2$.

**Ex22.** Проанализируем структуру порядка $\leqslant_{lex}$. Мы можем сгруппировать элементы $\omega \times \omega$ по их первой координате $n$. Пусть $R_n = \{\langle n, m\rangle \mid m \in \omega\}$ будет $n$-й «строкой».

1. Внутренняя структура строки: Внутри фиксированной строки $R_n$, первые координаты равны, поэтому порядок определяется вторыми координатами $m$. Так как $m$ пробегает $\omega$, каждая строка $R_n$ порядково изоморфна $\omega$.

2. Упорядочение строк: Так как первая координата сравнивается первой в $\leqslant_{lex}$, для любых $n_1 < n_2$, все элементы строки $R_{n_1}$ строго предшествуют всем элементам строки $R_{n_2}$.

3. Общая структура: Множество $P$ состоит из последовательности строк $R_0, R_1, R_2, \dots$, где каждая строка — копия $\omega$, и они расположены в порядковом типе $\omega$. Это соответствует ординальной сумме $\omega$ копий $\omega$:

$$\underbrace{\omega}_{R_0} + \underbrace{\omega}_{R_1} + \underbrace{\omega}_{R_2} + \dots = \omega \cdot \omega.$$

Ответ: Порядковый тип равен $\omega \cdot \omega$.

**Ex23.** Аксиома выделения (subset axioms) ведет к парадоксу Рассела, если применить её к $V$. Также нарушается регулярность (хотя парадокс первичен).

**Ex24.** Комплексные числа.

1. $\langle a, b\rangle +_{\mathbb{C}} \langle c, d\rangle \overset{\text{def}}{=\!=} \langle a +_{\mathbb{R}} c, b +_{\mathbb{R}} d\rangle$;

2. $\langle a, b\rangle \cdot_{\mathbb{C}} \langle c, d\rangle \overset{\text{def}}{=\!=} \langle a \cdot_{\mathbb{R}} c -_{\mathbb{R}} b \cdot_{\mathbb{R}} d, a \cdot_{\mathbb{R}} d +_{\mathbb{R}} b \cdot_{\mathbb{R}} c\rangle$.

Проверка для $i = \langle 0, 1\rangle$: $i \cdot_{\mathbb{C}} i = \langle 0 \cdot_{\mathbb{R}} 0 -_{\mathbb{R}} 1 \cdot 1, 0 \cdot_{\mathbb{R}} 1 +_{\mathbb{R}} 1 \cdot_{\mathbb{R}} 0\rangle = \langle -1, 0\rangle$. Верно.

**Ex25.** Пусть $\mathscr{P}$ — множество всех частичных порядков $R$ на $A$, таких что $\leqslant \subseteq R$. Мы упорядочиваем множество $\mathscr{P}$ теоретико-множественным включением $\subseteq$. Чтобы применить Лемму Цорна, проверим, что каждая цепь в $\mathscr{P}$ имеет верхнюю грань.

Пусть $\mathscr{C} \subseteq \mathscr{P}$ — непустая цепь. Определим $U = \bigcup \mathscr{C}$.

- *Рефлексивность:* Так как $\leqslant \subseteq U$, $U$ рефлексивно.
- *Транзитивность:* Пусть $(x, y) \in U$ и $(y, z) \in U$. Тогда существуют $R_1, R_2 \in \mathscr{C}$, такие что $(x, y) \in R_1$ и $(y, z) \in R_2$. Так как $\mathscr{C}$ — цепь, предположим $R_1 \subseteq R_2$. Тогда обе пары в $R_2$. Так как $R_2$ транзитивен, $(x, z) \in R_2 \subseteq U$.
- *Антисимметричность:* Пусть $(x, y) \in U$ и $(y, x) \in U$. Аналогично, существует некоторое $R \in \mathscr{C}$, содержащее обе пары. Так как $R$ антисимметрично, $x = y$.

Таким образом, $U$ — частичный порядок, продолжающий $\leqslant$, поэтому $U \in \mathscr{P}$. $U$ очевидно является верхней гранью для $\mathscr{C}$.

По Лемме Цорна, $\mathscr{P}$ имеет максимальный элемент $L$. Мы утверждаем, что $L$ — линейный порядок. Предположим противное. Тогда существуют несравнимые элементы $a, b \in A$ (т.е. $\neg(aLb) \wedge \neg(bLa)$). Определим новое отношение $L'$ как транзитивное замыкание $L \cup \{(a, b)\}$:

$$L' = L \cup \{(x, y) \mid xLa \wedge bLy\}.$$

Очевидно $L \subsetneq L'$ (так как $(a, b) \in L'$, но $(a, b) \notin L$). Чтобы показать $L' \in \mathscr{P}$, мы должны проверить антисимметричность (транзитивность и рефлексивность верны по построению). Если $L'$ не антисимметрично, существуют $x, y$, такие что $xL'y$ и $yL'x$ с $x \neq y$. Так как $L$ антисимметрично, по крайней мере одно отношение должно исходить из нового множества. Это влечет цикл, включающий $a$ и $b$, который редуцируется к $bLa$, что противоречит предположению о несравнимости. Таким образом, $L'$ — строго больший частичный порядок, что противоречит максимальности $L$. Следовательно, $L$ должен быть линейным.

# Глава D1

**Ex1.** a) $\pi$: Самостоятельная, основная (специальный символ/буква); b) $\subseteq$: Несамостоятельная, основная (оператор); c) $\hat{y}$: Самостоятельная, производная (буква + акцент); d) $\nabla$: Несамостоятельная, основная (оператор, образован от перевернутой буквы, но считается основным оператором в $\mathfrak{Math}$); e) { }: Несамостоятельная, основная (группиратор).

**Ex2.** a) $\Sigma$ — самостоятельная, основная (буква). b) $\sum$ — несамостоятельная, основная (оператор, образован от буквы). c) $\overline{z}$ — самостоятельная, производная (буква + акцент). d) ; — несамостоятельная, основная (разделитель). e) $\to$ — несамостоятельная, основная (оператор).

**Ex3.** Жесткие: a) Да. b) Да. c) Нет (составная лексема). d) Да.

**Ex4.** 1. 3 аргумента (переменная, предельная точка, выражение).

2. 2 аргумента (основание, аргумент).

3. 1 аргумент (выражение).

4. 2 аргумента (функция числителя, переменная знаменателя).

**Ex5.** Структура дерева (от корня к листьям):

- Корень: Равенство $\sqcup = \sqcup$ (Слева: $\sigma(x)$, Справа: Дробь).
- Правый узел (Дробь $\frac{\sqcup}{\sqcup}$): Числитель 1, Знаменатель Сложение.
- Знаменатель (Сложение $\sqcup + \sqcup$): Слева 1, Справа Возведение в степень.
- Правый узел Сложения (Степень $\sqcup^{\sqcup}$): Основание $e$, Показатель Отрицание.
- Показатель (Отрицание $-\sqcup$): Операнд $x$.

**Ex6.** 1) $div(a, b)$. 2) $pow(a, b)$. 3) $root(x, n)$.

**Ex7.** 1) $\cdot + ab - cd$. 2) $ab + cd - \cdot$.

**Ex8.** 1. $(a + \sin(\omega t)) \cdot y$;

2. $\int_0^{x^2} f(t)dt$ (Примечание: переменная интегрирования $t$ связана и обычно не подлежит подстановке, верхний предел $x$ свободен);

3. $P(g(z), y) \to Q(g(z))$.

**Ex9.** 1) $(f(u))^2$. 2) $\sin(2 \cdot f(u))$. 3) $D_{f(u)}$.

**Ex10.** $\sum_{k=0}^{\infty}(2k + 1)$. Результат — допустимая лексема.

**Ex11.** 1. Аргументы: векторы; Результат: скаляр (число).

2. Аргумент: вектор; Результат: скаляр (неотрицательное число).

3. Аргументы: множества; Результат: логическое значение (булево).

**Ex12.** 1) $V \times V \to S$. 2) $V \times V \to V$. 3) $S \times V \to V$. 4) $V \to S$.

**Ex13.** 1) Корень: $+$. Потомки: $\sin x$ и $y$. (Стандартное соглашение). 2) Корень: sin. Потомок: $x + y$.

**Ex14.** $(1, (2, (3, ())))$.

**Ex15.** $\overline{x}$, $x'$, $\hat{x}$.

**Ex16.** 1) Переменная (Терм). 2) Формула. 3) Связка. 4) Формула (Свертка).

**Ex17.** $((\neg A) \wedge B) \to C$.

**Ex18.** Переименование: $t$: $\int_a^b t^2 dt$. Смысл не меняется (фиктивная переменная). $a$: $\int_a^b a^2 da$. Смысл меняется! Коллизия с пределом интегрирования $a$.

**Ex19.** Лексема построена с использованием следующей иерархии шаблонов:

- Уровень 1 (Корень): Шаблон суммирования $\sum_{\sqcup}^{\sqcup}\sqcup$.
- Уровень 2 (Нижнее знакоместо): Шаблон равенства $\sqcup = \sqcup$ (объединяющий жесткие графемы $i$ и 1).
- Уровень 2 (Главное знакоместо): Шаблон степени $\sqcup^{\sqcup}$.
- Уровень 3 (Основание степени): Шаблон индекса $\sqcup_{\sqcup}$ (объединяющий жесткие графемы $x$ и $i$).
- Листья (Жесткие графемы): $i, 1, n, x, 2$.

# Глава D2

**Ex1.** Определим формулу $\Phi = (P \to E) \lor (L \to F)$. Раскроем импликации, используя эквивалентность $A \to B \equiv \neg A \lor B$:

$$\Phi \equiv (\neg P \lor E) \lor (\neg L \lor F).$$

Используя ассоциативность и коммутативность дизъюнкции, перегруппируем члены, чтобы они соответствовали посылкам:

$$\Phi \equiv (\neg P \lor F) \lor (\neg L \lor E).$$

Напомним, что $\neg P \lor F \equiv P \to F$ и $\neg L \lor E \equiv L \to E$. Так как обе посылки $(P \to F)$ и $(L \to E)$ даны как Истинные, их дизъюнкция также Истинна.

*Комментарий:* Этот парадокс иллюстрирует, что материальная импликация не требует причинно-следственной связи. Даже если «Париж влечет Англию» и «Лондон влечет Францию» звучит ложно по отдельности, их дизъюнкция логически необходима при данных посылках, потому что по крайней мере одно из условий антецедента ($P$ или $L$) должно быть ложным, или консеквенты ($E$ или $F$) истинными, таким образом, что делает логическую структуру верной.[18]

**Ex2.** 1. $\varphi(t) \to \exists x \varphi(x)$ есть Аксиома ($\exists$).

2. Примените MP к гипотезе $\varphi(t)$ и аксиоме.

**Ex3.** 1. Гипотеза: $\forall x(\varphi \to \psi)$.

2. $\varphi(a) \to \psi(a)$ (Аксиома $\forall$).

3. Гипотеза: $\forall x \varphi$.

4. $\varphi(a)$ (Аксиома $\forall$).

5. $\psi(a)$ (MP из 2 и 4).

6. $\forall x \psi(x)$ (Gen).

7. Результат по Теореме о дедукции.

**Ex4.** 1. ($\to$): Предположим $\forall x(\varphi \land \psi)$. Тогда $\varphi(a) \land \psi(a)$. Тогда $\varphi(a)$ и $\psi(a)$. Обобщим (Правило Бернайса R1') до $\forall x \varphi$ и $\forall x \psi$.

2. ($\leftarrow$): Предположим $\forall x \varphi \land \forall x \psi$. Тогда $\varphi(a)$ и $\psi(a)$. Тогда $\varphi(a) \land \psi(a)$. Обобщим.

**Ex5.** Аналогично предыдущему. Используйте эквивалентность $\exists x \chi \leftrightarrow \neg \forall x \neg \chi$ и законы Де Моргана.

**Ex6.** Используйте разбор случаев по $\forall y \varphi(y) \lor \neg \forall y \varphi(y)$. Случай 1: Если $\forall y \varphi(y)$ истинно, то для любого $x$, $\varphi(x) \to \forall y \varphi(y)$ истинно. Значит $\exists x(\dots)$ истинно. Случай 2: Если $\neg \forall y \varphi(y)$, то $\exists x \neg \varphi(x)$. Пусть $x_0$ таков, что $\neg \varphi(x_0)$. Тогда $\varphi(x_0) \to \dots$ истинно (Ложь $\to$ Что угодно). Значит $\exists x(\dots)$ истинно.

**Ex7.** 1. ($\to$): Предположим $\varphi \to \forall x \psi(x)$ и $\varphi$. Тогда $\forall x \psi(x)$, значит $\psi(a)$. Так как $a$ произвольно и нет в $\varphi$, получаем $\varphi \to \psi(a)$, затем $\forall x(\varphi \to \psi(x))$.

[18] Этот вывод сильно зависит от Закона исключенного третьего. В интуиционистской логике, которая требует конструктивных доказательств, это утверждение не может быть выведено, так как мы не можем доказать ни одну из импликаций по отдельности.

2. ($\leftarrow$): Предположим $\forall x(\varphi \to \psi(x))$ и $\varphi$. Тогда $\varphi \to \psi(a)$, значит $\psi(a)$. Обобщим до $\forall x \psi(x)$.

**Ex8.** Используйте правило Бернайса (R1): если $\Gamma \vdash \varphi \to \psi(x)$ и $x$ не свободна в $\varphi$ (и $\Gamma$), то существует конечное $\Delta \subseteq \Gamma$ т.ч. $\Delta \vdash \varphi \to \psi(x)$, тогда используя $\gamma$ как конъюнкцию всех формул из $\Delta$, получаем по Т.Д., что $\vdash \gamma \wedge \varphi \to \psi(x)$, затем по правилу Бернайса (R1) следует, что $\vdash \gamma \wedge \varphi \to \forall x \psi(x)$, значит $\Delta \vdash \varphi \to \forall x \psi(x)$ и, следовательно $\Gamma \vdash \varphi \to \forall x \psi(x)$.

**Ex9.** Пусть $\exists x \forall y \varphi(x, y)$ Истинно в некоторой модели. Возьмем такой элемент $a$, что $\forall y \varphi(a, y)$ Истинно. Это означает, что для всех $b$ в этой модели $\varphi(a, b)$ Истинно. Значит, для всех $b$ существует $x$ (на самом деле $x = a$) т.ч. $\varphi(x, b)$ Истинно, т.е. $\exists x \varphi(x, b)$. И, вообще, $\forall y \exists x \varphi(x, y)$ в этой модели. Мы доказали, что $\exists x \forall y \varphi(x, y) \Vdash \forall y \exists x \varphi(x, y)$, и по теореме Гёделя о полноте получаем $\exists x \forall y \varphi(x, y) \vdash \forall y \exists x \varphi(x, y)$.

**Ex10.** $\forall x \forall y (x < y \to \exists z (x < z \wedge z < y))$ (Плотность). Истинно в $\mathbb{Q}$, ложно в $\mathbb{Z}$.

**Ex11.** 1. $\varphi(x, y) \equiv \exists z (z \neq 0 \wedge x + z = y)$. В $\mathbb{N}$, если $y > x$, разность $y - x$ существует и является натуральным числом.

2. Рассмотрим функцию $f : \mathbb{Z} \to \mathbb{Z}$, заданную как $f(x) = -x$. Так как $-(a + b) = (-a) + (-b)$, $f$ является автоморфизмом аддитивной группы. Однако, $f$ не сохраняет порядок: $1 < 2$, но $-1 > -2$. Таким образом, $<$ не может быть определено формулой, включающей только $+$.

**Ex12.** 1. $\varphi(x) \equiv \exists y (y \cdot y = x)$. В $\mathbb{R}$, число является квадратом тогда и только тогда, когда оно неотрицательно.

2. $x \leqslant y \iff \exists z (z \cdot z = y - x)$. (Так как $y - x \geqslant 0$).

**Ex13.** 1. Нет (автоморфизмы $\langle \mathbb{R}, < \rangle$ действуют транзитивно, напр., $x \mapsto x + c$).

2. Нет (по той же причине).

3. Нет.

(Примечание: В структуре чистого порядка без констант ни один индивидуальный элемент не определим).

**Ex14.** Это следует из $\aleph_0$-категоричности $\mathrm{DLO}_\infty$.

**Ex15.** 1. Поле алгебраических чисел $\mathbb{A}$ (множество всех корней многочленов с рациональными коэффициентами). Оно счетно и алгебраически замкнуто.

2. По Теореме Лёвенгейма-Сколема (вверх). Так как PA имеет бесконечную модель $\mathbb{N}$, она должна иметь модели любой бесконечной мощности $\kappa > \aleph_0$.

**Ex16.** Стандартная модель $\mathbb{N}$ и модель $\mathbb{N} + \mathbb{Z}$ (натуральные числа, за которыми следует копия целых) обе счетны, но не изоморфны (во второй некоторые элементы имеют предшественников, но недостижимы из 0). Таким образом, теория не категорична в мощности $\aleph_0$.

**Ex17.** $a < b$: $\mathrm{DLO} \vdash \exists x (a < x \wedge x < b) \leftrightarrow (a < b)$ (плотность и транзитивность).

**Ex18.** $b \leqslant a$: $\mathrm{DLO} \vdash \forall x (a < x \to b < x) \leftrightarrow (b \leqslant a)$ (связность и транзитивность).

**Ex19.** $\top$ (Истина). Так как область бесконечна, мы всегда можем найти $x$, отличный от любых двух фиксированных элементов $a$ и $b$.

**Ex20.** Условие есть $(a = 0 \land b > 0) \lor (a \neq 0)$. Если $a = 0, b > 0$, $0x + b > 0$ есть $b > 0$ (Истинно для всех $x$, значит $\exists$ Истинно). Если $a = 0, b \leqslant 0$, $0 > 0$ (Ложно). Если $a \neq 0$, прямая $y = ax + b$ пересекает ноль, так что есть область, где она положительна. Упрощенная бескванторная форма: $(a \neq 0) \lor (b > 0)$.

**Ex21.** $(a = 0 \land b = 0 \land c = 0) \lor (a \neq 0 \land b^2 - 4ac \geqslant 0) \lor (a = 0 \land b \neq 0)$. (По сути: либо тождество $0 = 0$, либо квадратное ур-ние имеет вещественные корни, либо линейное ур-ние имеет корень).

**Ex22.** Проверим условия критерия Лося—Воота:

1. *Нет конечных моделей:* Аксиомы требуют бесконечных классов, поэтому область должна быть бесконечной.
2. $\aleph_0$*-категоричность:* Пусть $\mathcal{M}$ — любая счетная модель $T$. Её область $M$ разбита на два класса, $C_1$ и $C_2$. Так как $\mathcal{M}$ счетна и $C_1, C_2$ бесконечные подмножества, $|C_1| = \aleph_0$ и $|C_2| = \aleph_0$. Любая другая счетная модель $\mathcal{M}'$ будет аналогично иметь классы $C_1', C_2'$ мощности $\aleph_0$. Мы можем построить биекцию $f : M \to M'$, которая отображает $C_1$ в $C_1'$ и $C_2$ в $C_2'$. Так как структура определена исключительно отношением эквивалентности, такая биекция является изоморфизмом.

Заключение: $T$ непротиворечива, не имеет конечных моделей и категорична в мощности $\aleph_0$. Следовательно, $T$ полна.

# Глава D3

**Ex1.** 1. $a + S(0) = S(a + 0)$ (PA5). 2. $a + 0 = a$ (PA5). 3. $S(a + 0) = S(a)$ (Конгруэнтность). 4. $a + S(0) = S(a)$ (Транзитивность).

**Ex2.** $x \cdot S(0) = x \cdot 0 + x = 0 + x = x$ (PA6).

**Ex3.** $a < b \iff \exists x(b = a + Sx) \iff \exists x(b = S(a + x))$. По Лемме D3.1, $x = 0 \lor \exists y(x = Sy)$. Если $x = 0$, $b = S(a) \implies S(a) \leqslant b$. Если $x = Sy$, $b = S(a) + Sy \implies S(a) < b$. В обоих случаях $S(a) \leqslant b$.

**Ex4.** Мы доказываем $S(a) + b = S(a + b)$ индукцией по $b$.

▶ *Базовый случай ($b = 0$):* Проверяем равенство $S(a) + 0 = S(a + 0)$.

- Левая часть: Рассмотрим терм $S(a) + 0$. По аксиоме PA5 $(\forall x(x + 0 = x))$, подставляя терм $S(a)$ вместо $x$, получаем $S(a) + 0 = S(a)$.
- Правая часть: Рассмотрим терм $S(a + 0)$. По аксиоме PA5, имеем $a + 0 = a$. По аксиоме PA2 $(x = y \to S(x) = S(y))$, применяя $S$ к обеим сторонам, получаем $S(a + 0) = S(a)$.

Так как обе части сводятся к $S(a)$, равенство выполняется.

▶ *Индуктивный шаг ($b \to Sb$):* Предположим гипотезу $S(a) + b = S(a + b)$. Мы должны доказать $S(a) + Sb = S(a + Sb)$.

- Левая часть: Рассмотрим $S(a) + Sb$. По аксиоме PA5 $(\forall x, y(x + Sy = S(x + y)))$ с $x = S(a), y = b$, имеем $S(a) + Sb = S(S(a) + b)$. Используя индуктивную гипотезу $(S(a) + b = S(a + b))$ и аксиому PA2, заменяем внутренний терм: $S(S(a) + b) = S(S(a + b))$.

– Правая часть: Рассмотрим $S(a + Sb)$. По аксиоме PA5 ($a + Sb = S(a + b)$) и применяя PA2 к этому равенству, получаем $S(a + Sb) = S(S(a + b))$.

Обе части равны $S(S(a + b))$.

**Ex5.** Случай $b < a$: $a \dot{-} b = c \implies b + c = a$. $c \leqslant a$. Случай $b \geqslant a$: $a \dot{-} b = 0 \leqslant a$. Для эквивалентности: если $a \dot{-} b = a$, то в случае $b < a$, $b + a = a \implies b = 0$. В случае $b \geqslant a$, $0 = a$, значит $a = 0$.

**Ex6.** $(a \dot{-} b) + b = a$ выполняется тогда и только тогда, когда мы в случае $b < a$ (где $b + c = a$) или в случае, где результат 0 и $a = b$. Если $b > a$, $0 + b \neq a$. Значит $b \leqslant a$.

**Ex7.** $x = (a + b) \dot{-} a$. Так как $a + b \geqslant a$, $x$ — единственное число, такое что $a + x = a + b$, что есть $b$.

**Ex8.** Случай $b + c \geqslant a$: левая часть 0. Правая часть $(a \dot{-} b) \dot{-} c$: если $b \geqslant a$, то $0 \dot{-} c = 0$. Если $b < a$, то пусть $k = a \dot{-} b$, $b + k = a$. $b + c \geqslant b + k \implies c \geqslant k$. Значит $k \dot{-} c = 0$. Случай $b + c < a$: левая часть есть $x$ т.ч. $b + c + x = a$. Правая часть: $b < a$, пусть $k = a \dot{-} b$ $(b + k = a)$. Так как $b + c < b + k$, $c < k$. Тогда $(a \dot{-} b) \dot{-} c = k \dot{-} c = y$ т.ч. $c + y = k$. Подст: $b + (c + y) = a \implies (b + c) + y = a$. Единственно.

**Ex9.** Случай $c = 0$: $0 = 0$. Случай $a \leqslant b$: слева $c \cdot 0 = 0$, справа $ca \leqslant cb \implies 0$. Случай $a > b$: пусть $a = b + k$. Слева $ck$, справа $c(b + k) \dot{-} cb = (cb + ck) \dot{-} cb = ck$.

**Ex10.** Пусть $a \leqslant b$. Сравним $a \dot{-} c$ и $b \dot{-} c$. Случай $c \geqslant b$: оба 0. Случай $a \leqslant c < b$: слева 0, справа $> 0$. Случай $c < a$: $a = c + x, b = c + y$. $a \leqslant b \implies c + x \leqslant c + y \implies x \leqslant y$.

**Ex11.** Пусть $a \leqslant b$. Сравним $c \dot{-} b$ и $c \dot{-} a$. Случай $c \leqslant a$: оба 0. Случай $a < c \leqslant b$: слева 0, справа $> 0$. Случай $c > b$: $c = b + x, c = a + y$. $b + x = a + y$. Так как $a \leqslant b$, $y \geqslant x$.

**Ex12.** $R(a, b, r) \overset{\text{def}}{\leftrightarrow} r < b \wedge \exists q(a = b \cdot q + r)$.

**Ex13.** Если $a = 0$, то $a \mid b \implies b = 0$, так что $a = b$. Если $a \neq 0$, то $b \neq 0$ (так как $b \mid a$). $a = kb, b = ma \implies a = kma$. Сократим $a$: $km = 1 \implies k = 1, m = 1$. Таким образом $a = b$.

**Ex14.** Нам нужно $12s - 18t = \gcd(12, 18) = 6$. Решение $s = 2, t = 1$ $(24 - 18 = 6)$.

**Ex15.** 1) $m_0 = 1 + 1 \cdot 3 = 4$, $\beta = \mathrm{rem}(10, 4) = 2$; 2) $m_1 = 1 + 2 \cdot 3 = 7$, $\beta = \mathrm{rem}(10, 7) = 3$; 3) $m_2 = 1 + 3 \cdot 3 = 10$. $\beta = \mathrm{rem}(10, 10) = 0$.

**Ex16.** 1) $m_0 = 1 + (0 + 1)2 = 3$, $\beta = \mathrm{rem}(13, 3) = 1$; 2) $m_1 = 1 + (1 + 1)2 = 5$, $\beta = \mathrm{rem}(13, 5) = 3$.

Последовательность есть $\langle 1, 3 \rangle$.

**Ex17.** Нужно $c \equiv 1 \pmod{1 + d}$, $c \equiv 2 \pmod{1 + 2d}$. Пробуем $d = 1$: модули 2, 3. $c \equiv 1 \pmod 2, c \equiv 2 \pmod 3 \implies c = 5$. Пара $(5, 1)$.

**Ex18.** Если $(c, d)$ подходит, то $(c + K \cdot \mathrm{lcm}(m_i), d)$ тоже подходит для любого $K$.

**Ex19.** Положительные числа $\langle 0, n \rangle$, отрицательные $\langle n, 0 \rangle$. $5 \to \langle 0, 5 \rangle$. $-3 \to \langle 3, 0 \rangle$.

**Ex20.** $\langle 0, 5 \rangle +_{\mathbb{Z}} \langle 3, 0 \rangle$. Случай $a_1 = b_2 = 0$: результат $\langle 0, a_2 \dot{-} b_1 \rangle = \langle 0, 5 \dot{-} 3 \rangle = \langle 0, 2 \rangle$ (что соответствует 2).

**Ex21.** $\langle 0, 2 \rangle +_{\mathbb{Z}} \langle 5, 0 \rangle$. Случай $a_1 = b_2 = 0$: результат $\langle b_1 \dot{-} a_2, 0 \rangle$ (так как $b_1 > a_2$) $= \langle 5 \dot{-} 2, 0 \rangle = \langle 3, 0 \rangle$ (соответствует -3).

**Ex22.** $\langle 2, 0 \rangle \cdot_{\mathbb{Z}} \langle 3, 0 \rangle$. Случай «одинаковые знаки» $(a_2 = b_2 = 0)$. Результат $\langle 0, (a_1 + a_2)(b_1 + b_2) \rangle = \langle 0, (2 + 0)(3 + 0) \rangle = \langle 0, 6 \rangle$. (Положительное, $+6$).

**Ex23.** $\langle 0,3\rangle \cdot_{\mathbb{Z}} \langle 2,0\rangle$. Случай «разные знаки» (иначе). Результат $\langle (a_1+a_2)(b_1+b_2), 0\rangle = \langle (0+3)(2+0), 0\rangle = \langle 6, 0\rangle$. (Отрицательное, -6).

**Ex24.** 1. Любое доказуемо ложное предложение, например, $0 = S0$.

2. Любое доказуемо истинное предложение, например, $0 = 0$.

**Ex25.** 1. $\exists y\ (a = SSSSSSSSS0 \cdot y + SSSSSS0)$.

2. $0 = S0$. Оно ложно, и его код не оканчивается цифрой 6.

3. $0 = 0 \cdot (0+0)$. Оно истинно, и его код оканчивается цифрой 6.

**Ex26.** 1. $\neg\exists y\ (a = SSS0 \cdot y)$.

2. $0 + 0 = 0$. Его код равен 13141, что не делится на 3 (сумма цифр равна 10). Таким образом, $\varphi(\underline{13141})$ истинно, и предложение $0 + 0 = 0$ также истинно.

# Глава D4

**Ex1.** Двойственное: $(a \wedge b) \vee (a \wedge \neg b) = a$. Доказательство: $a \wedge (b \vee \neg b) = a \wedge 1 = a$. Истинно.

**Ex2.** 1. *Ноль/Один:* $\varnothing$ конечно, $X$ кофинитно (дополнение $\varnothing$). *Дополнение:* Если $S$ конечно, $S^c$ кофинитно. Если $S$ кофинитно, $S^c$ конечно. *Объединение:* - Конечное $\cup$ Конечное = Конечное. - Кофинитное $\cup$ Что угодно = Кофинитное (так как дополнение объединения есть пересечение дополнений: бесконечное $\cap$ конечное = конечное). Таким образом, $\mathscr{A}$ замкнуто относительно всех булевых операций.

2. Нет. Рассмотрим семейство синглтонов $\{\{x\} \mid x \in X\}$. Каждое в $\mathscr{A}$. Их бесконечное объединение есть $X$. Однако, пусть $X = \omega$ и возьмем объединение синглтонов всех четных чисел. Результат — множество четных чисел $E$. $E$ бесконечно, и его дополнение (нечетные) бесконечно. Значит $E \notin \mathscr{A}$.

3. Атомы — это в точности одноэлементные множества (синглтоны) $\{x\}$ для $x \in X$.

**Ex3.** Сначала проверим замкнутость. Пусть $e, f \in B$. $\neg e$: $(1-e)^2 = 1-2e+e^2 = 1-2e+e = 1-e$. (Замкнуто). $e \wedge f$: $(ef)^2 = e^2f^2 = ef$. (Замкнуто). $e \vee f$: Пусть $s = e+f-ef$. Тогда $s^2 = e^2+f^2+e^2f^2+2ef-2e^2f-2ef^2 = e+f+ef+2ef-2ef-2ef = e+f-ef = s$. (Замкнуто). Теперь проверим дистрибутивность (одну из них): $x \wedge (y \vee z) = x(y+z-yz) = xy + xz - xyz$. $(x \wedge y) \vee (x \wedge z) = xy + xz - (xy)(xz) = xy + xz - x^2yz = xy + xz - xyz$. Они совпадают. Другие аксиомы выполняются аналогично.

**Ex4.** 1. Нам нужно показать две вещи: $(a \to b) \in S$ и $\forall y \in S, y \leqslant (a \to b)$.

   - Подставим $x = (a \to b)$ в формулу адъюнкции. Так как $x \leqslant x$ всегда истинно (рефлексивность), эквивалентность дает $(a \to b) \wedge a \leqslant b$. Таким образом, $(a \to b) \in S$.
   - Пусть $y \in S$. Это означает $y \wedge a \leqslant b$. Используя формулу адъюнкции справа налево (подставляя $x = y$), немедленно получаем $y \leqslant (a \to b)$.

   Таким образом, $a \to b$ является наибольшим элементом $S$.

2. Мы покажем, что произвольный элемент $x$ меньше левой части тогда и только тогда, когда он меньше правой.

Анализ левой части: $x \leqslant (a \vee b) \to c$. По свойству адъюнкции, это эквивалентно:

$$x \wedge (a \vee b) \leqslant c.$$

Используя дистрибутивность пересечения относительно объединения:

$$(x \wedge a) \vee (x \wedge b) \leqslant c.$$

По *универсальному свойству объединения* (супремума), объединение меньше $c$ тогда и только тогда, когда оба операнда меньше $c$:

$$(x \wedge a \leqslant c) \quad \text{И} \quad (x \wedge b \leqslant c).$$

Анализ правой части: $x \leqslant (a \to c) \wedge (b \to c)$. По свойству пересечения (инфимума), $x$ меньше пересечения тогда и только тогда, когда он меньше каждого компонента:

$$x \leqslant (a \to c) \quad \text{И} \quad x \leqslant (b \to c).$$

Применим свойство адъюнкции к каждому неравенству отдельно:

$$(x \wedge a \leqslant c) \quad \text{И} \quad (x \wedge b \leqslant c).$$

Заключение: Так как условие «$x$ меньше левой части» сводится к той же логической конъюнкции, что и условие «$x$ меньше правой части», элементы определяют один и тот же нижний конус и должны быть равны.

**Ex5.** 1. Доказательство $\neg(x \vee y) = \neg x \wedge \neg y$: Напомним, что $\neg a = a \to 0$. По свойству импликации в алгебрах Гейтинга, $a \vee b \to c = (a \to c) \wedge (b \to c)$. Полагая $c = 0$, получаем:

$$(x \vee y) \to 0 = (x \to 0) \wedge (y \to 0).$$

По определению отрицания, это в точности $\neg(x \vee y) = \neg x \wedge \neg y$.

2. Контрпример для $\neg(x \wedge y) = \neg x \vee \neg y$: Рассмотрим топологическое пространство $\mathbb{R}$. Алгебра открытых множеств является алгеброй Гейтинга. Пусть $U = (-\infty, 0)$ и $V = (0, +\infty)$.

- $U \wedge V = U \cap V = \varnothing$. Значит $\neg(U \wedge V) = \neg\varnothing = \mathbb{R}$ (все пространство).
- $\neg U = \mathrm{Int}(\mathbb{R} \setminus (-\infty, 0)) = \mathrm{Int}([0, +\infty)) = (0, +\infty) = V$.
- Аналогично, $\neg V = U$.
- Правая часть есть $\neg U \vee \neg V = V \cup U = (-\infty, 0) \cup (0, +\infty) = \mathbb{R} \setminus \{0\}$.

Так как $\mathbb{R} \neq \mathbb{R} \setminus \{0\}$, равенство нарушается. Пробел «закона исключенного третьего» в 0 не позволяет объединению отрицаний покрыть все отрицание пересечения.

**Ex6.** 1. Пусть $x \in \mathscr{B}$. Если $x = 0$, множество атомов под ним пусто, и $\bigvee \varnothing = 0$. Если $x \neq 0$, пусть $y = \bigvee\{a \in A \mid a \leqslant x\}$. Очевидно $y \leqslant x$. Рассмотрим $z = x \wedge \neg y$. Если $z \neq 0$, то $z$ должен содержать атом $a_0$ (так как алгебра конечна). Тогда $a_0 \leqslant x$ и $a_0 \leqslant \neg y$. Так как $a_0$ — атом под $x$, он включен в объединение $y$, значит $a_0 \leqslant y$. Таким образом $a_0 \leqslant y \wedge \neg y = 0$, противоречие. Следовательно, $z = 0$, что влечет $x \leqslant y$. Поэтому $x = y$.

2. Отображение $\varphi(x) = \{a \in A \mid a \leqslant x\}$ сохраняет операции. $\varphi(x \wedge y) = \{a \mid a \leqslant x \wedge a \leqslant y\} = \varphi(x) \cap \varphi(y)$. Инъективность: Если $\varphi(x) = \varphi(y)$, то множества атомов под ними идентичны. По шагу 1, $x$ и $y$ суть объединения этих множеств, значит $x = y$. Сюръективность: Для любого подмножества $S \subseteq A$, пусть $x = \bigvee S$. Тогда $\varphi(x) = S$ (так как атомы дизъюнктны, атом $b$ находится под $\bigvee S$ тогда и только тогда, когда $b \in S$).

**Ex7.** 1. Инъекция $f : \mathbb{R} \to \mathbb{R}^2$ просто $x \mapsto \langle x, 0\rangle$.

2. Инъекция $g : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$. Сначала отобразим $\mathbb{R}$ в $(0,1)$ через гомеоморфизм. Достаточно отобразить $(0,1) \times (0,1)$ в $(0,1)$. Пусть $x = 0.a_1a_2a_3\ldots$ и $y = 0.b_1b_2b_3\ldots$. Чтобы избежать проблемы с девятками на конце, просто запретим их (используем только представления без бесконечных хвостов из 9). Определим $h(x,y) = 0.a_1b_1a_2b_2a_3b_3\ldots$. Это отображает две последовательности в одну. Это инъективно, так как позиция цифр уникальна. Полученное число находится в $(0,1)$. По теореме Кантора-Бернштейна-Шрёдера, $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$.

**Ex8.** Пусть $R$ — конечная область целостности и пусть $a \in R$ с $a \neq 0$. Рассмотрим функцию $\varphi_a : R \to R$, заданную как $\varphi_a(x) = ax$. Сначала покажем, что $\varphi_a$ инъективна. Предположим $\varphi_a(x) = \varphi_a(y)$. Тогда $ax = ay \implies a(x-y) = 0$. Так как $R$ — область целостности и $a \neq 0$, должно быть $x - y = 0$, значит $x = y$. Так как $R$ конечно, любая инъективная функция из $R$ в себя сюръективна (по Принципу Дирихле). Следовательно, 1 находится в образе $\varphi_a$. Это означает, что существует некоторое $b \in R$, такое что $ab = 1$. Таким образом, $a$ обратимо. Так как $a$ было произвольным, $R$ является полем.

**Ex9.** Пусть $S = \omega^{<\omega}$. Мы можем записать $S = \bigcup_{n\in\omega} \omega^n$, где $\omega^n$ — множество последовательностей длины $n$. Для $n = 1$, $|\omega| = \aleph_0$. Для любого $n$, если $|\omega^n| = \aleph_0$, то $|\omega^{n+1}| = |\omega^n \times \omega| = \aleph_0 \cdot \aleph_0 = \aleph_0$ (по индукции). Таким образом, $S$ — счетное объединение счетных множеств: $|S| = \sum_{n\in\omega} \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0$.

**Ex10.** 1. Множество многочленов степени $n$ с рациональными коэффициентами можно отождествить с $\mathbb{Q}^{n+1} \setminus \{\overline{0}\}$. Так как $\mathbb{Q}$ счетно, $\mathbb{Q}^{n+1}$ счетно. Множество всех многочленов $\mathscr{P} = \bigcup_{n\in\omega} \mathbb{Q}^{n+1}$ является счетным объединением счетных множеств, следовательно счетно. Каждый многочлен $P \in \mathscr{P}$ имеет конечное число корней. Таким образом, множество алгебраических чисел является объединением счетного семейства конечных множеств, что влечет $|\mathbb{A}| = \aleph_0$.

2. Так как $\mathbb{R}$ несчетно (Теорема Кантора) и $\mathbb{R} = \mathbb{A} \cup (\mathbb{R} \setminus \mathbb{A})$, если бы множество трансцендентных чисел $\mathbb{R} \setminus \mathbb{A}$ было счетным, то $\mathbb{R}$ было бы объединением двух счетных множеств, что невозможно. Значит, трансцендентные числа несчетны.

**Ex11.** База $\omega$: $1 + \omega = \sup_{n<\omega}(1+n) = \omega$. Шаг: $1 + (\alpha+1) = (1+\alpha)+1 = \alpha+1$. Предел: $1 + \lambda = \sup(1+\alpha) = \sup(\alpha) = \lambda$.

**Ex12.** 1. Лемма о росте ($\gamma \leqslant \omega^\gamma$): Используем трансфинитную индукцию по $\gamma$.

- *База:* $0 < 1 = \omega^0$.
- *Последователь:* Если $\gamma \leqslant \omega^\gamma$, то $\gamma + 1 \leqslant \omega^\gamma + 1$. Так как $\omega^\gamma \geqslant 1$, имеем $\omega^\gamma + 1 \leqslant \omega^\gamma + \omega^\gamma = \omega^\gamma \cdot 2 < \omega^\gamma \cdot \omega = \omega^{\gamma+1}$. Значит $\gamma + 1 < \omega^{\gamma+1}$.
- *Предел:* Если $\lambda$ — предельный ординал и $\forall \xi < \lambda (\xi \leqslant \omega^\xi)$, то $\lambda = \sup_{\xi<\lambda} \xi \leqslant \sup_{\xi<\lambda} \omega^\xi$. По непрерывности возведения в степень, правая часть есть $\omega^\lambda$. Значит $\lambda \leqslant \omega^\lambda$.

2. Степень (Логарифм): Пусть $\alpha > 0$. Рассмотрим $E = \{\gamma \in \mathrm{Ord} \mid \omega^\gamma \leqslant \alpha\}$. Из Леммы о росте, для любого $\gamma$, если $\omega^\gamma \leqslant \alpha$, то $\gamma \leqslant \omega^\gamma \leqslant \alpha$. Значит $E \subseteq \alpha + 1$, так что $E$ — множество. Пусть $\beta_1 = \sup E$. Так как возведение в степень непрерывно и строго возрастает:

   - Если $\beta_1 \in E$, то $\omega^{\beta_1} \leqslant \alpha$.
   - Если $\beta_1 \notin E$ (предельный случай), то $\omega^{\beta_1} = \sup_{\gamma \in E} \omega^\gamma \leqslant \alpha$.

   Таким образом $\omega^{\beta_1} \leqslant \alpha$. Однако, $\beta_1 + 1 > \beta_1$, поэтому $\beta_1 + 1 \notin E$ (иначе $\sup E$ был бы больше). Следовательно, $\omega^{\beta_1+1} > \alpha$. Мы нашли уникальное $\beta_1$, такое что $\omega^{\beta_1} \leqslant \alpha < \omega^{\beta_1+1}$.

3. Основное доказательство (Индукция по $\alpha$): Предположим, теорема верна для всех $\delta < \alpha$. Найдем степень $\beta_1$ для $\alpha$, как в шаге 2. По Теореме о делении, разделим $\alpha$ на $\omega^{\beta_1}$:

$$\alpha = \omega^{\beta_1} \cdot k + \delta, \quad \text{где } \delta < \omega^{\beta_1}.$$

   *Анализ k:* Так как $\alpha < \omega^{\beta_1+1} = \omega^{\beta_1} \cdot \omega$, частное $k$ должно быть меньше $\omega$. Так как $\alpha \geqslant \omega^{\beta_1}$, $k \geqslant 1$. *Анализ δ:* Так как $\delta < \omega^{\beta_1} \leqslant \alpha$, имеем $\delta < \alpha$.

   - Если $\delta = 0$, $\alpha = \omega^{\beta_1} \cdot k$, и мы закончили.
   - Если $\delta > 0$, по индуктивной гипотезе, $\delta$ имеет НФК: $\delta = \omega^{\gamma_1} c_1 + \dots$. Старший член $\omega^{\gamma_1}$ должен удовлетворять $\omega^{\gamma_1} \leqslant \delta$. Так как $\delta < \omega^{\beta_1}$, имеем $\omega^{\gamma_1} < \omega^{\beta_1}$, что влечет $\gamma_1 < \beta_1$. Таким образом, приписывание разложения $\delta$ к $\omega^{\beta_1} \cdot k$ сохраняет строго убывающий порядок степеней.

   Единственность следует из единственности степени $\beta_1$ и единственности частного/остатка.

**Ex13.** 1. Сложение не коммутативно. $\alpha + \beta = (\omega^\omega + \omega \cdot 2 + 1) + (\omega^\omega + \omega) = \omega^\omega + (\omega \cdot 2 + 1 + \omega^\omega) + \omega$. Так как $1 + \omega^\omega = \omega^\omega$ и $\omega \cdot 2 + \omega^\omega = \omega^\omega$, получаем $\omega^\omega + \omega^\omega + \omega = \omega^\omega \cdot 2 + \omega$. $\beta + \alpha = (\omega^\omega + \omega) + (\omega^\omega + \omega \cdot 2 + 1) = \omega^\omega \cdot 2 + \omega \cdot 2 + 1$.

2. Умножение: $\alpha \cdot 2 = (\omega^\omega + \dots) \cdot 2 = \omega^\omega \cdot 2 + \omega \cdot 2 + 1$. (Дистрибутивность работает слева, но здесь мы умножаем порядковый тип). На самом деле, $(\omega^\omega + \delta) \cdot 2 = \omega^\omega \cdot 2 + \delta$. $\beta \cdot \omega = (\omega^\omega + \omega) \cdot \omega = \omega^\omega \cdot \omega = \omega^{\omega+1}$. (Младшие члены поглощаются).

**Ex14.** 1. $n_1 = 2^k = p_1^k$. Индекс равен 1. Показатель $\omega$ равен $1 - 1 = 0$.

$$c(2^k) = \omega^0 \cdot k = k.$$

$n_2 = 3^k = p_2^k$. Индекс равен 2. Показатель $\omega$ равен $2 - 1 = 1$.

$$c(3^k) = \omega^1 \cdot k = \omega \cdot k.$$

$n_3 = 2^k 3^j 5^t = p_1^k p_2^j p_3^t$. Упорядочиваем индексы по убыванию: $3, 2, 1$.

$$c(2^k 3^j 5^t) = \omega^{3-1} \cdot t + \omega^{2-1} \cdot j + \omega^{1-1} \cdot k = \omega^2 \cdot t + \omega \cdot j + k.$$

2. Отображение переводит разложение на простые множители в Нормальную форму Кантора, где показатели — натуральные числа. Так как можно сформировать любой конечный набор натуральных показателей и коэффициентов, образ покрывает все ординалы ниже $\omega^\omega$.

**Ex15.** 1. Сначала вспомним базовые значения: $o(1) = 0$, поэтому для индекса 1 ($p_1 = 2$), показатель $o(1) = 0$. Для индекса 2 ($p_2 = 3$), показатель $o(2) = \omega^0 \cdot 1 = 1$. Для индекса 3 ($p_3 = 5$), показатель $o(3) = \omega^{o(2)} \cdot 1 = \omega^1 = \omega$.

$n_1 = 2^k$: индекс 1.

$$o(2^k) = \omega^{o(1)} \cdot k = \omega^0 \cdot k = k.$$

$n_2 = 3^k$: индекс 2.

$$o(3^k) = \omega^{o(2)} \cdot k = \omega^1 \cdot k = \omega \cdot k.$$

$n_3 = 2^k 3^j 5^t$: индексы 1, 2, 3.

$$o(2^k 3^j 5^t) = \omega^{o(3)} \cdot t + \omega^{o(2)} \cdot j + \omega^{o(1)} \cdot k = \omega^\omega \cdot t + \omega \cdot j + k.$$

2. Вычисление последовательности $h_n$: $h_0 = 1$. $h_1 = p_{h_0} = p_1 = 2$. $h_2 = p_{h_1} = p_2 = 3$. $h_3 = p_{h_2} = p_3 = 5$. $h_4 = p_{h_3} = p_5 = 11$. (Примечание: $h_5 = p_{11} = 31$).

3. Ординальные значения: $o(h_0) = o(1) = 0$. $o(h_1) = o(2) = \omega^{o(1)} = \omega^0 = 1$. $o(h_2) = o(3) = \omega^{o(2)} = \omega^1 = \omega$. $o(h_3) = o(5) = \omega^{o(3)} = \omega^\omega$. $o(h_4) = o(11) = \omega^{o(5)} = \omega^{\omega^\omega}$. В общем виде, $o(h_{n+1}) = \omega^{o(h_n)}$.

4. Пусть $\alpha_n = o(h_n)$. Имеем рекуррентность $\alpha_0 = 0$, $\alpha_{n+1} = \omega^{\alpha_n}$. Последовательность строго возрастает. Её предел $\lambda = \sup \alpha_n$ должен удовлетворять $\lambda = \sup \omega^{\alpha_n}$. По непрерывности возведения в степень, $\sup \omega^{\alpha_n} = \omega^{\sup \alpha_n} = \omega^\lambda$. Таким образом, $\lambda = \omega^\lambda$. Ординал $\varepsilon_0$ определяется как *наименьшая* неподвижная точка отображения $\xi \mapsto \omega^\xi$. Так как наша последовательность начинается с 0, она сходится к наименьшей неподвижной точке. Значит $\lambda = \varepsilon_0$.

**Ex16.** $\aleph_1 + \aleph_0 \cdot \aleph_1 = \aleph_1 + \aleph_1 = \aleph_1$.

**Ex17.** 1. $\kappa$ (поглощение).

2. $\kappa$ (так как $3 \leqslant \kappa$).

3. $2^\kappa$ (так как $(\kappa^2)^\kappa = \kappa^\kappa = 2^\kappa$).

**Ex18.** 1. $|V_0| = 0$, $|V_1| = 1$, $|V_2| = 2$, $|V_3| = 2^2 = 4$. (В общем случае $|V_{n+1}| = 2^{|V_n|}$ для конечных $n$, тетрация).

2. Индукция. $V_0$ транзитивно. Если $V_\alpha$ транзитивно, то для любого $x \in V_{\alpha+1} = \mathscr{P}(V_\alpha)$, $x \subseteq V_\alpha$. Если $y \in x$, то $y \in V_\alpha$. Так как $V_\alpha$ транзитивно, $y \subseteq V_\alpha$, поэтому $y \in \mathscr{P}(V_\alpha) = V_{\alpha+1}$.

3. Доказательство трансфинитной индукцией по $\alpha$: Нам нужно показать, что $\forall x (x \in V_\alpha \to \operatorname{rank}(x) < \alpha)$.

- *Базовый случай:* $\alpha = 0$. $V_0 = \varnothing$, поэтому посылка $x \in V_0$ ложна для любого $x$. Импликация выполняется тривиально.
- *Предельный шаг:* Пусть $\alpha = \lambda$ — предельный ординал. По определению, $V_\lambda = \bigcup_{\gamma<\lambda} V_\gamma$. Если $x \in V_\lambda$, то существует некоторое $\gamma < \lambda$, такое что $x \in V_\gamma$. По индуктивной гипотезе для $\gamma$, имеем $\operatorname{rank}(x) < \gamma$. Так как $\gamma < \lambda$, следует, что $\operatorname{rank}(x) < \lambda$.
- *Шаг последователя:* Пусть $\alpha = \beta + 1$. По определению, $V_{\beta+1} = \mathscr{P}(V_\beta)$. Если $x \in V_{\beta+1}$, то $x \subseteq V_\beta$. Значит, $\operatorname{rank}(x) \leqslant \beta < \alpha$.

**Ex19.** *Часть 1:* $\rho(x) \leqslant \mathrm{rank}(x)$. Пусть $\mathrm{rank}(x) = \alpha$. По определению, $x \subseteq V_\alpha$. Это означает, что для каждого $y \in x$, $y \in V_\alpha$. Свойство иерархии таково, что $y \in V_\alpha \implies R(y) < \alpha$. (Доказательство: если $y \in V_\alpha$, то $y \in \mathscr{P}(V_\gamma)$ для некоторого $\gamma < \alpha$ или их объединения, что влечет $y \subseteq V_\gamma$, поэтому $\mathrm{rank}(y) \leqslant \gamma < \alpha$). Таким образом, для всех $y \in x$, $\mathrm{rank}(y) < \alpha$. Предполагая по индукции, что $\rho(y) = \mathrm{rank}(y)$, имеем $\rho(y) < \alpha$. Следовательно, $\rho(y) + 1 \leqslant \alpha$. Беря супремум по всем $y \in x$, получаем $\rho(x) \leqslant \alpha = \mathrm{rank}(x)$.

*Часть 2:* $\mathrm{rank}(x) \leqslant \rho(x)$. Пусть $\rho(x) = \alpha$. По определению супремума, для всех $y \in x$, $\rho(y) + 1 \leqslant \alpha$, что влечет $\rho(y) < \alpha$. По индукции, $\mathrm{rank}(y) < \alpha$. Это влечет $y \subseteq V_{\mathrm{rank}(y)}$. Так как $V_\xi$ кумулятивно, $V_{\mathrm{rank}(y)} \subseteq V_\gamma$ для любого $\gamma \geqslant \mathrm{rank}(y)$. Также, $y \subseteq V_{\mathrm{rank}(y)} \implies y \in V_{\mathrm{rank}(y)+1}$. Так как $\mathrm{rank}(y) < \alpha$, имеем $\mathrm{rank}(y) + 1 \leqslant \alpha$. Значит $y \in V_{\mathrm{rank}(y)+1} \subseteq V_\alpha$. Итак, для всех $y \in x$, $y \in V_\alpha$. Это означает $x \subseteq V_\alpha$. По определению $\mathrm{rank}(x)$ как минимального такого ординала, $\mathrm{rank}(x) \leqslant \alpha = \rho(x)$.

**Ex20.** *1. На основе образа → На основе сужения.* Это направление прямое. Так как образ $G[\alpha]$ — это просто область значений сужения $G \restriction \alpha$, любая зависимость от образа может быть выражена как зависимость от сужения: $\Psi(h) = \Phi(\mathrm{ran}(h))$.

*2. На основе сужения → На основе образа.* Пусть функция $F$ определена генератором $\Psi$: $F(\alpha) = \Psi(F \restriction \alpha)$. Построим вспомогательную функцию $G(\alpha) = \langle \alpha, F(\alpha) \rangle$. Заметим, что образ $G[\alpha] = \{\langle \beta, F(\beta) \rangle \mid \beta < \alpha\}$ есть в точности множество пар, составляющих функцию $f = F \restriction \alpha$. Из множества $f$ мы можем восстановить ординал $\alpha$ (как множество первых компонент, т.е. область определения) и значение $\Psi(f)$. Таким образом, мы можем определить генератор $\Phi$ для $G$, такой что $\Phi(S) = \langle \mathrm{dom}(S), \Psi(S) \rangle$, где $S$ рассматривается как отношение. Тогда $G(\alpha) = \Phi(G[\alpha])$ определено чисто рекурсией по образу. Наконец, $F(\alpha)$ получается взятием второй проекции $G(\alpha)$. Заключение: Схемы определяют один и тот же класс функций (с точностью до кодирования).

**Ex21.** 1. Предположим $f : \mathbb{Q} \to \alpha$ — порядковый изоморфизм. Возьмем любой $q \in \mathbb{Q}$. Так как $\mathbb{Q}$ не имеет минимального элемента (простирается до $-\infty$), существует $r < q$. Тогда $f(r) < f(q)$. Мы можем построить бесконечную убывающую последовательность $q_0 > q_1 > q_2 > \dots$ в $\mathbb{Q}$. Она отображается в бесконечную убывающую последовательность ординалов $f(q_0) > f(q_1) > \dots$, что противоречит фундированности ординалов.

2. *Построение методом «челнока» (back-and-forth).* Пусть $A = \{a_0, a_1, \dots\}$ и $B = \{b_0, b_1, \dots\}$ — два счетных плотных линейных порядка без концевых точек. Мы строим последовательность частичных изоморфизмов $p_n : A_n \to B_n$, где $A_n, B_n$ — конечные подмножества. *Этап 0:* Пусть $p_0 = \varnothing$. *Этап n (четный):* Выберем первый элемент $a \in A$, не входящий в $\mathrm{dom}(p_n)$. Мы должны отобразить его в некоторый $b \in B$, сохраняя порядок относительно уже отображенных элементов. Так как $B$ плотно и не имеет концов, такой $b$ всегда существует (в соответствующем интервале). Определим $p_{n+1} = p_n \cup \{\langle a, b \rangle\}$. *Этап n (нечетный):* Выберем первый элемент $b \in B$, не входящий в $\mathrm{ran}(p_n)$. Найдем прообраз $a \in A$, сохраняя порядок (возможно из-за плотности/отсутствия концов у $A$). Определим $p_{n+1} = p_n \cup \{\langle a, b \rangle\}$. Объединение $P = \bigcup p_n$ является требуемым изоморфизмом.

# ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

## Л



## М



## Н



## О



## П

## Р



## С



## Т



## У



## Ф



## Ц



## Ч

## Ш



## Э



## Я

# СПИСОК ОБОЗНАЧЕНИЙ

| | |
|---|---|
| $\mathfrak{Math}$ | Неформальный язык математики (предмет этой книги) |
| $\neg\varphi$ | Отрицание формулы $\varphi$ |
| $\varphi \wedge \psi$ | Конъюнкция («И») |
| $\varphi \vee \psi$ | Дизъюнкция («ИЛИ») |
| $\varphi \to \psi$ | Импликация («ЕСЛИ..., ТО...») |
| $\varphi \leftrightarrow \psi$ | Эквиваленция («тогда и только тогда») |
| $\varphi \equiv \psi$ | Формулы $\varphi$ и $\psi$ равносильны |
| $\vdash$ | Синтаксическая выводимость (доказуемость) |
| $\Vdash$ | Семантическое (логическое) следование |
| $\models$ | Отношение истинности в модели |
| $\top$ | Тождественная истина |
| $\bot$ | Тождественная ложь |
| $\overset{\text{def}}{\rightleftharpoons}$ | Равенство по определению |
| $\overset{\text{def}}{\leftrightarrow}$ | Равносильность по определению |
| $\mathrm{Th}(\mathscr{M})$ | Полная (элементарная) теория модели $\mathscr{M}$ |
| $\mathrm{Pr}(n, m)$ | Предикат доказуемости: формула с кодом $n$ имеет доказательство с кодом $m$ |
| $\mathrm{Con}(T)$ | Формула, выражающая непротиворечивость теории $T$ |
| $\ulcorner\gamma\urcorner$ | Геделев номер выражения $\gamma$ |
| PA | Арифметика Пеано |
| Q | Арифметика Робинсона |
| ZF | Теория множеств Цермело–Френкеля |
| ZFC | Теория множеств Цермело–Френкеля с аксиомой выбора |
| HF | Теория наследственно-конечных множеств |
| AC | Аксиома выбора (общая) |

| | |
|---|---|
| $\mathrm{AC}_{\omega}$ | Аксиома счетного выбора |
| $\mathrm{AC}_{\omega}^{fin}$ | Аксиома счетного выбора из конечных множеств |
| ZT | Теорема Цермело |
| ZL | Лемма Цорна |
| CH | Континуум-гипотеза Кантора |
| GB | Теория множеств Гёделя–Бернайса |
| $\forall x\ \varphi(x)$ | Квантор всеобщности: для любого $x$ истинно $\varphi(x)$ |
| $\exists x\ \varphi(x)$ | Квантор существования: существует $x$ такой, что $\varphi(x)$ |
| $\exists! x\ \varphi(x)$ | Существует единственный $x$ такой, что $\varphi(x)$ |
| $\forall x \in A:\ \varphi(x)$ | Ограниченный квантор всеобщности в теории множеств |
| $\exists x \in A:\ \varphi(x)$ | Ограниченный квантор существования в теории множеств |
| $\forall x < k:\ \varphi(x)$ | Ограниченный квантор всеобщности в арифметике |
| $\exists x < k:\ \varphi(x)$ | Ограниченный квантор существования в арифметике |
| $\forall \alpha:\ \varphi(\alpha)$ | Для любого ординала $\alpha$ истинно $\varphi(\alpha)$ |
| $\exists \alpha:\ \varphi(\alpha)$ | Существует ординал $\alpha$ такой, что $\varphi(\alpha)$ |
| $\varnothing, \{\}$ | Пустое множество |
| $a \in b$ | $a$ является элементом множества $b$ |
| $a \notin b$ | Отрицание $a \in b$ |
| $A \subseteq B$ | Множество $A$ является подмножеством $B$ |
| $A \subsetneq B$ | Множество $A$ является собственным подмножеством $B$ |
| $\{a, b, \dots, c\}$ | Множество, состоящее из элементов $a, b, \dots, c$ |
| $\{x \mid \varphi(x)\}$ | Множество всех $x$, удовлетворяющих свойству $\varphi(x)$ |
| $A \cup B$ | Объединение множеств $A$ и $B$ |
| $A \cap B$ | Пересечение множеств $A$ и $B$ |
| $\bigcup A$ | Объединение всех элементов множества $A$ |
| $\bigcap A$ | Пересечение всех элементов множества $A$ |
| $A \setminus B$ | Разность множеств $A$ и $B$ |
| $A \triangle B$ | Симметрическая разность множеств $A$ и $B$ |
| $\mathscr{P}(A)$ | Множество всех подмножеств $A$ (булеан) |

| | |
|---|---|
| $A \sqcup B$ | Дизъюнктное объединение множеств $A$ и $B$ |
| $\langle a, b \rangle$ | Упорядоченная пара |
| $A \times B$ | Прямое (декартово) произведение множеств $A$ и $B$ |
| $\mathfrak{V}$ | Универсум фон Неймана, класс всех множеств |
| $TC(A)$ | Транзитивное замыкание множества $A$ |
| $\mathrm{rank}(x)$ | Ранг множества $x$ |
| $V_\alpha$ | Универсум фон Неймана ранга $\alpha$ |
| $S(x)$ | Операция взятия последователя (в PA и ZF) |
| $\omega, \aleph_0$ | Первый бесконечный ординал (кардинал) |
| $\lvert A \rvert,\ \#A$ | Мощность (кардинальное число) множества $A$ |
| $\mathrm{Card}(A)$ | Кардинальность: класс всех множеств, равномощных $A$ |
| $\mathfrak{c}, 2^{\aleph_0}$ | Мощность континуума |
| $A \simeq B$ | Множества $A$ и $B$ равномощны (существует биекция) |
| $A \preccurlyeq B$ | Мощность $A$ не больше мощности $B$ (существует инъекция) |
| $A \prec B$ | Мощность $A$ строго меньше мощности $B$ |
| Ord | Класс всех ординалов |
| Succ, Lim | Классы последующих и предельных ординалов |
| Card | Класс всех кардиналов |
| $ot(X, <)$ | Порядковый тип вполне упорядоченного множества |
| $\mathfrak{h}(A)$ | Число Хартогса для множества $A$ |
| $f : A \to B$ | Функция $f$ из множества $A$ в множество $B$ |
| $f : A \leftrightarrow B$ | Биекция между множествами $A$ и $B$ |
| $\hookrightarrow$ | Вложение (инъекция) с сохранением порядка |
| $\mathrm{dom}(f)$ | Область определения функции $f$ |
| $\mathrm{ran}(f)$ | Область значений функции $f$ |
| $f \restriction D$ | Сужение функции $f$ на множество $D$ |
| $f^{-1}$ | Обратная функция |
| $R^{-1}$ | Обратное отношение |
| $\chi_A$ | Индикаторная функция множества $A$ |

| | |
|---|---|
| $\mathrm{supp}(f)$ | Носитель функции $f$ |
| $F^{fin}(Y, X)$ | Множество функций из $Y$ в $X$ с конечным носителем |
| $\mathrm{pr}_A(p)$ | Проекция на компоненту $A$ |
| $aRb$ | $\langle a, b\rangle \in R$ (элементы $a, b$ находятся в отношении $R$) |
| $[a]_R$ | Класс эквивалентности элемента $a$ по отношению $R$ |
| $A/_R$ | Фактор-множество множества $A$ по отношению эквивалентности $R$ |
| $\mathfrak{A} \cong \mathfrak{B}$ | Структуры $\mathfrak{A}$ и $\mathfrak{B}$ изоморфны |
| $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ | Стандартные числовые системы |
| $a = b$ | Равенство |
| $a < b, a > b$ | Строгое неравенство |
| $a \leqslant b, a \geqslant b$ | Нестрогое неравенство |
| $a + b$ | Сложение |
| $a \cdot b, ab$ | Умножение |
| $a \dot{-} b$ | Монус (усеченное вычитание) |
| $a \mid b$ | $a$ делит $b$ |
| $a \equiv b \pmod m$ | $a$ сравнимо с $b$ по модулю $m$ |
| $\underline{n}$ | Нумерал, терм вида $S\ldots S0$, представляющий число $n$ |
| $\beta(c, d, i)$ | $\beta$-функция Гёделя для кодирования последовательностей |
| $\mathrm{Code}(S)$ | Функция кодирования множества натуральным числом |
| $\Lambda$ | Пустая строка (в грамматиках) |
| $\max A, \min A$ | Максимальный/минимальный элемент множества $A$ |
| $\sup A, \inf A$ | Точная верхняя/нижняя грань множества $A$ |

# СПИСОК ИСТОЧНИКОВ

## Общематематические книги и философия


[1] Арнольд В. И. *Гюйгенс и Барроу, Ньютон и Гук*. — М.: Наука, 1989.

[2] Бурбаки Н. Архитектура математики // *Очерки по истории математики*. — М.: ИИЛ, 1963. (Ориг.: Bourbaki, N. L'architecture des mathématiques // Les grands courants de la pensée mathématique. — 1948.)

[3] Feferman, S. Three conceptual problems that bug me. Lecture at 7th Scandinavian Logic Symposium, Uppsala, 1996.

[4] Фихтенгольц Г. М. *Курс дифференциального и интегрального исчисления*: в 3 т. — Изд. 8-е. — М.: ФИЗМАТЛИТ, 2003.

[5] Грэхем Р., Кнут Д., Паташник О. *Конкретная математика*. — М.: Мир, 1998. (Ориг.: Graham, R. L., Knuth, D. E., Patashnik, O. *Concrete Mathematics: A Foundation for Computer Science*. — Addison-Wesley, 1989.)

[6] Казимиров Н. И. *Архетипы математики: общие методы, приемы, конструкции, идеи математики и ее оснований*. — М.: Юстицинформ, 2019.

[7] Казимиров Н. И., Савватеев А. В. Введение в настоящую математику: пособие для учителей математики по мотивам курса «100 уроков математики» Алексея Савватеева. — М.: Русский фонд содействия образованию и науке. Университет Дмитрия Пожарского, 2022.

[8] Kazimirov, N. I. *Mathematics as a Foreign Language*. — Cham: Springer, 2026. — (Mathematics in Mind). — https://link.springer.com/book/9783032307200.

[9] Клайн М. *Математика. Утрата определенности*. — М.: Мир, 1984. (Ориг.: Kline, M. *Mathematics: The Loss of Certainty*. — Oxford University Press, 1980.)

[10] Курант Р., Роббинс Г. *Что такое математика?* 7-е изд. — М.: МЦНМО, 2015. (Ориг.: Courant, R., Robbins, H. *What Is Mathematics?*. — Oxford University Press, 1941.)

[11] Математическая составляющая / Ред.-сост. Н. Н. Андреев, С. П. Коновалов, Н. М. Панюнин. — М.: Фонд «Математические этюды», 2015.

[12] Проблемы Гильберта / под ред. П. С. Александрова — М., Наука, 1969.

[13] Рид К. *Гильберт*. — М.: Наука, 1977. (Ориг.: Reid, C. *Hilbert*. — Springer-Verlag, 1970.)

[14] Успенский В. А. *Предисловие к математике*. — СПб.: Амфора, 2015.

[15] Успенский В. А. *Труды по нематематике*. в 2-х томах. — М.: ОГИ, 2002.

[16] Виноградов С. Н., Кузьмин А. Ф. *Логика. Учебник для средней школы*. — М.: Учпедгиз, 1954.

[17] Shapiro, S. *Foundations without Foundationalism: A Case for Second-Order Logic*. — Oxford: Clarendon Press, 1991.

[18] Петцольд Ч. *Код: тайный язык информатики*. — М.: Русская редакция, 2004. (Ориг.: Petzold, C. *Code: The Hidden Language of Computer Hardware and Software*. — Microsoft Press, 1999.)

[19] Зорич В. А. *Математический анализ*: в 2 т. — Изд. 4-е, испр. — М.: МЦНМО, 2012.

## Классические работы по логике и теории множеств

[20] Буль Дж. *Исследование законов мышления, на которых основываются математические теории логики и вероятностей*. — М.: Наука, 1999. — (Классики науки). (Ориг.: Boole, G. *An Investigation of the Laws of Thought, on Which are Founded the Mathematical Theories of Logic and Probabilities*. — London: Walton and Maberly, 1854.)

[21] Фреге Г. Исчисление понятий, язык формул чистого мышления, построенный по образцу арифметического // *Фреге Г. Логика и логическая семантика: Сборник трудов*. — М.: Аспект Пресс, 2000. (Ориг.: Frege, G. *Begriffsschrift, eine der arithmetischen nachgebildete Formelsprache des reinen Denkens*. — Halle: Louis Nebert, 1879.)

[22] Gödel, K. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I // *Monatshefte für Mathematik und Physik*. — 1931. — Vol. 38. — P. 173–198.

[23] Gödel, K. Die Vollständigkeit der Axiome des logischen Funktionenkalküls // *Monatshefte für Mathematik und Physik*. — 1930. — Vol. 37. — P. 349–360.

[24] Гильберт Д., Бернайс П. *Основания математики*. в 2-х томах. — М.: Наука, 1979–1982. (Ориг.: Hilbert, D., Bernays, P. *Grundlagen der Mathematik*. — Berlin: Springer, 1934, 1939.)

[25] Gentzen, G. Neue Fassung des Widerspruhsfreiheitsbeweises für die reine Zahlentheorie // *Forschungen zur Logik und zur Grundlegung der exakten Wissenshaften*. — Neue Folge 4. — 1938. — P. 19–44.

[26] Hausdorff, F. *Grundzüge der Mengenlehre*. — Leipzig: Von Veit, 1914.

[27] Кантор Г. *Труды по теории множеств*. — М.: Наука, 1985. — (Классики науки).

[28] Клини С. К. *Введение в метаматематику*. — М.: ИИЛ, 1957. (Ориг.: Kleene, S. C. *Introduction to Metamathematics*. — Amsterdam: North-Holland, 1952.)

[29] Stone, M. H. The Theory of Representations for Boolean Algebras // *Transactions of the American Mathematical Society*. — 1936. — Vol. 40, No 1. — P. 37–111.

[30] Tarski, A. *A decision method for elementary algebra and geometry*. — Berkeley: University of California Press, 1951.

[31] Tarski, A. Sur quelques théorèmes qui équivalent à l'axiome du choix // *Fundamenta Mathematicae*. — 1924. — Vol. 5, No 1. — P. 147–154.

## Логика, теория множеств и теория моделей

[32] Александров П. С. *Введение в теорию множеств и общую топологию*. — М.: Наука, 1977.

[33] Беклемишев Л. Д., Яворская Т. Л. Доказуемость и формальная арифметика, г. Москва, 14 сентября — 14 декабря 2021 г.

[34] Беклемишев Л. Д., Яворская Т. Л. Доказуемость и формальная арифметика, часть 2, г. Москва, 12 сентября — 26 декабря 2023 г.

[35] Беклемишев Л. Д., Яворская Т. Л. Введение в теорию моделей, г. Москва, 13 февраля — 28 мая 2024 г.

[36] Беклемишев Л. Д., Пахомов Ф. Н. Введение в теорию доказательств и ординальный анализ, г. Москва, 24 сентября 2018 — 20 мая 2019 г.

[37] Беклемишев Л. Д. Теоремы Гёделя о неполноте и границы их применимости. // Успехи Математических Наук. — 2010. — Т.65, N5.

[38] Bezhanishvili G., Mines R., Morandi P. J. Scattered, Hausdorff-reducible, and hereditarily irresolvable spaces / Topology and its Applications 132 (2003) 291–306.

[39] Buhholz W. Explaining Gentzen's Consisteny Proof within Infinitary Proof Theory. Mn̈chen, 1997.

[40] Бурбаки Н. *Теория множеств*. — М.: Мир, 1965. (Ориг.: Bourbaki, N. *Théorie des ensembles*. — Paris: Hermann, 1970.)

[41] Вавилов Н. *Не совсем наивная теория множеств*. — 2017. (PDF)

[42] Верещагин Н. К., Шень А. Лекции по математической логике и теории алгоритмов. Часть 2. Языки и исчисления. — М.: МЦНМО, 2012.

[43] Верещагин Н. К., Шень А. Лекции по математической логике и теории алгоритмов. Часть 3. Вычислимые функции. — М.: МЦНМО, 2012.

[44] Ершов Ю. Л. Определимость и вычислимость. Сибирская школа алгебры и логики. — Новосибирск: Научная книга, 1996.

[45] Ершов Ю. Л., Палютин Е. А. *Математическая логика*. — М.: Физматлит, 2011.

[46] Bezhanishvili G., Esakia L., Gabelaia D. Some Results on Modal Axiomatization and Definability for Topological Spaces. Springer, 2005.

[47] Esakia L. Intuitionistic logic and modality via topology. Annals of Pure and Applied Logic 127 (2004) 155–170.

[48] Feferman, S. Arithmetization of Metamathematics in a General Setting // *Fundamenta Mathematicae*. — 1960. — Vol. 49. — P. 35–92.

[49] Grzegorczyk, A. Undecidability without arithmetization. // *Studia Logica* 79 (2005): 163-230.

[50] Hájek, P., Pudlák, P. *Metamathematics of First-Order Arithmetic*. — Springer-Verlag, 1993.

[51] Jech, T. J. *The Axiom of Choice*. — Amsterdam: North-Holland, 1973.

[52] Jech, T. *Set Theory*. The Third Millennium Edition. — Berlin: Springer-Verlag, 2003.

[53] Kaye, R. *Models of Peano Arithmetic*. — Oxford: Clarendon Press, 1991.

[54] Kirby, L., Paris, J. Accessible independence results for Peano arithmetic // *Bulletin of the London Mathematical Society*. — 1982. — Vol. 14, No 4. — P. 285–293.

[55] Клини С. К. *Математическая логика*. — М.: Мир, 1973. (Ориг.: Kleene, S. C. *Mathematical Logic*. — New York: John Wiley & Sons, 1967.)

[56] Колмогоров А. Н., Драгалин А. Г. *Математическая логика*. — М.: Изд-во «Едиториал УРСС», 2005.

[57] Колмогоров А. Н., Драгалин А. Г. *Математическая логика. Дополнительные главы*. — М.: Изд-во Моск. ун-та, 1984.

[58] Коэн П. Дж. *Теория множеств и континуум-гипотеза*. — М.: Мир, 1969. (Ориг.: Cohen, P. J. *Set Theory and the Continuum Hypothesis*. — New York: W. A. Benjamin, 1966.)

[59] Куратовский К., Мостовский А. *Теория множеств*. — М.: Мир, 1970. (Ориг.: Kuratowski, K., Mostowski, A. *Teoria mnogości*. — Warszawa: PWN, 1966.)

[60] Мендельсон Э. *Введение в математическую логику*. — М.: Наука, 1984. (Ориг.: Mendelson, E. *Introduction to Mathematical Logic*. — D. Van Nostrand, 1964.)

[61] Шёнфилд Дж. Р. *Математическая логика*. — М.: Наука, 1975. (Ориг.: Shoenfield, J. R. *Mathematical Logic*. — Reading, MA: Addison-Wesley, 1967.)

[62] Smith, P. *An Introduction to Gödel's Theorems*. 2nd ed. — Cambridge: Cambridge University Press, 2013.

[63] Smullyan, R. M. *Theory of Formal Systems*. — Princeton: Princeton University Press, 1961.

[64] Boolos, G. *The Logic of Provability*. — Cambridge: Cambridge University Press, 1993.

[65] Chomsky, N. *Syntactic Structures*. — The Hague/Paris: Mouton, 1957.

[66] Henkin, L., Monk, J. D., Tarski, A. *Cylindric Algebras, Part I*. — Amsterdam: North-Holland, 1971.

[67] Хенл Дж. М. *Введение в теорию множеств*. — М.: Радио и связь, 1993. (Ориг.: Henle, J. M. *An Outline of Set Theory*. — New York: Springer-Verlag, 1986.)

[68] Hrbacek, K., Jech, T. *Introduction to Set Theory*. 3rd ed. — New York: Marcel Dekker, 1999.

[69] Kunen, K. *Set Theory: An Introduction to Independence Proofs*. — Amsterdam: North-Holland, 1980.

[70] Кузнецов С. Л. Структурная теория доказательств и алгебраическая логика, г. Москва, 8 февраля – 17 мая 2021 г.

[71] Rasiowa, H., Sikorski, R. *The Mathematics of Metamathematics*. — Warsaw: PWN – Polish Scientific Publishers, 1963.

[72] Schütte, K. *Proof Theory*. — Berlin: Springer-Verlag, 1977.

[73] Suppes, P. *Axiomatic Set Theory*. — New York: Dover Publications, 1972.

## Ресурсы автора

YouTube

Telegram

mathem.at