НЕ СОВСЕМ НАИВНАЯ ТЕОРИЯ МНОЖЕСТВ

MENGENLEHRE

Николай Вавилов

Смотрю на него и не вижу, а поэтому называю его невидимым. Слушаю его и не слышу, а поэтому называю его неслышимым. Пытаюсь схватить его и не достигаю, поэтому называю его неуловимым. Не надо стремиться узнать об источнике этого, потому что оно едино. Его верх не освещен, его низ не затемнен. Оно бесконечно и не может быть названо. Оно снова возвращается к небытию. И вот называют его формой без форм, образом без существа. Поэтому называют его неясным и туманным. Встречаюсь с ним и не вижу лица его, следую за ним и не вижу спины его.

Дао дэ цзин, § 14 (перевод Ян Хин-шуна).

If the doors of perception were cleansed, everything would be seen as it is, **infinite**.

William Blake

Das Unendliche hat wie keine andere Frage von jeher so tief das Gemüt des Menschen bewegt; das Unendliche hat wie kaum eine andere Idee auf den Verstand so aufregend und fruchtbar gewirkt; das Unendliche ist aber auch wie kein anderer Begriff so der Aufklärung bedürftig[1].

David Hilbert[2]

Our minds are finite, and yet even in these circumstances of finitude we are surrounded by possibilities that are infinite, and the purpose of life is to grasp as much as we can out of that infinitude.

Alfred Whitehead[3]

Бесконечное, вот ответ на все вопросы. Все вопросы имеют один ответ. А потому нет многих вопросов, а есть только один вопрос. Этот вопрос: что такое бесконечное?

Даниил Хармс, “Бесконечное, вот ответ на все вопросы . . . ”

---

[1] С давних пор ни одна проблема не волновала так глубоко человеческий *дух*, как проблема бесконечного; ни одна *идея* не влияла на разум так возбуждающе и плодотворно, как идея бесконечного; но, вместе с тем, ни одно *понятие* не нуждается так остро в *разъяснении*, как нуждается в нем бесконечное.

[2] D. Hilbert, Über das Unendliche. – Math. Ann., 1925, Bd.95, S.161–190. Русский перевод: Д.Гильберт, О бесконечном. стр.433. – в книге: Д.Гильберт, Избранные Труды, т.I. – Факториал, М., 1998, с.431–448. Сокращенный русский перевод в книге Д.Гильберт, Основания геометрии. – М.–Л., ГИТТЛ, 1948, с.238–364.

[3] Цитируется по N.Rose, Mathematical maxims and minims. – Raleigh, North Caroline, 1988.

Оглавление

Аппендикс 5. Теоретико-множественная топология

§ 1 ♢
§ 2 ♢
§ 4 ♢
§ 5 ♢
§ 6 ♢

Аппендикс 6. Основные алгебраические системы

§ 1 ♢
§ 2 ♢
§ 4 ♢
§ 5 ♢
§ 6 ♢

Множества, отображения, отношения

> Я закрыл глаза, потом открыл их. И тут я увидел Алеф. Тут я подхожу к непересказуемому моменту своего повествования и признаюсь в своем писательском бессилии. Всякий язык представляет собой алфавит символов, употребление которых предполагает некое общее с собеседником *прошлое*. Но как описать другим Алеф, чья беспредельность непостижима и для моего робкого разума? Кроме того, неразрешима главная проблема: перечисление, пусть неполное, бесконечного множества. В грандиозный этот миг я увидел миллионы явлений – радующих глах и ужасающих, – ни одно из них не удивило меня так, как тот факт, что все они происходили в одном месте, не накладываясь одно на другое и не будучи прозрачными. То, что видели мои глаза, совершалось одновременно, но в моем описании предстанет в последовательности – таков закон языка.
>
> Хорхе Луис Борхес, Алеф

Хотя эта книга является частью учебника по алгебре, но не относится собственно к алгебре, а посвящена отработке основ теоретико-множественного языка. Мы систематически и с большим количеством конкретных примеров излагаем ту часть теории множеств, знакомство с которой совершенно необходимо для понимания всех математических дисциплин. Сам выбор материала вполне стандартен, сводится к абсолютному минимуму и диктуется непосредственными потребностями курса алгебры:

★ основы учения о множествах (принадлежность и включение, пустое множество, булевы операции и связывающие их тождества, табличная запись и выделение подмножеств свойствами, булеан);

★ декартовы произведения (упорядоченные пары и n-ки, проекции, прямое произведение отображений);

★ отображения (область, кообласть и график, композиция, инъективные, сюръективные и биективные отображения, обратное отображение, образы и прообразы);

★ конечная комбинаторика (правила суммы, произведения и степени, биномиальные коэффициенты, метод включения и исключения, правило подсчета двумя способами, принцип Дирихле, числа Стирлинга);

★ бесконечные мощности (эквивалентность множеств, сравнение мощностей, теорема Кантора-Бернштейна, счетная мощность и мощность континуума, канторовский диагональный процесс и теорема Кантора о мощности булеана, кардинальная арифметика);

★ отношения (композиция отношений, симметричное и дополнительное отношение, классы отношений);

★ отношения эквивалентности (классы эквивалентности, трансверсали, разбиения, схемы Юнга, фактор-множества, факторизация отображений);

★ отношения порядка (мажорирование и минорирование, наибольший и наименьший элементы, максимальный и минимальный элементы, лексикографический и покомпонентный порядок, диаграмма Хассе, лемма Куратовского-Цорна, фундированные множества, трансфинитная индукция, порядковые типы, основы ординальной арифметики).

Тем не менее, мы обсуждаем эти понятия более основательно и, по возможности, на чуть более современном языке, чем это обычно делается на первых

страницах курсов алгебры и математического анализа. Одна из наших главных целей состоит в том, чтобы на этом элементарном материале вывести читателя на принципиально другой уровень математической софистикации[4]. В соответствии с общей установкой нашего курса примерно половина текста посвящена не фактическому плану, а истории, мифологии, идеологии и приложениям. Некоторые части, например, три больших параграфа, посвященных парадоксам, носят чисто развлекательный характер. Я полностью разделяю сформулированное Литтлвудом[5] определение математики как 'веселой науки': 'a good mathematical joke is better and better mathematics, than a dozen mediocre papers'.

Мы предполагаем, что читатель уже видел основные элементарные понятия и символику теории множеств в школе и поэтому употребляем некоторые термины еще до того, как они будут формально определены в тексте. Поэтому мы не только углубим понимание тех аспектов теории множеств, с которыми он уже встречался в той или иной форме, а стараемся упоминать и такие принципиальные моменты (бесконечные кардиналы, аксиома выбора, аксиома регулярности, праэлементы, трансфинитная индукция, универсумы, классы, и т.д.), о которых он, скорее всего вообще не слышал. Кроме того, в разделах, посвященных прямым произведениям, отображениям и отношениям подчеркиваются теоретико-категорные аспекты этих понятий (множество всех отображений $\mathrm{Map}(X, Y)$, универсальное свойство, функториальность, ковариантность и контравариантность, определение инъекций и сюръекций как мономорфизмов и эпиморфизмов или как коретракций и ретракций и т.д.).

Mengenlehre: язык, инструмент, доктрина и теория

> Точное знание аксиом не является обязательным. Но обязательной является вера в то, что вся классическая математика следует из этих аксиом.
>
> Джон Берджес[6]

Говоря о 'теории множеств' разные авторы подразумевают, три *принципиально* различные вещи:

• **Наивную теорию множеств**. История наивной теории множеств насчитывает *по крайней мере* 3–4 тысячи лет. Например, традиционный порядок гексаграмм И-Цзин, приписываемый Фу-Си, содержит таблицы Кэли для булевых операций на конечных множествах[7]. Уже в совершенно современном виде **вся** наивная теория множеств (принадлежность, включение, свойства булевых операций, декартово произведение, конечная комбинаторика и т.д.) была развита в XVII – XVIII веках Пьером де Ферма, Рене Декартом, Готтфридом фон Лейбницем, Якобом и Иоганном Бернулли и Леонардом Эйлером.

• **Канторовское учение о множествах**. Обратите внимание, что немецкий оригинал говорит о `Mengenlehre`, а вовсе не `Mengentheorie`! Иными слова-

---

[4] **`Софистикация`** — усовершенствование мысленных способностей, умение замечать тонкие отличия, **`утонченность`**, **`искушенность`**, **`изощренность`**, **`изысканность`**.

[5] Дж.Литтлвуд, Математическая смесь. – М., Наука, 1978, с.1–143, стр.6.

[6] Дж.П.Берджес, Вынуждение. – Стр. 99–157 в книге [ML].

[7] Ю.К.Щуцкий, Классическая китайская 'Книга перемен'. – Изд-во 'Восточная Литература' РАН, М., 1997, с.1–605; см. форзац, схемы 8 и 10.

ми, о теоретико-множественной **доктрине**[8] или учении, но не о теории!!! Основы этого **учения** были заложены в XIX веке Бернардом Больцано[9], Георгом Кантором[10] и Рихардом Дедекиндом[11]. Как всякое **учение**, учение о множествах имеет фактические, теоретические, доктринальные и ритуальные аспекты. Основой этого учения, его **символом веры** является почти неограниченное принятие актуальной бесконечности. Нет сомнения, что это кредо в значительной степени определило математику XX века и ответственно за все ее достижения.

---

[8]**Доктрина** — **учение**, **вероучение**, система философских, религиозных, идеологических или теоретических взглядов.

[9]**Бернард Больцано** (05.10.1781, Прага – 18.12.1848, Прага) – чешский математик и теолог, основные математические работы которого относятся к обоснованию анализа. В 1805 годах занял кафедру философии религии в Пражском университете, но в 1819 году после кляузы Папы к Императору был отстранен от должности и сослан в деревню под надзор полиции, с лишением права публичных выступлений и публикаций. В Прагу смог вернуться лишь 1842 году. По описаным выше причинам многие из его результатов вошли в историю под именами Коши, Вейерштрасса, Дедекинда и Кантора. В 1830 году (за 30 лет до знаменитого примера Вейерштрасса!) в книге 'Учение о функциях' Больцано построил пример непрерывной кривой, не имеющей касательной ни в одной точке. В курсе анализа встречаются теоремы Больцано, Больцано-Вейерштрасса, и т.д. Был предшественником Кантора в интересе к математическому изучению понятия актуальной бесконечности. В книге 'Парадоксы бесконечного' Больцано определил бесконечное множество как множество, эквивалентное своей собственной части – то, что сегодня называется бесконечностью по Дедекинду.

[10]**Георг Кантор** (03.03.1845, Санкт-Петербург – 06.01.1918, Галле) – учился в ETH в Цюрихе, Берлинском и Геттингенском Университетах. С 1869 года работал в Университете Галле, где в 1879 году был избран ординарным профессором. Его ранние работы относились к теории чисел и теории функций. Начиная с середины 1870-х годов его интересы переносятся на математическую трактовку понятия актуальной бесконечности. Создание им теории множеств было, несомненно, одним из самых революционных открытий во всей истории науки. В 1874 году Кантор доказал несчетность множества вещественных чисел, а в 1878 году ввел понятия кардинальных и ординальных чисел, которые глубоко исследовал в цикле работ 1879–1884 годов. В нашем курсе встречаются аксиома Кантора, парадокс Кантора, теорема Кантора-Бернштейна, несколько теорем Кантора о мощностях, построение вещественных чисел по Кантору и т.д. Последние десятилетия его жизни были омрачены развязной и несправедливой травлей со стороны некоторых философов и математиков, которая привела к тяжелому психическому заболеванию. Основные работы Кантора по теории множеств опубликованы в Mathematische Annalen в 1878–1897 годах. Эти работы переведены на русский в книге Георг Кантор, Труды по теории множеств. – Наука, М., 1985, с.1–431.

[11]**Рихард Юлиус Вильгельм Дедекинд** (06.10.1831, Брауншвейг – 12.02.1916, ibid.) – общепризнанный классик науки XIX века, непосредственный ученик Гаусса и Дирихле, и близкий друг Римана Дедекинд был одним из основоположников современной алгебры и алгебраической теории чисел. После обучения в Брауншвейге, где он увлекался главным образом химией и физикой, в 1850 году Дедекинд поступил в Университет Геттингена. В 1858 году начал преподавать в ETH в Цюрихе. Приняв это предложение Дедекинд начал длительную традицию, когда работа в Цюрихе была для немецких алгебраистов первым шагом для получения профессорской должности в Германии, после Дедекинда тем же путем прошли Фробениус, Гурвиц, Вебер, Минковский и многие другие. В 1862 году Дедекинд вернулся в Брауншвейгский политехнический институт, где работал до самой смерти. Дедекинд первым включил в университетский курс алгебры теорию полей и теорию Галуа, ввел понятия кольца и идеала. Много размышлял над проблемами обоснования математики, и теорией множеств. Широкой публике известен своей порядковой конструкцией вещественных чисел (дедекиндовы сечения). В честь него названы дедекиндовы кольца, дедекиндовы решетки. В нашем курсе встречаются теорема Кронекера-Дедекинда, формула Мебиуса-Дедекинда, лемма Дедекинда, лемма Дедекинда-Артина и т.д., а также *десятки* введенных им терминов: отображение, идеал, коммутатор, гамильтоновы группы, ...

• Наконец, **аксиоматическую теорию множеств**. Эта развитая в XX веке теория представляет собой в высшей степени специализированнную область профессиональных исследований, с трудными и глубокими результатами. Владение *деталями* этой теории не является необходимым большинству математиков. Что, однако, полезно знать *каждому* математику, так это то, что эта теория способна служить надежным основанием для формализации **всех** обычных понятий, используемых в классической математике.

В настоящей книге теория множеств интересует нас, преимущественно как **язык** и **инструмент**. Однако серьезный читатель должен полностью отдавать себе отчет в том, что *сознательно* овладеть этим языком и *профессионально* использовать этот инструмент невозможно, не приобщившись хотя бы к *основам*[12] теоретико-множественной **доктрины** и не овладев рудиментами *аксиоматической* **теории** множеств.

§ 1. Множество как определяемое понятие

> Туземцы большей частью полагают, что Англия, Лондон и Северная Америка суть различные названия одного и того же места: однако находились и люди более сведущие, – они **знали**, что Лондон и Северная Америка – отдельные, но соседние между собой страны, а Англия – это большой город в Лондоне.
>
> Чарльз Дарвин[13]

> В то время, незадолго до экспедиции Пири, Цермело нравилось доказывать невозможность достижения Северного полюса. Он утверждал, что количество виски, требуемое для достижения некоторой широты, пропорционально тангенсу этой широты, тем самым оно стремится к бесконечности при приближении к полюсу. Когда приезжавшие в Геттинген математики задавали ему вопрос о его фамилии, он отвечал им: "Когда-то она звучала как Walzermelodie, но затем пришлось убрать первый и последний слоги".
>
> Констанс Рид[14].

> Современному математику и не придет в голову, что какое-либо соединение математических символов может иметь "смысл" до того, как ему *придан* смысл с помощью определения. Но это не было тривиальностью даже для наиболее выдающихся математиков восемнадцатого века. Определения не были в их обычае; для них не было естественно говорить "под X мы понимаем Y". С некоторыми оговорками верно будет сказать, что математики до Коши спрашивали не "*как определить* $1-1+1-\ldots$?", а "*что есть* $1-1+1-\ldots$?"; и этот склад мышдения приводил их к ненужным затруднениям и спорам, зачастую, по существу, число словесного характера.
>
> Гарольд Харди[15]

---

[12] О большем речи не идет. Понимание всех более глубоких слоев Канторовской доктрины без свободного владения немецким языком **невозможно**. Пересказать на другом языке тексты Кантора, столь же невозможно, как, скажем, пересказать тексты Новалиса, Ницше, Шпенглера или Юнга. Все известные мне переводы не только разрушают очарование, но и грубо искажают тональность, а часто и смысл сказанного.

[13] Ч.Дарвин, Путешествие натуралиста, Гл. III.

[14] К.Рид, Гильберт, с.131–132

[15] Г.Г.Харди, Расходящиеся ряды. – Л., 1951, с.1–504; стр.19.

> После того, как даны названия изучаемым объектам и их основным отношениям, а также аксиомы, которым эти отношения должны подчиняться, все дальнейшее изложение должно основываться исключительно на этих аксиомах, не опираясь на обычное конкретное значение этих объектов и их отношений.
>
> Андрей Колмогоров[16]

1. Множество как 'неопределяемое' понятие. Часто приходится читать, что понятие множества является первичным и, **поэтому**, 'неопределяемым'. Вот, что написано по этому поводу в классическом учебнике Эдуарда Гурса[17]: "Мы уже несколько раз употребляли слово *множество*. Понятие множества принадлежит к числу тех, которые, по-видимому, бесполезно определять иначе, как с помощью примеров. Всякая совокупность предметов в конечном или бесконечном числе составляет множество." А вот, что говорится в учебнике Лузина[18]: "Что такое "множество"? Мы не станем добиваться ответа на этот вопрос, потому что понятие множества является столь первоначальным, что затруднительно, по крайней мере на сегодняшний день, определить его при помощи более простых понятий. ... Итак, мы не станем искать определения слова "множество". Можно, разумеется, было бы сказать, что множество есть "собрание", "коллекция", "класс", "система", "семейство", "комплекс", "ансамбль", и так далее. Но такая замена одного слова другим никогда не может дать саму *идею* множества тому, кто раньше не приобрел ее каким-нибудь образом."

Это заблуждение более чем вековой давности часто повторяется в руководствах по математическому анализу и других научно-популярных сочинениях и сейчас (июнь 2003 года). Часто и сегодня приходится читать, что 'множество' есть просто синоним слов 'совокупность', 'класс', 'семейство', 'собрание'. Это **не так**, *множество* есть точно определенный **математический термин** для *классов*, образованных по **чрезвычайно простым** явно описанным правилам, и, в частности, **отнюдь** не любая бесконечная *совокупность* предметов будет образовывать множество[19]. Если читатель уже владеет теорией множеств на уровне, необходимом для понимания нехитрой мысли, что *не все, вокруг чего можно поставить фигурные скобки, представляет собой множество*, он может смело пропустить настоящую главу и перейти непосредственно к Главе 1.

2. Множества по Кантору и Дедекинду. Необходимость введения аксиоматики связана отнюдь не с мнимыми 'противоречиями' 'наивной' теории множеств. Повторяющееся из книги в книгу утверждение о противоречиях Канторовской теории множеств **совершенно абсурдно**. Эти противоречия обнаружились **не** в теории Кантора и Дедекинда, а в теориях, придуманных самими логиками, специально с целью обнаружить в них противоречия.

Все существенное для интуитивного понимания множества содержится в следующем классическом изречении Георга Кантора: "Unter einer Menge verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten in unserer Anschauung oder unseres Denkens (welche die Elemente von M

---

[16] А.Н.Колмогоров, Основные понятия теории вероятностей. – М., 1974, с.1–120; стр.9.

[17] Э.Гурса, Курс математического анализа, т.1. – М., ОНТИ, 1936, стр.19.

[18] Н.Н.Лузин, Теория функций действительного переменного. – ГУПИ, М., 1948, с.1–318; стр.7.

[19] В то же время *семейство* есть отображение, рассматриваемое с точностью до равенства, не учитывающего область значений.

genannt werden) zu einem ganzen" – "Под множеством мы понимаем любое соединение M определенных различных (различимых) объектов нашего умозрения или нашей мысли (которые будут называться элементами M) в единое целое". Это определение указывает, что понятие множества оформляет идею **принадлежности**, отношение между множеством и его элементами. Множество – это то, что имеет элементы, или, если угодно, **состоит** из элементов, но при этом само мыслится как некое новое **единство**, некий новый объект более высокого уровня. Другое ключевое слово в этом определении, 'wohlunterschiedenen', трудно переводимое на русский язык, может указывать на то, что, во-первых, элементы множества попарно *различны*, во-вторых, что они попарно *различимы*, т.е. мы можем сказать, равны два элемента множества между собой или нет[20]. Оба эти значения слова 'wohlunterschiedene' раскрываются в следующей фразе[21]: "Eine Mannigfaltigkeit (ein Inbegriff, eine Menge) von Elementen, die irgendwelcher Begriffssphäre angehören, nenne ich *wohldefiniert* wenn ... es als *intern bestimmt* angesehen werden muß, **sowohl** ob irgendein derselben Begriffsphäre angehöriges Objekt zu der gedachten Mannigfaltigkeit als Element gehört oder nicht, **wie auch**, ob zwei zur Menge gehörige Objekte, trotz formaler Unterschiede in der Art des Gegebenseins, eindander gleich sind oder nicht."

В книге 'Was sind und was sollen die Zahlen'[22] Рихард Дедекинд писал "Множество S полностью определено **только** тогда, когда относительно всякой вещи известно, является ли она элементом множества S или нет". Ясно, что такой взгляд на множества устраняет все парадоксы до их появления, но его слабость состоит не в излишней широте, а в недопустимой узости понятия множества. В действительности, описываемая ниже теория Цермело-Френкеля понимает множества значительно более широко, чем их понимали основатели теории множеств Кантор и Дедекинд, хотя, конечно, более узко, чем их первоначально понимали Фреге и Рассел.

3. Аксиоматика Цермело-Френкеля. Первая *непротиворечивая*[23] система аксиом для теории множеств была предложена в 1908 году[24] Эрнстом Цермело[25]. Она состояла из аксиом объемности, существования, пары, объединения,

---

[20]И, в-третьих, на *произвольность* этих элементов.

[21]G.Cantor, Ges. Abh., S.150.

[22]Р.Дедекинд, Что такое числа и для чего они служат. – Изв. Физ.–Мат. Об-ва Казанского Ун-та, 1906, т.15, с.25–104. Точнее было бы перевести название как 'Что такое числа и зачем они нужны'.

[23]Конечно, как мы теперь знаем, непротиворечивость систем **Z**, **ZF** и **ZFC** не может быть установлена *финитными средствами* и, таким образом, в известном смысле, представляет собой **вопрос веры**. Некоторые авторы шли настолько далеко, что даже определяли математика как того, кто верит в непротиворечивость системы **ZF**. Следует однако заметить, что как чисто формальных, так и эпистемологических оснований для такой веры значительно больше, чем оснований для веры в существование внешнего мира.

[24]E.Zermelo, Untersuchungen über die Grundlagen der Mengenlehre. I. – Math. Ann., 1908, Bd.65, S.261–281.

[25]**Эрнст Цермело** (27.06.1871, Берлин – 21.05.1953, Фрайбург) – немецкий математик. В 1894 году окончил Берлинский Университет, после чего работал в Геттингене, Цюрихе и Фрайбурге. Наибольшей известностью пользуются его исследования по основаниям теории множеств и частично упорядоченным множествам. В нашем курсе встречаются системы Цермело, Цермело-Френкеля и их варианты, аксиома Цермело и теорема Цермело о полном упорядочении. Кроме того, Цермело занимался теорией вероятностей и теорией динамических систем.

бесконечности, подмножеств, степени и выбора. **Система Цермело**, обозначаемая обычно через **Z**, достаточна для обоснования всей классической доканторовской математики, и, заметим, почти всей современной математики, кроме самой канторовской теории множеств. В 1922 году Абрахам Френкель[26] заменил в системе Цермело одну из аксиом, аксиому подмножеств, на значительно более сильную аксиому подстановки[27]. Впрочем, в последнее время она все чаще обозначается **ZFC** (=**ZF**+Choice), чтобы подчеркнуть, что в нее входит аксиома выбора, а через **ZF** обозначается система из 8 аксиом, без аксиомы выбора. В системе **ZFC** всего один тип объектов – множества, всего одно отношение $\in$, всего одна константа – $\varnothing$, в нее входит всего 9 чрезвычайно естественных и удивительно простых аксиом, а ее выразительная мощь чудовищно велика.

В § 10 мы дадим **полное определение** понятия множества так, как оно понимается сегодня большинством математиков. Это полное определение состоит в том, что множества и отношение принадлежности $\in$ удовлетворяют аксиомам Цермело-Френкеля **ZF1** – **ZF9** перечисляющим **все** основные общепринятые способы образования множеств. Согласно этим аксиомам множеством называется то, что **либо** состоит из конечного числа объектов, **либо** является множеством всех натуральных чисел, **либо** получается применением к уже имеющемуся множеству уже имеющейся функции (или, что почти то же самое, получается взятием подмножества уже имеющегося множества), **либо** является объединением уже имеющегося множества уже имеющихся множеств, **либо**, наконец, является множеством всех подмножеств уже имеющегося множества. **Все!** Для *совокупности* объектов не существует никаких других причин быть множеством, кроме перечисленных выше и аксиомы выбора. Т.е. если какое-то множество не получается при помощи перечисленных выше конструкций, то **единственной** причиной, по которой оно может существовать, во всех случаях является аксиома выбора.

При этом аксиома регулярности **ZF9**, по-видимому, **никогда** не использовалась в обычной математике, а там, где она использовалась по неведению (например, определение упорядоченной пары (a,b) как $\{a,\{a,b\}\}$), ее легко обойти. В то же время отбросить аксиому выбора **ZF8** без нарушения целостности математики невозможно, поскольку она используется постоянно и большей частью бессознательно. Таким образом, ядро системы Цермело-Френкеля состоит из аксиом **ZF1** – **ZF8**. В рассужденях о множествах могут использоваться и дополнительные предположения (гипотеза континуума, существование универсумов, существование больших кардиналов, аксиома конструктивности и т.д.), но эти предположения **не являются общепринятыми** и их использование должно каждый раз тщательно оговариваться. Причины, по которым мы основываем наше изложение на **ZF**, носят не философский или умозрительный, а чисто практический характер. За 80 лет существования системы **ZF** не было предложено **ни одного** нового принципа образования множеств, который

---

[26] **Абрахам (Адольф) Френкель** (17.02.1891, Мюнхен – 15.10.1965, Иерусалим) – один из ведущих специалистов по аксиоматической теории множеств и философии математики. Преподавал в Марбурге и Киле, а в 1933 году перехал в Еврейский Университет Иерусалима. Кроме работ по теории множеств написал несколько статей по алгебре. На русский переведена его совместная с И.Бар-Хиллелом книга ‘Основания теории множеств’.

[27] A.Frenkel, Zu den Grundlagen der Cantor-Zermeloschen Mengenlehre. – Math. Ann., 1922, Bd.86, S.230–237.

получил бы достаточно широкое признание или как-то повлиял бы на обычную математику.

4. Место теории множеств в математике. Именно система Цермело-Френкеля **ZFC**, ее модификации и разновидности (например, система, изложенная в первом томе трактата "Элементы математики" Никола Бурбаки) или эквивалентная ей для всех практических целей **система Геделя-Бернайса GB** лежат в основе подавляющей части современной математики и в течение многих десятилетий вообще не имели сколь-нибудь серьезной альтернативы в качестве основания математики.

У многих математиков даже возникла иллюзия, что математика является разделом теории множеств. Эта иллюзия поддерживалась тем, что язык теории множеств удивительно силен и гибок, и что вся классическая математика действительно легко может быть проинтерпретирована на этом языке. Так, например, в 1949 году Никола Бурбаки писал "Все математические теории можно рассматривать как расширения общей теории множеств. Я утверждаю, что на этом фундаменте можно построить все здание сегодняшней математики." Соглашается с этим и Поль Коэн: "Анализируя математические рассуждения, логики пришли к убеждению, что понятие множества является самым основным в математике". За прошедшие полвека перспектива несколько изменилась, так как за это время возникли точки зрения на основания математики альтернативные к теории множеств и, в действительности, гораздо более общие, чем теория множеств. Тем не менее, и сегодня теория множеств продолжает оставаться важнейшей частью математического языка и полностью достаточна для обоснования математических дисциплин аналитического цикла (собственно математический анализ, теория вероятностей, теория дифференциальных уравнений и т.д.).

Культурная отсталость

> Ситуацию, которая возникла затем, социологи описали бы в терминах *культурной отсталости*[28]. Несмотря на наличие непротиворечивой теории множеств, математики продолжали беспокоиться о непротиворечивости. Некоторые сомневались даже в непротиворечивости самой арифметики! Ситуацию еще более ухудшали гротескные попытки Л.Э.Я.Брауэра превратить математику в религию.
>
> К.Сморинский[29]

Всякий, кто говорит о 'противоречиях' или 'парадоксах' теории множеств должен быть признан культурно отсталым: в теории множеств никогда не было никаких противоречий. Все слухи о противоречиях являются либо журнализмом, либо сознательной дезинформацией, либо порождены культурной или умственной отсталостью тех, кто их распускает.

Чтобы понять обстановку, которая привела к формированию этого стереотипа, нужно знать как в то время была организована математическая жизнь. Германия была не центром математического мира — Германия была математическим миром. Это не значит, что

---

[28]В оригинале написано — или должно быть написано — *mental retardation*.

[29]К.Сморинский, Теоремы о неполноте. В кн.: Справочная книга по математической логике. т.IV, М., Наука, 1983, с.9–53; стр.

С одной стороны, это связано крайне поверхностным пониманием теории множеств большинством французских аналистов, которые не владели в достаточной степени немецким языком[30]

С другой стороны, в самой Германии были чрезвычайно сильны традиции конструктивизма. Кронекер

Некоторые *необычные* с точки зрения математиков начала XX века теоремы, утверждающие несуществование или, наоборот, существование некоторых множеств, такие как теорема Кантора—Рассела или теорема Банаха—Тарского было принято называть парадоксами.

5. Парадоксы и кризис оснований. В 1902 г. Бертран Рассел[31] попытался "выгнать нас из рая, который создал нам Кантор". Однако попытка Рассела оказалась неудачной[32]. Эти так называемые 'парадоксы', как и их решение, были известны Кантору лет за 20 до этого. Вот, например, отрывок из письма Кантора Гильберту от 20 сентября 1897 года[33]: "*Totalitäten* die nicht als "Mengen" von uns gefaßt werden können (wovon ein Beispiel die Totalität aller Alefs ist, wie oben bewiesen wurde) habe ich schon *vor vielen Jahren* "absolut unendliche" Totalitäten genannt und sie von den *transfiniten Mengen* scharf unterschieden" – "*Совокупности*, которые мы не можем рассматривать как "множества" я уже *много лет назад* назвал "абсолютно бесконечными" совокупностями и тщательно отличал от *трансфинитных множеств*". А вот отрывок из письма Кантора Дедекинду от 28 августа 1899 года[34]: "Eine Vielheit kann nähmlich so beschaffen sein, daß die Annahme eines "zusammenseins" *aller* ihrer Elemente auf eine Widerspruch führt, so daß es unmöglich ist, die Vielheit als eine Einheit, als ein "fertiges Ding" aufzufassen. Solche Vielheiten nenne ich *absolut unendliche* oder *inkonsistente Vielheiten* ... Wenn hingegen die Gesamtheit der

---

[30]следует ли это отнести к культурной или к умственной отсталости?

[31]**Бертран Рассел** (18.05.1872, Trelleck (Monmouthshire)– 02.02.1970, Penrhyndedraeth (Wales)) – английский философ, логик, писатель и политический деятель, автор десятков блистательных книг на научные, исторические и политические темы. Среди этих книг такие замечательные произведения как 'Человеческое познание, его границы и сфера', 'История Западной философии'. В логике и основаниях математики был партизаном **логицизма**, состоящего в пропаганде нелепой идеи, что математика есть часть логики: 'Principles of Mathematics', 'Principia Mathematica' (совместная с А.Н.Уайтхедом). В философии знаменит как один из самых ярких представителей логического позитивизма. В широких кругах известен главным образом пацифизмом, борьбой против ядерного оружия и книгой 'Почему я не христианин'. Его тексты представляют собой непревзойденные шедевры английской прозы XX века и с полным основанием были удостоены Нобелевской премии 1954 года по литературе. К сожалению, Рассел не понимал духа математики: все его суждения на математические темы совершенно абсурдны и справедливо высмеивались его современниками, в том числе Гильбертом, Пуанкаре и Германом Вейлем. Винер вспоминал: 'Рассел внушил мне весьма разумную мысль, что человек, собирающийся специализироваться по математической логике и философии математики, мог бы знать кое-что и из самой математики.' Остается только гадать, почему сам Рассел не пытался следовать столь разумному рецепту.

[32]H.Weyl, The philosophy of Bertrand Russell. – Amer. Math. Monthly, 1946, vol.53, p.208–214.

[33]W.Purkert, Georg Cantor und die Antinomien der Mengenlehre. – Bull. Soc. Math. Belg., 1986, v.38, p.313–327. Эта статья содержит публикацию архивных писем Кантора Гильберту. К сожалению, эти принципиально важные для понимания истории теории множеств документы **не** включены в Ges. Abh. 1932 года. Оригиналы хранятся в Niedersächsische Staats- und Universitätsbibliothek Göttingen, Handschriftenabteilung.

[34]Aus dem Briefwechsel zwischen Cantor und Dedekind. – in G.Cantor, Gesammelte Abhandlungen, Hrsg. von E.Zermelo, Berlin, 1932, S.443–451.

Elemente einer Vielheit ohne Wiederspruch als "zusammenseiend" gedacht werden kann, so daß ihr Zusammengefaßtwerden zu "*einem* Ding" möglich ist, nenne ich sie eine *konsistente Vielheit* oder eine Menge". Заметим, что все это происходило задолго до ажиотажа по поводу 'парадоксов' 'наивной' теории множеств.

Нам здесь нет нужды обсуждать шок, трепет и прочую дурь, типа интуиционизма, которые охватили не умевшую читать по-немецки часть математического мира в первые десятилетия XX века. "Суеверен страх и благоговеен трепет математиков перед лицом противоречия" – Г.Фреге[35]. Но Фреге был логиком, а не математиком, напротив, Г.Кантор был математиком и он сказал "То, что получил Бурали-Форти - сущая чепуха." (см. Ван Хао).

В любой аксиоматической теории множеств имплементирован механизм, позволяющий избежать появления логических парадоксов. Современному математику трудно понять, "даже с трудом", почему логические парадоксы произвели такой ажиотаж в начале XX века. Тем не менее, мы подробно обсуждаем парадоксы ввиду их большой развлекательной ценности. Однако смысл аксиоматической теории множеств состоит вовсе не в том, чтобы избавиться от парадоксов (которые и так **никогда не возникали** в обычно проводимых в математике доказательствах), а в том, чтобы явно зафиксировать допустимые способы рассуждения о множествах.

Behaupte, wo du stehst!

> Сомнения по поводу классической математики кажутся более сомнительными, чем она сама. Обычные умозаключения о бесконечном вполне убедительны для понимающего математика. Элиминация понятий, относящихся к бесконечному, не дает нам дополнительной уверенности в теоремах. *Напротив*, опыт показывает, что финитизированные, формализованные доказательства приводят к трудно отслеживаемым вычислительным ошибкам. Концептуальные доказательства вполне убедительны и наглядны, даже если они используют понятия, относящиеся к бесконечному.
>
> Эрвин Энгелер[36]

> Бессмертие канторовской теории множеств состоит не в том, что она настоящая, а как раз, наоборот, в ее фантастичности, в ее способности наводить на размышления, которые позволили ей вдохновлять математику целой эпохи.
>
> Петр Вопенка[37]

Для квалифицированного читателя выскажем несколько *принципиальных* – как принято говорить, 'философских', но в действительности, скорее идеологических и мифологических – соображений.

---

[35]**Готтлоб Фреге** (08.11.1848, Висмар – 26.07.1925, Бад Кляйнен) – немецкий логик, который пытался вывести арифметику из логических принципов. Учился в Геттингене, а в 1879–1918 годах был профессором в Йене. Разработал очень сложную двумерную систему нотации логических понятий (Begriffsschrift) (на русском языке пример использования системы Фреге приводится на стр.429–431 книги Н.И.Стяжкин, Формирование математической логики, М., Наука, 1967, с.1–508.), которая, однако, не получила никакого распространения, проиграв значительно более простой нотации Пеано.

[36]Э.Энгелер, Метаматематика элементарной математики. – М., Мир, 1987, с.1–127; стр.11.

[37]П.Вопенка, Математика в альтернативной теории множеств, М., Мир, 1983, с.1–150; стр.132.

• Канторовская теория множеств – *независимо от того, как к ней относиться* – представляет собой самое важное из всего, что до сих пор произошло в математике. Не представляет труда даже значительно усилить это утверждение. Создание Mengenlehre это одно из трех самых важных событий произошедших в истории человечества за последние 6000 лет, сопоставимое по своему значению только с изобретением письма и открытием квантовой механики. Уже одна только роль теории множеств в истории нашей науки обязывает каждого серьезного студента – и, тем более, преподавателя – математики попытаться постичь дух и пафос этой теории, а не просто научиться использовать пару теоретико-множественных значков. Кроме того, не видно никаких симптомов того, что роль понятия актуальной бесконечности в качестве основы и сущности математического мышления может подвергнуться ревизии в ближайшие столетия.

• В вопросе о бесконечности существуют две последовательные точки зрения: действия и суждения ('действие мое ограничено, но суждение не знает границ'). С одной стороны, это пропагандируемая математиками и разделяемая продвинутыми теоретическими физиками точка зрения **актуальной бесконечности**. С другой стороны, это точка зрения **фактической осуществимости**, которой руководствуются все остальное человечество, включая инженеров и программистов. Все попытки логиков и философов осесть между двумя этими стульями со своей 'абстракцией потенциальной бесконечности' бесславно провалились, и я верю, что так будет и впредь. Я склонен соглашаться с Кантором, что *никакая* математически последовательная трактовка понятия бесконечности, отрицающая актуальную бесконечность, невозможна.

• Конечные натуральные числа, уже такие сравнительно небольшие, как $10^{10^{10}}$ являются не более, а менее доступными нашей интуиции, чем бесконечные мощности. Я не верю, что у нас может быть ясная и отчетливая идея о различии между конечными кардинальными (или ординальными) числами[38] $10^{10^{10}}$ и $10^{10^{10}}+1$, в то время как многие математики верят, что у них есть совершенно четкое понимание различия между ω и $\omega+1$ или, скажем, между $\aleph_0$ и $\aleph_1$. Наша интуиция больших конечных объектов вторична по отношению к интуиции бесконечности. В большинстве осмысленных и правильно поставленных вопросов трактовка бесконечного проще или *много* проще, чем трактовка конечного: 'the infinite we'll do rightaway, the finite may take a little bit longer'.

• Изложение теории множеств, претендующее на какую-то степень научности, может вестись только на аксиоматической основе. Однако природа математики состоит не просто в точности, а в *контролируемой* точности. В фокусе собственно математического исследования (в противоположность логическому или философскому!) находится **математическая реальность** – точно в таком же смысле, в котором естественные науки сконцентрированы на понимании *физической* реальности. Математическая реальность является **свободным творением человеческого разума**. Однако, будучи однажды переведена из предсуществования в существование, она приобретает такую степень независимости, что большинство математиков не готовы воспринимать свою деятельность как чисто лингвистическую. Я, как и все профессионалы, с кем мне довелось обсуждать этот вопрос, склонен считать, что, большая часть математических понятий, фактов и теорий имеет смысл и **ценность** ('существует') независимо от туманных аксиом логики и теории множеств. А раз так, то уточнение языка *сверх необходимых пределов*, в частности, эксплицирование правил вывода, не только не является желательным, но, наоборот, имеет тот же эффект, что приблизительность и расплывчатость, то есть смазывает картину и заслоняет от нас реальность.

• При решении вопроса о выборе конкретной аксиоматики следует руководствоваться практическими, а не умозрительными соображениями. Основным критерием здесь является близость к живому математическому языку, принятому большинством математиков. С

---

[38]Разумеется, это высказывание относится лишь к **величине** этих чисел. Как заметил Пифагор, рассматриваемые как элементы кольца $\mathbb{Z}$, числа $10^{10^{10}}$ и $10^{10^{10}}+1$ отличаются: первое из них является женским/четным, а второе – мужским/нечетным! Это отличие находит отражение и в строении конечных множеств. Так, на множестве порядка $10^{10^{10}}$ существуют инволюции без неподвижных точек, в то время как каждая инволюция на множестве порядка $10^{10^{10}}+1$ имеет неподвижную точку. Но это общее суждение никак не связано с нашим восприятием величины этих чисел, его смысл и содержание для пары $10^{10^{10}}$ и $10^{10^{10}}+1$ такие же, как для пары 16 и 17.

этой точки зрения достоинство системы Цермело-Френкеля **ZFC** состоит в том, что она не вводит никаких экзотических понятий и основана исключительно на *общепризнанных*[39] принципах образования множеств. Более того, за восемьдесят лет не было предложено **ни одной** общезначимой новой конструкции множеств, которая не моделировалась бы в системе Цермело-Френкеля. При всех лингвистических преимуществах системы Геделя-Бернайса, все мои симпатии как работающего математика – и, *тем более*, как преподавателя, – находятся на стороне системы Цермело-Френкеля.

Рассмотрим с этой точки зрения статус трех важнейших классических утверждений: аксиомы выбора, аксиомы регулярности (alias аксиомы фундирования) и гипотезы континуума.

• Использование **аксиомы выбора** в математике невозможно проконтролировать, так как она используется *на каждом шагу*, причем такое использование происходит большей частью бессознательно. Грубо говоря, как только мы произносим что нибудь в духе 'возьмем ...' или 'пусть ...' в применении к бесконечным множествам, иногда – обыкновенно – всегда нет никаких причин, по которым это можно проделать, кроме аксиомы выбора **AC**. Таким образом, никакая элиминация аксиомы выбора из математики невозможна без фактического разрушения большей части классической математики, в том числе и ее прикладных разделов[40]. Кроме того, как показал Гедель, никакая фальсификация **AC** в рамках теории **ZF** невозможна. Мы можем лишь *постулировать*, что **AC** не имеет места. Роль детального обсуждения аксиомы выбора на начальном этапе изучения математики состоит в том, чтобы приучить начинающего к мысли, что никакое особое обсуждение аксиомы выбора не нужно. Нет *никаких* оснований отвергать аксиому выбора.

• В противоположность аксиоме выбора **аксиома регулярности** никогда не использовалась в обычной математике. *Отрицание* аксиомы регулярности невозможно фальсифицировать в $\mathbf{ZFC}^-$, наоборот, весьма просто построить множества, не удовлетворяющие этой аксиоме. Мне кажется, что отбрасывание этой аксиомы приводит к плодотворным новым точкам зрения и обогащает нашу теоретико-множественную интуицию. Нужно ли вводить в аксиоматику явное требование существования нефундированных множеств, для меня вопрос неясный. С одной стороны, аксиомы антифундирования явно симпатичны тем, что возвращают рассмотрение порочного круга (vicious circle) в область строгого математического изучения. С другой стороны, никакая их этих аксиом не обладает *пока* статусом общезначимости. Однако, в любом случае, нет *никаких* оснований принимать аксиому регулярности.

• Статус **гипотезы континуума CH** принципиально отличен как от статуса аксиомы выбора, так и от статуса аксиомы регулярности. Принадлежащая Геделю половина решения гипотезы континуума состоит в том, что **CH** невозможно *опровергнуть*. Точнее, его результат имеет такую природу, что его можно интерпретировать в том смысле, что никакого контр-примера к **CH** невозможно построить, мы можем только *постулировать* существование такого контр-примера. Принадлежащая Коэну половина решения гипотезы континуума состоит в том, что **CH** невозможно *доказать*, причем снова в самом сильном смысле слова 'невозможно'. Большинство математиков согласны с тем, что у нас нет *никаких* априорных оснований занимать какую-либо позицию в вопросе о справедливости гипотезы континуума.

• Отведение основной роли вполне упорядоченным множествам и ординалам в настоящее время полностью утратило смысл. Большинство современных математиков воспринимает именно понятие частично упорядоченного, а не линейно упорядоченного множества, как первичное. Все рассуждения, связанные с трансфинитной индукцией, становятся более простыми и естественными, а их применимость увеличивается, если рассматривать их для *про-*

---

[39] За исключением включенной в нее позже аксиомы регулярности!

[40] В этом месте Виктор Петров сделал следующее примечание: 'Сказанное безусловно справедливо по отношению к *счетной* аксиоме выбора **CC**. В то же время мое глубокое убеждение состоит в том, что в науках 'аналитического цикла' несчетная аксиома выбора глубоко деструктивна и может использоваться только в подрывных целях (например, для построения множества, не имеющего меры, или 'теоремы такого-то о безмерной мере', как Фейнман назвал парадокс Банаха-Тарского). В то же время, в алгебре **AC** нужна **безусловно**, чтобы не добавлять каждый раз идиотские присказки вроде 'мы предполагаем, что во всех рассматриваемых кольцах любой идеал содержится в максимальном'. Таким образом, моя точка зрения состоит в том, что для разных наук нужны **разные** теории множеств: для анализа **ZF+AD**, а для алгебры – **ZFC**.'

извольных фундированных частично упорядоченных множеств. Фактически, большинство математиков, конечно, так и поступает.

• В самом понятии множества нет ничего неприкосновенного. Нам необходимо *какое-то* первичное понятие для организации математической реальности и моделирования математических объектов. Множества являются традиционным и наиболее распространенным, но не единственным возможным инструментом для этого. На самом деле, в качестве основания математики можно было бы взять **любое** другое понятие, эквивалентное понятию множества по своей выразительной силе, например, понятие списка, набора, частично упорядоченного множества, отображения, отношения, графа, дерева, ... В действительности, computer science оперирует с понятием списка (массива), и если бы мы должны были принимать решение *сегодня*, то, вероятно, положили бы и в основу преподавания математики какое-нибудь более сильное понятие, скорее всего, либо понятие списка, либо понятие набора (мультимножества) поскольку большинство математических конструкций допускают *более короткие* описания в терминах этих понятий, чем в терминах множеств.

• Теория множеств не является единственнымым способом мыслить математические объекты и в чисто фактическом плане. **Теория категорий** является не только реальной альтернативой теоретико-множественному мировоззрению, но и гораздо более общей точкой зрения. Уже сегодня многие алгебраисты и топологи владеют теоретико-категорным языком столь же хорошо, как – или лучше, чем теоретико-множественным. Недавно я с изумлением заметил, что единственный способ вспомнить определение эквивариантного отображения $f(gx) = gf(x)$ состоял для меня в том, чтобы нарисовать соответствующую коммутативную диаграмму. Любое современное изложение теории множеств должно подчеркивать теоретико-категорные понятия и конструкции и готовить студента к переходу на категорный язык.

• В действительности теория множеств и теория категорий являются лишь первыми двумя членами бесконечной иерархии теорий. Говорить о множестве всех множеств не только нельзя, но и бессмысленно, полезно рассматривать *категорию* множеств. Точно так же, бессмысленно рассматривать категорию всех категорий как категорию – категория всех категорий представляет собой **2-категорию**, морфизмами которой являются функторы, а 2-морфизмами – естсественные преобразования функторов. Теория множеств описывает объекты, теория категорий – преобразования объектов, теория 2-категорий – преобразование этих преобразований, и т.д. Поясним это метафорой из программирования. Теория множеств описывает данные. Теория категорий описывает программы, которые являются способами преобразования одних данных в другие. Но после этого возникает уровень 2-категорий, состоящий в изучении способов переписывания одних программ в другие, уровень 3-категорий, состоящий в изучении способов переписывания способов переписывания программ и т.д.

• Специфика теории множеств состоит в том, что она использует классическую двузначную логику для классификации подобъектов. Это значит, что для любого $x \in X$ и любого $Y \subseteq X$ имеет место альтернатива: либо $x \in Y$, либо $x \notin Y$. Иными словами, характеристическая функция подмножества принимает значения в двухэлементном множестве $\{0, 1\}$. Вплоть до конца 1960-х годов было предпринято много наивных попыток расширить логику до *трехзначной* (когда в качестве классификатора подобъектов выступает $\{0, 1/2, 1\}$) или *нечеткой* (где классификатором подобъектов является сегмент $[0, 1] \subseteq \mathbb{R}$). Однако все эти теории легко моделируются в теории множеств и не составляют ей никакой реальной альтернативы. Подлинное освобождение от классической логики приходит только в **теории топосов**, где выясняется, что классификатором подобъектов может быть *что угодно*.

§ ?. О чем не говорил Конфуций

Я чту богов и демонов, но держу их от себя в отдалении.

Конфуций

Теорема Геделя в чем-то нуждается, чтобы стать теоремой Геделя, но то, в чем она нуждается, слишком неопределенно.

Чжуан Чжоу

Нет ничего более обманчивого, чем ясная и отчетливая идея, кроме неясной и неотчетливой идеи.

Рене Декарт

Сколько лампочек нужно, чтобы вкрутить лампочку?
Одна, если она знает свой геделевский номер.

Курт Гедель

В популярных изложениях мы часто заменяем точные утверждения неточными или даже точными, но ложными.

К.Сморинский[41]

Интерес такого изучения состоит в том же, что и в известных математических исследованиях вопроса о том, *какого рода задачи можно решить данными ограниченными средствами*, вроде построения циркулем и линейкой.

Соломон Феферман[42]

Есть несколько вещей, которые я категорически не хочу упоминать в этой книге. К таким вещам относятся, в частности, правила вывода, язык первого порядка и теорема Геделя.

'Невежество Бурбаки'[43]

• Во-первых, я считаю, что бóльшая часть математической логики абсолютно **иррелевантна** при изучении математики. Вопросы, которые интересуют нас в этой книге, это *конкретные* вопросы, в ответе на которые используемые правила вывода не могут играть вообще никакой роли, а используемые аксиомы теории множеств — почти никакой. Никакая — *никакая*!!! — ревизия 'оснований', правил вывода и туманных аксиом логики и теории множеств не в состоянии отменить сияющие факты, такие как, скажем, то, что существует ровно 17 групп симметрии плоскости или ровно 6 правильных многогранников в четырехмерном пространстве. А именно факты такого рода, их объяснения, истолкования, следствия и взаимосвязи составляют основное содержание математики. Это значит, что любая попытка

• Чисто лингвистические упражнения. Интуиционисты и конструктивисты предлагают заменить выражение 'множество X конечно' на 'множество X не может не быть конечным'. Я не вижу в этом ничего, кроме ман[ь]еризма. Человек может следить либо за тем, что он говорит, либо за тем, как он это говорит, но не за тем и другим сразу. Даже с точки зрения профессионала

[41]К.Сморинский, Теоремы о неполноте. В кн.: Справочная книга по математической логике. т.IV, М., Наука, 1983, с.9–53; стр.18.

[42]С.Феферман, Теории конечного типа, родственные математической практике. — В кн.: Справочная книга по математической логике. т.IV, М., Наука, 1983, с.100–159; стр.101.

[43]К сожалению, сам я был лишен возможности избежать изучения математической логики, хотя бы потому, что реформа ВАК 1977 года влила специальность 01.01.03 — алгебра и теория чисел в специальность 01.01.06 — математическая логика и основания математики ??, в результате чего образовалась новая специальность 01.01.06 — математическая логика, алгебра и теория чисел. Одним из побочных результатов этого была тотальная пересдача всеми аспирантами первой части кандидатского экзамена, с включением в нее вопросов по математической логике, в том числе, конечно, и доказательства теорем Геделя. В настоящее время в официальной программе первой части экзамена по специальности 01.01.06 вообще не осталось никакого контента, ничего, кроме логики.

непонятно, какую пользу подобная вычурность могла бы принести при изучении собственно математических вопросов. Как в исследовании, так и особенно в преподавании аккумуляция подобных чисто вербальных экзерсисов неминуемо приводит к разрыву с традицией, разрушению связей с другими раздалами математики и полной потере смысла. Все это обильно проиллюстрировано писаниями некоторых логически ориентированных очень общих[44] алгебраистов.

• Сомнения в классической математике более сомнительны, чем она сама. Математик — это тот, кто все подвергает сомнению. Но подвергая сомнению все, он, разумеется, подвергает сомнению и то, что все следует подвергать сомнению.

Потрясает наивность людей, которые считают, что понятия элемента, множества, функции, бесконечности, числа требуют дальнейшего анализа и обоснования, в то время как понятия символа, текста, конструктивного объекта, правильно составленной формулы, формального языка, выводимости, доказуемости, истинности ясны сами по себе. В действительности это иллюзия, обоснование математики с помощью логики — это обоснование прозрачного с помощью туманного.

Когда конструктивист[45] говорит, что натуральное число выражается в алфавите, состоящем из одного символа |, ||, |||, и заявляет, что этот процесс можно *неограниченно продолжать*, мне кажется, он не учитывает чего-то весьма существенного. А именно, того, что в процессе написания таким образом уже крошечных чисел, ну хотя бы $10^{10^{10}}$ мы собъемся со счета, кончатся чернила, кончится бумага, кончится время, но главное все-таки, состоит в том, что если мы будем писать все дальше и дальше, то под действием гравитации чернила и бумага превратятся в чер[ниль]ную дыру. Словом, требуемого количества черточек ему написать не удастся.

Конструктивная математика опирается на т ысячи неявных предположений, подразумеваемых, но не сформулированных аксиом. Кто может гарантировать, что за ночь в тексте не появляются новые символы и не исчезают старые, что мы в состоянии отличить один символ от другого

• Если упоминать теорему Геделя, то только в паре с теоремой Генцена. Дело в том, что теорема Геделя утверждает, что непротиворечивость арифметики невозможно доказать *определенными средствами*. Однако она не говорит, что этого нельзя сделать другими, не менее надежными средствами!!! Теорема Геделя[46] Доказательство Геделя состояло в том, что он сопоставлял каждой формуле некоторое очень большое *натуральное* число — геделевский номер. С другой стороны — и это почему-то уже гораздо менее известно, в 1936 году Герхард Генцен[47] *точно так же* доказал непротиворечивость арифметики, сопоставляя каждой формуле некоторое не очень большое счетное *ординальное* число. Разница между доказательством Геделя и доказательством Генцена не

---

[44]Или, как ласково называет их Арнольд, *преступных*.

[45]П.Мартин-Лёф, Очетки по конструктивной математике. — Изд-во Мир, 1975, с.1—136, стр.9.

[46]K.Gödel, Über formal unentscheidbare Sätze der *Principia Mathematica* und verwandter Systeme. I. — Monatshefte für Math. und Physik, 1931, Bd.38, S.173–198.

[47]G.Gentzen, Die Widerspuchsfreiheit der reinen Zahlentheorie. — Math. Ann., 1936, Bd.112, N.2, S.493–565; русский перевод в книге Математическая теория логического вывода, М., Наука, 1967, с.77–153.

заметна невооруженным глазом. Степень нашей уверенности в справедливости той формы индукции, которой пользовался Генцен, ничуть не меньше, чем в обычных аксиомах арифметики. Разумеется, результат Генцена не приобрел скандальной известности за пределами логического сообщества ровно потому, что он доказывает то, во что все и так верят, непротиворечивость арифметики!

Теорема Геделя занимает такое же место в истории математики, как доказательство невозможности трисекции угла при помощи циркуля и линейки и невозможность решения уравнения пятой степени в радикалах. Это очень почетное место!!! Эти проблемы сыграли огромную роль в историческом развитии математики. Однако они не имеют никакого отношения к ее сегодняшнему состоянию и никаким образом не рассматриваются математиками в качестве ограничений.

• задолго до того, как наступают ограничения, проистекающие из теоремы Геделя ... чисто физические ограничения на длину доказательства, связанные с ограничением времени или памяти.

• Теорема Геделя есть математическая теорема, которая состоит из контекста(ов?), формулировки(ок?), доказательства(в?), интерпретации(ий?) и т.д. Однако обычная журналистская практика состоит в том, чтобы позиционировать ее не как теорему математики, а как теорему **о** математике. Но теорема Геделя не говорит *ничего* о математике. Она говорит *нечто* о генерации некоторого специального вида *текстов* в некотором специальном типе формальных систем.

Программа Гильберта носит чисто апологетический характер. Он хотел ограничить те средства, которые используются для обоснования (или, как говорит Феферман, *оправдания*) математики, до абсолютного минимума, до средств признаваемых как допустимые *всеми* математиками, *включая* Брауэра. Сам Гильберт, как совершенно ясно из всех оставленных им текстов, никогда не стоял на финитистских позициях и полностью разделял обычную математическую интерпретацию канторовского учения с неограниченным признанием актуальной бесконечности. Поэтому смешно называть **тезисом Гильберта** одиозное утверждение, что *нет логики, кроме логики первого порядка*. Теорема Геделя представляет собой не крах Гильбертовской программы обоснования математики, как об этом пишут журналисты. Она утверждает лишь, что Гильберту не удалось бы убедить Брауэра.

Краткий путеводитель по литературе

> Когда появилось мудрствование, возникло и великое лицемерие. Когда будут устранены мудрствование и ученость, народ будет счастливее во сто крат. Все эти вещи происходят от недостатка знаний. Поэтому нужно указывать людям, что они должны быть простыми и скромными. Когда будет уничтожена ученость, тогда не будет и печали.
>
> Дао дэ цзин, §§18–20.

Рекомендация студентам: прочтите [VSh], после этого сводку результатов к [B], потом [KuM] и [Co]. Если Вы хотите действительно понять организм теории множеств, переходите к [JW].

Вводные главы всех учебников дискретной математики, алгебры, топологии и математического анализа содержат сведения по теории множеств. При этом большая часть того, что сообщается из области теории множеств в учебниках математического анализа, состоит

из смеси невнятного **`булькань`**я[48], прямого вранья и фактических ошибок[49] и не заслуживает вообще **никакого** доверия, особенно там, где появляются так называемые *доказательства*[50]. То, что пишется в учебниках функционального анализа [Di], [KF], алгебры и общей топологии, как правило, несколько вразумительнее и чуток достовернее, но тоже обычно поверхностно и не только дает весьма слабое представление о канторовской теории множеств, но даже не предостерегает от источников прямых ошибок. Исключения составляют полуаксиоматические изложения теории множеств в [K], [Co], [Fa].

Из совсем элементарных введений в наивную теорию множеств и популярных книг на русском языке упомянем [S1], [Sta], [Vil]. Самым тщательным и детальным из них является книга [Shi], основанная на лекциях для лингвистов. Из недавних более продвинутых книг можно упомянуть совершенно замечательные по ясности записки курса [VSh]. Со свойствами *алгебры множеств* можно детально познакомиться по любой[51] книге по решеткам или булевым алгебрам, если иметь в виду, что подмножества фиксированного множества образуют дистрибутивную решетку с дополнениями.

Из полунаивных изложений большой интерес представляет книга Феликса Хаусдорфа [Ha]. Эта замечательная книга является гибридом двух книг Grundzüge der Mengenlehre (1914) (это первый учебник по теории множеств в мировой литературе!) и Mengenlehre (1927), с включением нескольких фрагментов, написанных П.С.Александровым. Несомненный исторический интерес представляют также книги Куратовского и Мостовского [KuM] и Серпиньского [S2], [S3]. Книга Куратовского и Мостовского, конечно, порядком устарела, тем не менее и сегодня она остается самым основательным и заслуживающим доверия изложением теории множеств на русском языке. Книга Н.Бурбаки [B] претендует на то, чтобы быть введением в аксиоматическую теорию множеств, но не может рассматриваться в качестве таковой в силу полной некомпетентности ее автора в математической логике. С другой стороны, эта книга является незаменимым источником знаний по вопросу о том, сколько существует отображений из пустого множества в пустое множество. Среди сотен книг на английском можно отметить [F], [H], [HJ], [Ro], [R], каждая из которых по своему совершенно замечательна. Однако для полного понимания сущности Mengenlehre ничто не может заменить чтения работ Кантора [C1], [C2], [PB] **на немецком языке**.

На русском имеется изумительное по красоте и ясности введение в аксиоматическую теорию множеств, написанное одним из лучших профессионалов в этой области [Co] и, рассчитанная на более подготовленного читателя [J1]. Совершенно феерическая монография [JW], позволяет неспециалисту приобщиться к духу и проблематике современных исследований. В захватывающих книгах [J2] и [RR] перечисляется несколько сотен утверждений, эквивалентных аксиоме выбора. История и философия теории множеств детально обсуждаются в

---

[48]**`Булькань`**е — невразумительное изложение булевой алгебры. **`Булева алгебра`** — наука о разливании бутылок по количеству содержащихся в них булек. **`Булька`** — крупная капля или пузырь, глобула, шарик, мячик, клубок, бусина, снежок, биток, катышек, четка, шишка, желвак, комок, клубень, луковица, (круглая) пилюля, или любой другой небольшой предмет круглой формы. В русском языке широко представлены однокоренные слова: **`булла`**, **`булава`**, **`бульба`**, **`булочка`**, **`булавка`**, **`булыжник`**, **`бульон`**, **`пуля`**, **`баллон`**, **`баллотироваться`**, **`волдырь`** (**`булдырь`**) (сравни также латинское `pila`, `bulla`, `bullire`, `bolus`, французское `boule`, итальянское `bolla`, `palla`, немецкое `Ball`, `Bolle`, английское `ball`, `bullet`, `boulder`, `pill`, `pellet`, голландское `puyl`, литовское `bulìs`, санскритское `bulíṣ` и т.д.) Поэтому оставим на совести Фассмера заявление, что **`булькать`** представляет собой заимствование тюркского звукоподражания **`буль-буль`** или **`буль-муль`**. По свидетельству крупнейшего отечественного специалиста в области булевой алгебры Венечки Ерофеева в правильно разливаемой стандартной бутылке водки ровно 39 булек.

[49]Рекорд здесь принадлежит, по-видимому, Л.Д.Кудрявцеву, который делает ошибки уже на уровне *определения* упорядоченной пары и отображения, см., в частности, его статью 'функция' в 'Математической энциклопедии', т.5, Советская Энциклопедия, М., 1985, с.712–720.

[50]Есть, конечно, несколько отрадных исключений, most notably, книга Зорича [Zor], которая и во всех остальных аспектах представляется мне *с большим отрывом* лучшим базовым учебником анализа на русском языке.

[51]Книги Биркгофа [Bi1] и [Bi2] представляют собой не разные издания одной и той же книги, а совершенно разные книги, причем первая гораздо лучше.

[BHF], [Hal]. Из нестандартных теорий множеств наибольшее впечатление производит теория гипермножеств [Acz], [BM].

Все серьезные учебники по математической логике и метаматематике [EP], [Cur], [Kl2], [Me], [Sh] содержат главу или две, посвященные логическим парадоксам и аксиоматической теории множеств. Однако все эти изложения ведутся с точки зрения логиков, не отражают потребностей математики и абсолютно непригодны для первоначального ознакомления с предметом.

Совершенно особое место во всей околоматематической литературе, по существу промежуточное между религией, идеологией, логикой и философией, занимают труды по логицизму, интуиционизму, конструктивизму и другим сектантским направлениям в области 'оснований математики', которые поддерживались их представителями с фанатизмом и религиозным рвением ('война мышей и лягушек'), со всеми атрибутами идеологической борьбы, типа ссылок на марксизм и пр. В мировоззренческом плане дискуссии об основаниях не оказали **никакого** влияния на позицию подавляющего большинства математиков, но на определенном этапе своего развития конкретные исследования в области интуиционистской и конструктивной математики были инкорпорированы в классическую математику и в настоящее время являются вполне респектабельными, хотя и весьма эзотерическими разделами теории алгоритмов, теории булевых алгебр и топосов.

Настоящая библиография не претендует на полноту, я привожу лишь немногие книги, которые, по моему мнению, могли бы быть полезными или интересными студенту, а также те книги, которые повлияли на мое собственное понимание теории множеств или которые многократно цитируются в дальнейшем тексте. В то же время по тем темам, где на русском языке имеется обширная литература (логика, конструктивизм и т.д.), я вообще не привожу ссылок на книги на других языках. Однако полных современных учебников по теории множеств и теории категорий на русском языке просто **нет**, поэтому я вынужден указывать иноязычные книги.

История и философия теории множеств

[C2] Г.Кантор, *Труды по теории множеств*, Наука, М., 1985, pp. 1–431.
[PB] *Парадоксы бесконечного*, Издатель В.П.Ильин, Минск, 2000, pp. 1–366.
[FBH] А.Френкель, И.Бар-Хиллел, *Основания теории множеств*, Мир, М., 1966, pp. 1–555.
[C1] G.Cantor, *Gesammelte Abhandlungen*, Berlin, 1932.
[Hal] M.Hallett, *Cantorian set theory and limitations of size*, Claredon Press, Oxford, 1984, pp. 1–343.

Руководства по наивной теории множеств

> То обстоятельство, что профессор читал "Драматургию", может показаться несколько неожиданным. Однако профессор, известный не только как ученый, но и как педагог, непременно, насколько позволяло ему время, просматривал книги, не нужные ему по специальности, но в какой-то степени близкие мыслям и чувствам современного студенчества.
>
> Акутагава Рюноске[52]

[Al] П.С.Александров, *Введение в теорию множеств и общую топологию*, Наука, М., 1977.
[Br] А.Л.Брудно, *Теория функций действительного переменного*, Наука, М., 1971, pp. 1–119.
[VSh] Н.К.Верещагин, А.Шень, *Начала теории множеств*, МЦНМО, М., 1999, pp. 1–127.
[Vil] Н.Я.Виленкин, *Рассказы о множествах, 2-е изд.*, Наука, М., 1969, pp. 1–159.
[Di] Ж.Дьедонне, *Основы современного анализа*, Мир, М., 1964, pp. 1–430.
[Zam] М.Заманский, *Введение в современную алгебру и анализ*, Наука, М., 1974, pp. 1–487.
[Zor] В.А.Зорич, *Математический анализ, т.I,II*, М., 2002.
[KST] Дж.Кемени, Дж.Снелл, Дж.Томпсон, *Введение в конечную математику*, ИИЛ, М., 1963, pp. 1–486.

[52] Носовой платок, в книге Акутагава, сочинения, т.I, Полярис, М., 1998, с.106–114.

[KF] А.Н.Колмогоров, С.В.Фомин, *Элементы теории функций и функционального анализа*, Наука, М., 1968, pp. 1–496.
[NO] В.Н.Нефедов, В.А.Осипова, *Курс дискретной математики*, Изд-во МАИ, М., 1992, pp. 1–262.
[S1] В.Серпинский, *О теории множеств*, Просвещение, М., 1966, pp. 1–61.
[Sta] Р.Р.Столл, *Множества, логика, аксиоматические теории*, Просвещенре, М., 1966, pp. 1–231.
[FKD] Р.Фор, А.Кофман, М.Дени-Папен, *Современная математика*, Мир, М., 1966, pp. 1–271.
[Shi] Ю.А.Шиханович, *Введение в современную математику*, Наука, М., 1965, pp. 1–376.

Руководства по полунаивной теории множеств

[AD] Г.П.Акилов, Дятлов, *Основы математического анализа*, Наука, Новосибирск, 1980.
[B] Н.Бурбаки, *Теория множеств*, Мир, М., 1965.
[K] Дж.Л.Келли, *Общая топология*, Наука, М., 1981, pp. 1–431.
[Co] П.М.Кон, *Универсальная алгебра*, Мир, М., 1968, pp. 1–351.
[KM] К.Куратовский, А.Мостовский, *Теория множеств*, Мир, М., 1970, pp. 1–416.
[Fa] К.Фейс, *Алгебра: кольца, модули и категории, т.*I, Мир, М., 1977, pp. 1–688.
[Ha] Ф.Хаусдорф, *Теория множеств*, Гостехиздат, М.–Л., 1937, pp. 1–34.
[H] P.R.Halmos, *Naive set theory*, Springer-Verlag, Berlin et al., 1991.
[HJ] K.Hrbacek, T.Jech, *Introduction to set theory*, Marcel Dekker, N.Y. et al., 1978, pp. 1–190.
[Ro] J.Roitman, *Introduction to modern set theory*, Graduate Studies in Math., 1996.
[R] J.E.Rubin, *Set theory for a mathematician*, Holden Day, San Francisco, 1967, pp. 1–387.
[S2] W.Sierpiński, *Algebre des ensèmbles*, Warszawa–Wrocław, 1951.
[S3] W.Sierpiński, *Cardinal and ordinal numbers*, PWN, Warszawa, 1965, pp. 1–491.

Руководства по аксиоматической теории множеств

[WM] Ван Хао, Р.Мак-Нотон, *Аксиоматические системы теории множеств*, ИЛ, М., 1963.
[J1] Т.Йех, *Теория множеств и метод форсинга*, Мир, М., 1983.
[Co] П.Дж.Коэн, *Теория множеств и континуум-гипотеза*, Мир, М., 1969, pp. 1–347.
[Mo] А.Мостовский, *Конструктивные множества*, Мир, М., 1973, pp. 1–256.
[ML] *Справочная книга по математической логике,* т.II*, Теория множеств*, Наука, М., 1982, pp. 1–374.
[Be] P.Bernays, *Axiomatic set theory*, North Holland, Amsterdam, 1958, pp. 1–225.
[F] A.A.Fraenkel, *Abstract set theory, 2nd ed.*, North Holland, Amsterdam, 1961, pp. 1–295.
[JW] M.Just, M.Weese, *Discovering modern set theory,* I – *Basics*, Graduate Studies in Math., 1996.

Аксиома выбора

[J2] T.Jech, *The axiom of choice*, North-Holland, Amsterdam, 1973.
[RR] H.Rubin, J.E.Rubin, *Equivalents of the axiom of choice*, North Holland, Amsterdam et al., 1968.

Логика и метаматематика

> Bienaventurados los que no saben leer ni escribir porque serán llamados analfabetos[53]
>
> Jose Bergamín, La casa a Pájaros

[GA] Д.Гильберт, В.Аккерман, *Основы теоретической логики*, ИЛ, 1947.
[EP] Ю.Л.Ершов, Е.А.Палютин, *Математическая логика*, Наука, М., 1979, pp. 1–320.
[Cur] Х.Б.Карри, *Основания математической логики*, Мир, М., 1969, pp. 1–568.
[K1] С.К.Клини, *Введение в метаматику*, ИЛ, М., 1957.

[53] ‘Блаженны те, кто не умеют ни читать, ни писать, потому что будут названы неграмотными.’

[K2] С.К.Клини, *Математическая логика*, Мир, М., 1973, pp. 1–480.
[M] Ю.И.Манин, *Доказуемое и недоказуемое*, Советское Радио, М., 1979, pp. 1–167.
[Me] Э.Мендельсон, *Введение в математическую логику*, Наука, М., 1971, pp. 1–319.
[Chu] А.Черч, *Введение в математическую логику,* т.I, ИИЛ, М., 1960, pp. 1–485.
[Sh] Дж.Шенфилд, *Математическая логика*, Наука, М., 1975, pp. 1–527.
[En] Э.Энгелер, *Метаматематика элементарной математики*, Мир, М., 1987, pp. 1–127.

Нестандартные теории множеств

[Vo] П.Вопенка, *Математика в альтернативной теории множеств*, Мир, М., 1983.
[Acz] P.Aczel, *Non-well-founded sets*, SCLI, Stanford, 1988.
[BM] J.Barwise, L.Moss, *Vicious circles and the Mathematics of Non-Wellfounded Phenomena*, CSLI Public., 1996, pp. 1–390.

Применения аксиоматической теории множеств в математике

[Ecl] П.Эклоф, *Теоретико-множественные методы в гомологической алгебре и теории абелевых групп*, Мир, М., 1986, pp. 1–91.

Конечная комбинаторика

[Ai] М.Айгнер, *Комбинаторная теория*, Мир, М., 1982, pp. 1–556.
[GKP] Р.Грэхем, Д.Кнут, О.Паташник, *Конкретная математика*, Мир, М., 1998, pp. 1–703.
[tD] Т.том Дик, *Группы преобразований и теория представлений*, Мир, М., 1982.
[Iv] О.А.Иванов, *Избранные главы элементарной математики*, Изд-во СПбГУ, 1995, pp. 1–223.
[Ka] А.Кофман, *Введение в прикладную комбинаторику*, Наука, М., 1975, pp. 1–479.
[Ry] Г.Дж.Райзер, *Комбинаторная математика*, Мир, М., 1966, pp. 1–154.
[Ri] Дж.Риордан, *Введение в комбинаторный анализ*, ИЛ, М., 1963.
[Hl] М.Холл, *Комбинаторика*, Мир, М., 1970, pp. 1–424.

Булевы алгебры и решетки

[Bi1] Г.Биркгоф, *Теория структур*, ИИЛ, М., 1952, pp. 1–407.
[Bi2] Г.Биркгоф, *Теория решеток*, Наука, М., 1984, pp. 1–566.
[BS] Ф.М.Богомолов, В.Н.Салий, *Алгебраические основы теории дискретных систем*, Наука, М., 1997, pp. 1–368.
[Vla] Д.А.Владимиров, *Булевы алгебры*, Наука, М., 1969, pp. 1–318.
[Gr] Г.Гретцер, *Общая теория решеток*, Мир, М., 1982, pp. 1–452.
[RS] Х.Расева, Р.Сикорский, *Математика метаматематики*, Наука, М., 1972, pp. 1–591.
[Sal] В.Н.Салий, *Решетки с единственными дополнениями*, Наука, М., 1984, pp. 1–127.
[Sik] Р.Сикорский, *Булевы алгебры*, Мир, М., 1969, pp. 1–375.
[Sko] Л.А.Скорняков, *Дедекиндовы структуры с дополнениями и регулярные кольца*, Физматгиз, М., 1961, pp. 1–198.
[Sko] Л.А.Скорняков, *Элементы теории структур*, Наука, М., 1982, pp. 1–148.
[Fu] Л.Фукс, *Частично упорядоченные алгебраические системы*, Мир, М., 1965, pp. 1–342.

Общая теория категорий

[BD] И.Букур, А.Деляну, *Введение в теорию категорий и функторов*, Мир, М., 1972, pp. 1–259.
[GZ] П.Габриэль, М.Цисман, *Категории частных и теория гомотопий*, Мир, М., 1971, pp. 1–295.
[GM] С.И.Гельфанд, Ю.И.Манин, *Введение в теорию когомологий и производные категории*, Наука, М., 1998, pp. 1–412.
[Gr] А.Гротендик, *О некоторых вопросах гомологической алгебры*, ИИЛ, М., 1961, pp. 1–175.
[CSh] М.Ш.Цаленко, Е.Г.Шульгейфер, *Основы теории категорий*, М., 1974.

[AM] M.A.Arbib, E.G.Manes, *Arrows, structures and functors: the categorical imperative*, N.Y., 1975.
[BP] H.B.Brinkmann, D.Puppe, *Kategorien und Funktoren*, Springer, Berlin, 1966.
[Ehr] Ch.Ehresman, *Catégories et structures*, Dunod, Paris, 1965.
[F] P.Freyd, *Abelian categories*, N.Y., 1964.
[HM] M.Hasse, I.Michler, *Theorie der Kategorien*, Verlag der Wissenschaften, Berlin, 1966.
[HS] H.Herrlich, G.Strecker, *Category theory*, Boston, 1973.
[ML] S.MacLane, *Categories for the working mathematician*, Berlin, 1972.
[Mit] B.Mitchell, *Theory of categories*, Academic Press, N.Y., 1965.
[Par] B.Pareigis, *Kategorien und Funktoren*, Stuttgart, 1969.
[Sch] H.Schubert, *Kategorien,* Bd.I,II, Akademie-Verlag, Berlin, 1970, pp. 1–160, 1–148.
[SW] Z.Semadeni, A.Wiweger, *Wstęp do teorii kategorii i funktorów*, PWN, Warszawa, 1978, pp. 1–297.

Топосы

[Go] Р.Гольдблатт, *Топосы: категорный анализ логики*, Мир, М., 1983, pp. 1–486.
[Jon] П.Т.Джонстон, *Теория топосов*, Наука, М., 1986, pp. 1–438.

Интуиционизм, конструктивизм, омфалоскепсис

Забрать все книги бы да сжечь.

Грибоедов

[Hey] А.Гейтинг, *Интуиционизм*, Мир, М., 1965.
[Goo] Р.Л.Гудстейн, *Рекурсивный математический анализ*, Наука, М., 1970, pp. 1–472.
[Dra] А.Г.Драгалин, *Математический интуиционизм*, Наука, М., 1979, pp. 1–256.
[KV] С.Клини, Р.Весли, *Основания интуиционистской математики*, Наука, М., 1978, pp. 1–271.
[Kus] Б.А.Кушнер, *Лекции по конструктивному математическому анализу*, Наука, М., 1973, pp. 1–417.
[ML] П.Мартин-Леф, *Очерки по конструктивной математике*, Мир, М., 1975, pp. 1–136.
[Nov] П.С.Новиков, *Конструктивная математическая логика с точки зрения классической*, Наука, М., 1977, pp. 1–328.

Глава 1. Аксиоматика Цермело–Френкеля

> Мы будем повсюду, где открываются хотя бы малейшие перспективы, заботливо следить за плодотворными понятиями и способами умозаключений, будем ухаживать за ними, поддерживать их, делать их пригодными к использованию. Никто не сможет изгнать нас из рая, который создал нам Кантор.
>
> Давид Гильберт[54]

> В истории науки очень редко случается, чтобы целая научная дисциплина основополагающего значения возникла в трудах одного человека. Это произошло с построенной Георгом Кантором теорией множеств. Все более поздние исследования в этой области воспринимаются лишь как дополнительное развитие его основных мыслей.
>
> Эрнст Цермело[55].

> Завоевание актуальной бесконечности методами теории множеств можно рассматривать как расширение нашего научного горизонта, не меньшее по значению, чем чем коперниковская система в астрономии и теория относительности или даже квантовая механика в физике.
>
> Абрахам Френкель[56]

> Мы посвящаем эту главу предмету, близко соприкасающемуся с основами нашей науки, не в силу философской важности этих основ, а по той причине, что крайне простые в своей сущности, не требующие никаких предварительных познаний идеи и выводы великого основоположника теории множеств Георга Кантора являют собой образец *подлинно математического стиля*. Подлинная математика заключается не в нагромождении искусственных вычислительных приемов, а в умении получать нетривиальные результаты путем размышления при минимуме применяемого аппарата.
>
> Ганс Радемахер, Отто Теплиц[57]

Альберт Эйнштейн как то заметил, что “все нужно сделать настолько простым, насколько возможно, **но не проще**”. По моему мнению, обычные аксиоматические изложения теории множеств, принадлежащие логикам, создают излишние трудности своим языком, не имеющим ничего общего с повседневной практикой математиков. В то же время, ‘наивные’ изложения теории множеств на первых страницах книг по алгебре, топологии или анализу изобилуют **фактическими ошибками**. Например, говорится, что декартово произведение множеств некоммутативно, в том смысле, что $A \times B \neq B \times A$, но при этом на той же самой странице декартово произведение трех множеств *определяется* формулой $A \times B \times C = (A \times B) \times C$, с беззастенчивым знаком равенства[58]. Или повествуется о нежелательности пользоваться аксиомой выбора ввиду ее

[54] ibid. стр.439.

[55] Из предисловия к Gesammelte Abhandlungen von Georg Cantor, Berlin, 1932, S.III

[56] A.Fraenkel, Abstract Set Theory, Amsterdam, 1953, p.331.

[57] Г.Радемахер, О.Теплиц, Числа и фигуры. – РХД, Ижевск, 2000, с.1–258. стр.45.

[58] Подобное чудовищное утверждение можно найти даже в ‘Теории множеств’ Н.Бурбаки, претендующей на некоторую степень научности. Правда, в оправдание этого автора следует уточнить, что эта ошибка допущена в основном тексте на стр.84, до которой долетит только редкая птица, в то время как в сводке результатов (единственно полезной части этого труда) на стр.370–371 этот вопрос трактуется абсолютно правильно!

'неконструктивности' и тут же 'доказывается', что любое бесконечное множество содержит счетное подмножество, т.е. используется именно эта аксиома (или, как минимум, какая-то из ее ослабленных форм). Кстати, по абсолютно загадочным причинам аксиома выбора – единственная аксиома, неизменно упоминаемая во всех этих 'наивных' изложениях.

Мы постараемся избежать как безудержного формализма, свойственного логикам, так и безответственности и приблизительности 'наивного' подхода. Наша точка зрения **полуаксиоматическая**[59], т.е. мы явно формулируем аксиомы теории множеств, но не правила вывода. Мне совершенно непонятно, почему изложение теории множеств на первом курсе университета не может происходить хотя бы на уровне, соответствующем изложению эвклидовой планиметрии в шестом классе средней школы. Мы обсуждаем различные версии аксиоматики теории множеств, но не пытаемся последовательно встать на формальную точку зрения. Я считаю, что общее знакомство с аксиоматической теорией множеств не только увлекательно и чрезвычайно полезно для 'общего развития', но и абсолютно необходимо для каждого математика, независимо от его специальности.

Работающему математику редко приходится обращаться непосредственно к аксиомам теории множеств, обычно ему достаточно следствий из них, но он должен четко понимать, из каких аксиом эти следствия в конечном счете могут вытекать. Впрочем, в последнее время, в связи с постоянно растущей ролью теории категорий, выдвинувшей на первый план **громадные** образования типа категории всех категорий, эта ситуация меняется и многим математикам приходится чаще задумываться о вопросах теоретико-множественной гигиены. Кроме того, знакомство с аксиоматикой нужно хотя бы для того, чтобы развеять до сих пор кочующие из учебника в учебник мифы вековой давности ('парадоксы' теории множеств, 'неопределяемые понятия', 'единственность' прямого произведения, 'особый статус' аксиомы выбора etc., etc., etc.).

§ 2. Множества и элементы, принадлежность

1. Множества и принадлежность. В **ортодоксальной**[60] теории множеств Цермело-Френкеля **ZF** существует *единственный* тип объектов – **множества** и единственное нелогическое отношение, в котором множества могут находиться между собой – **отношение принадлежности**, обозначаемое $\in$. Эти два понятия определяются аксиомами, все остальные понятия явно выражаются через эти два. Характеристикой множеств является то, что им могут принадлежать **элементы**.

Определение. *Если вещь x находится в отношении $\in$ с множеством y, то говорят, что x* **принадлежит** *множеству y или что x является* **элементом** *множества y.*

Символ '$\in$' называется знаком **принадлежности**, TEXнически `\in`. Формула $a \in A$ читается еще как 'A **содержит** a **в качестве элемента**', впрочем, последняя фраза записывается и как $A \ni a$. Используемый в этой последней

[59] Или, если угодно, **полунаивная**.

[60] **ортодоксальный** – соответствующий единственно правильному всепобеждающему учению, **общепринятый**, **обыкновенный**, **обычный**, **традиционный**, **стандартный**, **конвенциональный**, **правоверный**.

формуле знак $\ni$, TEXнически \ni, является отраженным знаком $\in$. Запись $a, b, c \in A$ означает, что все элементы a, b, c принадлежат множеству A. Аналогично, запись $a \in A, B, C$ означает, что элемент a принадлежит всем множествам A, B, C, впрочем, в дальнейшем мы будем чаще записывать это как $a \in A \cap B \cap C$. Специальное обозначение для отношения принадлежности было введено Джузеппе Пеано[61], который использовал для этой цели *греческую* букву ϵ, первую букву *греческого* слова '$\epsilon\sigma\tau\iota$' – 'есть'[62] Во многих старых книгах используется обозначение Пеано, т.е. вместо $a \in A$ пишут $a\epsilon A$. Общеупотребительный сегодня символ $\in$ является просто стилизованным изображением ϵ.

Для отрицания принадлежности эти символы перечеркиваются. Например, $a \notin A$ означает, что a **не принадлежит** A, т.е. не является элементом множества A. Таким образом, $a \notin A$ является сокращением для $\neg(a \in A)$. Запись $a, b, c \notin A$ означает, что ни один из элементов a, b, c не принадлежит A. Аналогично, запись $a \notin A, B, C$ означает, что элемент a не принадлежит ни одному из множеств A, B, C, впрочем, в дальнейшем мы будем чаще записывать это как $a \notin A \cup B \cup C$.

Комментарий 1: Принадлежность versus включения. К сожалению, как термин слово 'содержать' весьма неудачно, так как оно используется еще и в совершенно другом смысле, как синоним *включения* $\subseteq$. Так как оно прочно укоренилось в математическом обиходе, мы будем им пользоваться, но для точности лучше говорить полностью 'содержит в качестве элемента' versus 'содержит в качестве подмножества'. Эта двусмысленность слова 'содержать' относится к большинству Западных языков и связана с тем, что до Пеано Европейские логики и философы вообще не различали $\in$ и $\subseteq$ ('Сократ есть кот' и 'Кот есть животное').

Комментарий 2: Теория множеств с праэлементами. Иногда удобно считать, что существуют объекты, которые сами *не являются* множествами. Теория множеств, в которой существуют объекты, не являющиеся множествами, называется **неортодоксальной** или **теорией с праэлементами**. Например, хотя целые числа, вещественные числа, точки плоскости и т.д. легко проинтерпретировать в ортодоксальной теории множеств, некоторые авторы рассматривают их как самостоятельные объекты, существующие до и независимо от теории множеств. Объекты теории множеств, которые сами не являются множествами, называются **праэлементами** (от немецкого **Urelement**, что часто переводится на русский и как **урэлемент**). Некоторые логики называют праэлементы **атомами** или **индивидами**. Множества и праэлементы называются **вещами**. Теория множеств Цермело-Френкеля с праэлементами обозначается **ZFU**. В ней, кроме пустого множества $\varnothing$, вводится еще одна константа **Ur** – *множество* праэлементов. Подробное обсуждение целесообразности введения праэлементов можно найти в книге Барвайса[63]

Комментарий 3: Употребление прописных и строчных букв. Здесь, как и во многих других элементарных руководствах, мы обозначаем множества прописными латинскими

---

[61] **Джузеппе Пеано** (27.08.1858, Кунео – 20.04.1932, Турин) – итальянский математик. С 1890 года был профессором Туринского Университета. Его основные работы относятся логике и основаниям математики. Написал несколько влиятельных учебников, в том числе многотомный 'Формуляр математики'. Там Пеано ввел употребляемые нами символы, в том числе, $\in$, $\subset$, $\cup$, $\cap$, и многие другие. В университетских курсах встречаются аксиоматика Пеано, кривая Пеано и теорема Пеано о решениях дифференциальных уравнений. Среди других вещей Пеано интересовался искусственными языками и разработал latino sine flessioni – латынь без флексий.

[62] А вовсе не первую букву *латинского* слова 'элемент', как полагает Ян Стюарт! См. Я.Стюарт, Концепции современной математики. – Вышейшая школа, Минск, 1980, с.1–382.. Как известно, по гречески 'элемент' называется 'стихией', и в этом случае Пеано остановился бы на букве σ.

[63] J.Barwise, Admissible sets and structures. – Springer, Berlin et al., 1975.

буквами A, B, C, ..., а их элементы – строчными a, b, c, ... Конечно, с точки зрения ортодоксальной теории множеств такое различение не имеет никакого смысла, поскольку элементы множеств сами являются множествами, потому что **ничего, кроме множеств, не существует**. В более продвинутых руководствах по математической логике и аксиоматической теории множеств как множества, так и их элементы всегда обозначаются строчными буквами, а прописные буквы обозначают собственно классы (т.е. настолько большие 'множества', что они не могут быть элементами никаких других 'множеств'). Заметим, что в элементарной геометрии принято соглашение прямо противоположное нашему. В школьных учебниках точки плоскости или трехмерного пространства обозначаются *прописными* буквами, а прямые – *строчными*. При этом точки обычно мыслятся как праэлементы ('точка есть то, что не имеет частей'), а прямые – как множества лежащих на них точек. Впрочем, это лишь одна из возможных теоретико-множественных интерпретаций элементарной геометрии. Часто значительно удобнее мыслить прямые как праэлементы, а точки – как множества проходящих через них прямых. Возможно, принятое в элементарной геометрии обозначение является подсознательным указанием на эту интерпретацию.

2. Первые примеры: числовые множества. Так как множества интересуют нас главным образом как инструмент для уточнения математического языка и интуиции, мы не будем обсуждать анекдотические примеры[64] вроде 'множества зеленых яблок' или 'множества букв на данной странице' (кстати, *различных* букв или как?), а сразу перейдем к множествам, реально возникающим в математике. Основную роль играют следующие числовые множества. В дальнейшем мы дадим точные определения всех этих множеств, пока же будем считать, что читатель уже встречался с ними в школьном курсе математики (по крайней мере с $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ и $\mathbb{R}$).

• **Натуральные числа.** Через $\mathbb{N}$ обозначается множество натуральных чисел. При этом $1, 2, 17, 1999, 10^{10^{10}} \in \mathbb{N}$, а $0, -1, 1/17 \notin \mathbb{N}$.

• **Целые числа.** Через $\mathbb{Z}$ обозначается множество целых чисел. При этом $0, 1, -17, -10^{10^{10}} \in \mathbb{Z}$, а $-1/2, 1/17 \notin \mathbb{Z}$.

• **Рациональные числа.** Через $\mathbb{Q}$ обозначается множество рациональных чисел. При этом $0, 1/2, -1/17, 137/253 \in \mathbb{Q}$, а $\sqrt{2}, e, \pi \notin \mathbb{Q}$.

• **Алгебраические числа.** Через $\overline{\mathbb{Q}}$ обозначается множество алгебраических чисел. Напомню, что **алгебраическими** числами называются числа, являющиеся корнями алгебраических уравнений с целыми коэффициентами. Например, $\sqrt{2}, -1/\sqrt{3}, 1+\sqrt{5}/2 \in \overline{\mathbb{Q}}$, а $e, \pi \notin \overline{\mathbb{Q}}$.

• **Вещественные числа.** Через $\mathbb{R}$ обозначается множество вещественных чисел. При этом $\sqrt{2}, e, \pi, 1/2\pi^2 \in \mathbb{R}$, а $i, 1+i, -1/2+i\sqrt{3}/2 \notin \mathbb{R}$.

• **Единичный отрезок.** Через $\mathbb{I} = [0,1]$ обозначается единичный отрезок вещественной оси, т.е. множество вещественных чисел x таких, что $0 \leq x \leq 1$.

• **Комплексные числа.** Через $\mathbb{C}$ обозначается множество комплексных чисел. Например $i, 1-i, -1/2-\sqrt{3}/2 \in \mathbb{C}$.

• **Группа углов.** Через $\mathbb{T}$ обозначается множество комплексных чисел, по модулю равных 1, называемое обычно **группой углов** или **единичной окружностью**. При этом $-1, i, -1/\sqrt{2}+i/\sqrt{2}, -1/2-\sqrt{3}/2 \in \mathbb{T}$, а $2i, 1+i, 2+3i \notin \mathbb{T}$.

3. Одноэлементное множество. Множество $\{x\}$ имеет своим единственным элементом x. Такое множество называется **одноэлементным множеством**

[64] Р.Р.Столл, Множества, логика, аксиоматические теории. – Просвещение, М., 1966, с.1–231.

или **синглетоном** (Einermenge). Для разнообразия, единственным элементом множества $\{\{x\}\}$ является множество $\{x\}$, состоящее из x, но при этом сам x не является элементом множества $\{\{x\}\}$, так что $\{x\} \in \{\{x\}\}$, но $x \notin \{\{x\}\}$. Например, $x = \varnothing$ пусто, но $\{\varnothing\}$ не пусто, единственным его элементом является пустое множество $\varnothing$. С другой стороны, $\{\{\varnothing\}\}$ тоже является одноэлементным множеством, единственным элементом которого является одноэлементное множество $\{\varnothing\}$. Тем самым, $\{\varnothing\} \neq \{\{\varnothing\}\}$. Таким образом, отношение принадлежности не является **транзитивным**, т.е. из $x \in y$ и $y \in z$, вообще говоря, не следует, что $x \in z$. Хотя, конечно, легко привести примеры множеств с транзитивным отношением принадлежности. Так, $\{x, \{x\}\}$ содержит как x, так и $\{x\}$ в качестве элементов, причем если $x = \varnothing$, то никаких других элементов у множеств x, $\{x\}$ нет.

Комментарий. Формулируемая ниже аксиома **ZF9** стандартной теории множеств запрещает, среди прочего, включение $x \in x$, так что, в частности, $x \neq \{x\}$ для любого x. Однако даже без этой аксиомы $x \neq \{x\}$ для всех обычно возникающих множеств. В некоторых нестандартных теориях, например, в теории гипермножеств, существуют такие множества x, для которых $x = \{x\}$, и тогда, конечно, $x \in \{\{x\}\}$). Как заметил Освальд Шпенглер[65], уяснение разницы между *вещью* x и *множеством* $\{x\}$, единственным элементом которого является эта вещь, представляет серьезные психологические трудности для 'детей, народных масс и философов'. Так, например, Бертран Рассел[66] специально подчеркивает: '... a class, consisting of a single term, which in that case *is* the class' (курсив самого Рассела!!!). Непонимание разницы между x и $\{x\}$ порождает чудовищную путаницу. Как курьез упомянем, что и в системе **ML** Куайна праэлемент x отождествляется с одноэлементным классом $\{x\}$, что, конечно, нельзя расценивать иначе как пример регрессивного развития, откат к состоянию, предшествовавшему работам Кантора и Пеано.

4. Отношение вхождения. В отличие от отношения включения $\subseteq$, отношение принадлежности $\in$ не является транзитивным. Это значит, что из $x \in y$ и $y \in z$ вообще говоря, не следует, что $x \in z$. Сейчас мы определим в терминах отношение $\in$ новое отношение, которое уже транзитивно.

Определение. Отношением вхождения *называется* **транзитивное замыкание** *отношения принадлежности* $\in$. *Иными словами, говорят, что вещь* x **входит** *в множество* y *и пишут* $x \in\in y$, *если существуют такое натуральное* n *и такие множества* $z_1, \ldots, z_n$, *что* $z_n = y$ *и выполняется цепочка принадлежностей* $x \in z_1 \in z_2 \in \ldots \in z_{n-1} \in z_n = y$. *В этом случае* x *называется* **составляющей** *множества* y.

Таким образом, составляющие множества y – это элементы этого множества, элементы его элементов, элементы элементов его элементов и т.д. Тот факт, что x входит в y часто обозначается также через $x \in^* y$. В некоторых текстах составляющие называются также **конституентами**.

Упражнение. Считая, что x и y являются праэлементами, найдите, сколько составляющих у множества $\{\{x, \{y\}\}, \{y\}\}$, что это за составляющие?

Упражнение. Убедитесь, что отношение вхождения $\in\in$ **транзитивно**, т.е. если $x \in\in y$ и $y \in\in z$, то $x \in\in z$.

Иногда говорят о **глубине** вхождения. Элементы множества входят в него на глубине 1, элементы его элементов – на глубине 2, и так далее. Разумеется, в стандартной теории одна и та же составляющая может многократно входить в данное множество, как на одной и той же, так и на разных глубинах. Например, x входит в множество $\{x, \{x\}, \{x, \{x\}\}\}$ четыре раза, один раз как элемент, т.е. на глубине 1, два раза на глубине 2 и один раз на глубине 3. В некоторых нестандартных теориях множеств, например, в **теории типов**, глубина вхождения регламентируется типами x и y, так что все вхождения x в y происходят на одной и той же глубине. С другой стороны, имеются и такие нестандартные теории множеств,

[65] О.Шпенглер, Закат Европы.

[66] B.Russel, The principles of Mathematics. I. – London, 1903.

как **теория гипермножеств**, которые допускают наличие составляющих на **бесконечной глубине**.

§ 3. Табличное задание множества

1. Табличная запись. Часто множества задаются перечислением своих элементов или указанием правила, по которому эти элементы образуются. При этом для указания, что эти элементы рассматриваются как некоторое новое единство, используются фигурные скобки '{,}', называемые в дальнейшем **скрепами**. Если $a, b, \dots, c$ – все элементы множества A, то говорят, что множество A **состоит** из элементов $a, b, \dots, c$ и пишут $A = \{a, b, \dots, c\}$. Табличная запись особенно часто используется для конечных множеств, но и для бесконечного множества с элементами a, b, c, ... часто пишут $A = \{a, b, c, \dots\}$.

Например, $\{a, b, c\}$ – множество с тремя элементами a, b и c, так что $a, b, c \in \{a, b, c\}$ и, обратно, если $x \in \{a, b, c\}$, то $x = a$ или $x = b$ или $x = c$. Из приведенного выше Канторовского определения ясно (это будет формально включено в наше определение множества в качестве первой аксиомы **ZF1**), что множество полностью определяется своими элементами, при этом ни их порядок, ни их кратности ('повторения') не имеют значения. Таким образом, например, $\{b, c, a\} = \{a, b, c\}$ и $\{a, a, a, b, c\} = \{a, b, c\}$. На самом деле, в дальнейшем мы будем рассматривать системы элементов, зависящие

• от порядка – в этом случае они называются **упорядоченными множествами** или **чумами**);

• от кратности – в этом случае они обозначаются $[x_1, \dots, x_n]$ и называются **наборами** или **мультимножествами**;

• и от порядка и от кратности – в этом случае они обозначаются $(x_1, \dots, x_n)$ и называются **упорядоченными n-ками**, **списками**, **массивами**, **словами** или **векторами**.

Однако *все* эти понятия легко моделируются в рамках Канторовской теории множеств.

2. Примеры табличного задания множеств. В случае *небольшого* конечного множества его элементы можно явно перечислить.

• Множество $\{0\}$ состоит из одного элемента 0, множество $\{0, 1\}$ – из двух элементов, 0 и 1, а множество $\{-1, 0, 1\}$, обычно записываемое как $\{0, \pm 1\}$, – из трех элементов -1, 0 и 1,

• $\underline{n} = \{1, \dots, n\}$ – начальный отрезок натурального ряда длины n, например, $\underline{3} = \{1, 2, 3\}$, $\underline{5} = \{1, 2, 3, 4, 5\}$.

Замечание. С точки зрения ортодоксальной теории множеств подчеркивание в этом примере не имеет большого философского смысла, так как в ней натуральное число *определяется* рекурсивно как множество состоящее из 0 и всех натуральных чисел, меньших данного, например, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$, $4 = \{0, 1, 2, 3\}$ и так далее (см § 13). При этом нулем является пустое множество, см. § 6.

• $\mathrm{Digit} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ – множество 'арабских' цифр.

Замечание. Каждый, кто видел настоящие *арабские* цифры, знает, что арабское в множестве Digit только само слово 'цифра', по-арабски 'sifr', передаваемое в большинстве других европейских языков как 'zero'.

• В Главе 3 мы описываем структуру стандартной карточной колоды. При этом нам понадобится множество[67] мастей Suits = $\{\spadesuit, \heartsuit, \diamondsuit, \clubsuit\}$ и множество рангов Ranks = $\{$A,K,D,J$, 10, 9, 8, 7, 6, 5, 4, 3, 2\}$.

3. Задание множества указанием правила. Перечислить все элементы бесконечного множества обычно довольно затруднительно, поэтому перечисляют несколько первых элементов этого множества, в количестве, достаточном, чтобы восстановить **правило**, по которому образуются все его элементы, а иногда указывается еще и 'общий' элемент.

• $\omega = \mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$ – множество неотрицательных целых чисел;

• $2\mathbb{N} = \{2, 4, 6, \dots\}$ – множество четных натуральных чисел, записывается еще как $\{2, 4, \dots\ 2n, \dots\}$;

• $2\mathbb{Z} = \{0, \pm 2, \pm 4, \dots\}$ – множество четных целых чисел, записывается еще как $\{0, \pm 2, \dots\ \pm 2n, \dots\}$;

• $\{1, 4, 9, 16, \dots\}$ – множество квадратов натуральных чисел, записывается еще как $\{1, 4, 9, \dots\ n^2, \dots\}$;

• $\mathbb{P} = \{2, 3, 5, 7, \dots\} = \{2, 3, 5 \dots\ p, \dots\}$, – множество простых чисел. При этом считается, что из контекста ясно, что p обозначает именно простое число (будучи первой буквой слова 'prime', p является самым употребительным обозначением простых чисел, другие часто встречающиеся обозначения q и ℓ).

• $\{1, 2, 4, 8, \dots\} = \{1, 2, 4, \dots\ 2^n, \dots\}$ – множество степеней двойки.

4. Тесты IQ. В некоторых случаях правило, по которому образуется общий элемент множества, угадать не так просто и задачи такого типа часто входили в тесты для проверки уровня умственного развития, сокращенно называемые тестами IQ (а кто проверял уровень умственного развития авторов этих тестов?). Что, например, должно обозначать $\{2, 3, 5, 7, 13, \dots\}$ и как продолжить $\{1, 2, 5, 14, \dots\}$? Авторы большиства тестов IQ верят, что подобные вопросы допускают однозначные ответы. В действительности это, конечно, не так. Ответы на подобные вопросы обычно определяются контекстом и фоном (background), а вовсе не интеллектом. Если спросить профессионального алгебраиста, что будет следующим элементом

[67] В этом месте Виктор Петров заметил, что, поскольку 'масть' не сконструирована явным образом из пустых множеств, этот пример может быть подвергнут критике с тех же позиций, с которых далее я сам критикую 'множество зеленых яблок'. В том виде, в котором это здесь излагается, это, конечно, так, однако способность (и желание!!!) обращать внимание на подобные детали представляет следующий уровень софистикации, по сравнению с тем, на котором я обычно останавливаюсь в лекциях первому курсу. В действительности, с точки зрения излагаемого примера существенно лишь, что $\spadesuit, \heartsuit, \diamondsuit, \clubsuit$ представляют собой символы, которые читатель в состоянии отличить от всех остальных употребляемых символов. Существование таких символов как данностей языка не вызывает сомнения. Возможность сконструировать соответствующие объекты в рамках излагаемой здесь теории может быть обоснована, *например*, следующим образом: 1) они могут быть явным образом добавлены к множеству праэлементов; 2) из аксиомы подстановки следует существование **потусторонних вещей**, т.е. множеств, отличных от всех множеств, рассматривавшихся до сих пор. С точки зрения нашей теории важно лишь, что символы $\spadesuit, \heartsuit, \diamondsuit, \clubsuit$ отличаются друг от друга и от всех остальных рассматриваемых символов. Словом, 'Мы не будем обсуждать возможность обучить принципам формализованного языка существа, умственное развитие которых не доходило бы до умения читать, писать и считать.' [B], стр.26. Или, иначе, 'чтобы предупредить возражения: *одно* число, *ни одного* числа, *два* случая, *все* вещи из данной совокупности и т.п., все это – ясные языковые образования. Теорема 1, теорема 2, ..., теорема 301 (и аналогично для аксиом, определений, глав и параграфов) или 1), 2) и т.п. при разбиениях на случаи – просто **знаки**, отличающие друг от друга теоремы, аксиомы, ..., случаи и более удобные при ссылках, чем если бы я, скажем, говорил светлосиняя теорема, темносиняя теорема и т.п.' – Э.Ландау, Основы анализа, ИЛ, М., 1947, с.1–182. стр.7.

множества

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, \dots\},$$

то он, несомненно, тут же заметит, что указанные числа представляют собой порядки конечных простых групп и ответит, что это 60. Специалист же по теории чисел, решит, что это рациональные простые числа, следующее из которых 61. В то же время, не имеется никаких достоверных исследований, которые подтверждали бы статистически значимые отличия в уровне умственного развития алгебраистов и теоретико-числовиков.

§ 4. Алфавит

> В тридцатые годы математический уровень физика-теоретика свелся к рудиментарному владению латинским и греческим алфавитами.
>
> Рес Йост[68]

> Если Вы не изучали греческих классиков в подлиннике, то Вы не можете знать названий греческих букв.
>
> Майкл Спивак[69]

> Карамзин изобрел только букву ё: **х, п, ж** изобрели Кирилл и Мефодий.
>
> Венедикт Ерофеев, Из записных книжек

1. Русский алфавит. Обозначим через Cyr = {а,б,в,...,э,ю,я} – множество букв современного русского алфавита, содержащее 32 элемента (мы считаем 'й' отдельной буквой, но 'ё' таковой не является, так что ё=е). Для многих формулируемых в дальнейшем задач, в которых встречается Cyr, существенно, что ни одно русское слово не может начинаться с 'ь', 'ъ', которые в современном русском языке не выражают фонем, не имеют собственных чтений и фактически выполняют функцию диакритических знаков, а не букв, что подчеркивается и их общепринятыми названиями. Впрочем, традиционно 'ъ', он же 'еръ', был полугласной, читавшейся как 'schwa' в современном английском языке (и сохранившей это чтение в некоторых других славянских языках, например, в *българском*). Так как генетически 'ы' является диграфом, состоящим из 'ъ' и 'i', то по тем же историческим причинам ни одно фактически существующее русское слово не начинается с 'ы'. Но, поскольку буква 'ы' имеет самостоятельное фонетическое значение, легко представить себе заимствованное слово, например, личное имя, с нее начинающееся. Таким образом, во всех задачах об инициалах и т.д. мы считаем, что русское слово может начинаться с любого из 30 элементов Cyr отличных от 'ь' и 'ъ'.

2. Латинский алфавит. Обозначим через Lat = $\{a, b, c, \dots, x, y, z\}$ – множество букв латинского алфавита. Разумеется, при использовании в математической речи понятие 'латинского' алфавита, как и любое другое понятие, нуждается в точном определении, так как в обиходе под 'латинским' алфавитом может пониматься практически что угодно, некоторые 'латинские' алфавиты содержат более 50 букв. Помимо дополнительных букв и букв с диакритическими знаками многие языки используют сочетания двух букв как единые буквы, так что, например, 'латинский' алфавит, используемый для записи современного испанского языка, содержит буквы ch и ll, открывающие отдельные разделы словаря. Даже филологи классики расходятся в вопросе о том, сколько элементов, 22, 23, 24 или 25, содержит Lat. Это связано, прежде всего, не с невозможностью определить, какие элементы принадлежат Lat (эта трудность возникает лишь в случае $w = vv$), а с невозможностью решить, когда два элемента Lat равны между собой (а именно, верно ли, что $c = g$, $i = j$ и $u = v$? Вот тут то и нужно вспомнить Канторовское 'wohlunterschiedene'!). Если противное не оговорено явно, в этой книге под 'латинским' алфавитом мы всюду подразумеваем *английский* алфавит, так что, в частности, $g, j, v, w \in$ Lat и множество Lat содержит 26 элементов. В то же

[68] Цитируется по М.Рид, Б.Саймон, Методы современной Математической физики, т. 4, Анализ операторов. – Мир, М., 1982, с.1–428. стр.11.

[69] М.Спивак, Восхитительные TEX (The Joy of TEX). – М., Мир, 1993, с.1–284; стр.54.

время, традиционно используемые русскими математиками *названия* элементов Lat, основанные на гимназической латыни с французским акцентом, заметно отличаются от чтения соответствующих букв английского языка и приведены ниже:

A a	B b	C c	D d	E e	F f	G g	H h	I i
а	бэ	цэ	дэ	э	эф	жэ	аш	и
J j	K k	L l	M m	N n	O o	P p	Q q	R r
йот	ка	эль	эм	эн	о	пэ	ку	эр
S s	T t	U u	V v	W w	X x	Y y	Z z	
эс	тэ	у	вэ	дубль вэ	икс	игрек	зэт	

3. Готический алфавит. В классических книгах по алгебре (в частности, в учебнике ван дер Вардена) широко используется 'готический' алфавит Frac $= \{\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots, \mathfrak{x}, \mathfrak{y}, \mathfrak{z}\}$. Приведем начертания и традиционные названия *печатных* готических букв[70]:

$\mathfrak{A}\mathfrak{a}$	$\mathfrak{B}\mathfrak{b}$	$\mathfrak{C}\mathfrak{c}$	$\mathfrak{D}\mathfrak{d}$	$\mathfrak{E}\mathfrak{e}$	$\mathfrak{F}\mathfrak{f}$	$\mathfrak{G}\mathfrak{g}$	$\mathfrak{H}\mathfrak{h}$	$\mathfrak{I}\mathfrak{i}$
а	бэ	цэ	дэ	э	эф	гэ	ха	и
$\mathfrak{J}\mathfrak{j}$	$\mathfrak{K}\mathfrak{k}$	$\mathfrak{L}\mathfrak{l}$	$\mathfrak{M}\mathfrak{m}$	$\mathfrak{N}\mathfrak{n}$	$\mathfrak{O}\mathfrak{o}$	$\mathfrak{P}\mathfrak{p}$	$\mathfrak{Q}\mathfrak{q}$	$\mathfrak{R}\mathfrak{r}$
йот	ка	эль	эм	эн	о	пэ	ку	эр
$\mathfrak{S}\mathfrak{s}$	$\mathfrak{T}\mathfrak{t}$	$\mathfrak{U}\mathfrak{u}$	$\mathfrak{V}\mathfrak{v}$	$\mathfrak{W}\mathfrak{w}$	$\mathfrak{X}\mathfrak{x}$	$\mathfrak{Y}\mathfrak{y}$	$\mathfrak{Z}\mathfrak{z}$	
эс	тэ	у	фау	вэ	икс	юпсилон	цэт	

Обратите внимание, что чтения букв $\mathfrak{g}$, $\mathfrak{h}$, $\mathfrak{v}$, $\mathfrak{w}$, $\mathfrak{y}$, $\mathfrak{z}$, отличаются от чтения соответствующих 'латинских' букв!

4. Греческий алфавит. Обозначим через Greek $= \{\alpha, \beta, \gamma, \ldots, \chi, \psi, \omega\}$ – множество букв греческого алфавита. Если противное не оговорено явно, под 'греческим' алфавитом мы понимаем древнегреческий алфавит классического периода, содержащий 24 элемента. Таким образом, множеству Greek *не принадлежат* ни архаические буквы дигамма, стигма, коппа и сампи, ни используемые в новогреческом в качестве букв диграфы $\mu\pi$, $\nu\tau$ и т.д. Так как греческие буквы чрезвычайно широко используются в математике, ниже мы воспроизводим начертания прописных и строчных греческих букв и их традиционные русские названия:

A α	B β	Γ γ	Δ δ	E ε	Z ζ	H η	Θ θ
альфа	бета	гамма	дельта	эпсилон	дзета	эта	тэта
I ι	K κ	Λ λ	M μ	N ν	Ξ ξ	O o	Π π
йота	каппа	ламбда	мю	ню	кси	омикрон	пи
P ρ	Σ σ	T τ	Υ υ	Φ φ	X χ	Ψ ψ	Ω ω
ро	сигма	тау	ипсилон	фи	хи	пси	омега

Эти традиционно используемые русскими учеными названия не имеют никакого отношения к чтению этих букв ни в древнегреческом (филологи-классики считают, что древние называли эту букву **тхэта**), ни в новогреческом (где β называется **вита**, а θ, естественно, θ**ита** — или, при отсутствии передних зубов, **фита**), ни, конечно, в английском, (где ε называется **ипсайлен**, а χ – **кай**).

Предостережение. Некоторые греческие буквы имеют два традиционных начертания, например, буква **сигма** в начале или середине слова пишется как σ, а в конце слова — как ς. Большинство математиков используют приведенные выше начертания букв **эпсилон** ε и **фи** φ. Между тем, TEX трактует как основные начертания ϵ и ϕ. С другой стороны, использование начертаний **тета** как ϑ, **ро** как ϱ и **каппа** как $\varkappa$ вместо обычных θ, ρ и κ ограничено некоторыми специальными контекстами, такими как теория ϑ-функций. В свою очередь, графический вариант ϖ буквы **пи** используется чрезвычайно часто (это стандартное обозначение

[70]Это германское начертание, которое профессионалы называют **фрактурой**, чтобы отличить его от 'латинского' начертания, называемого **антиквой**.

для фундаментальных весов в теории алгебр Ли), но подавляющее большинство математиков, которым не удалось прочесть греческих классиков в оригинале, считает, что это просто плохо пропечатанная ϖ — еще один повод вспомнить Канторовское 'wohlunterschiedene'! Чтобы различать эти начертания TEX использует различные командные последовательности, а именно,

\epsilon	\theta	\kappa	\pi	\rho	\sigma	\phi
ϵ	θ	κ	π	ρ	σ	ϕ
\varepsilon	\vartheta	\varkappa	\varpi	\varrho	\varsigma	\varphi
ε	ϑ	$\varkappa$	ϖ	ϱ	ς	φ

В качестве еще одного предостережения стоит упомянуть, что по-гречески буква **ипсилон** передает огубленный звук близкий к немецкому ü и поэтому υ порождается контрольной последовательностью \upsilon, а вовсе не \ipsilon, как можно было бы ожидать из русского чтения.

В продвинутых работах по теории множеств для обозначения бесконечных мощностей обычно используется еврейский алфавит Hebrew $= \{\aleph, \beth, \gimel, \daleth, \dots\}$ но, так как различать печатные (и, тем более, непечатные) еврейские буквы начинающему трудно, мы постараемся обойтись латинским и греческим алфавитами.

§ 5. Почему нельзя говорить о множестве зеленых яблок?

> В действительности, теория множеств не имеет ничего общего с научно-техническим прогрессом и не является новейшим достижением математики. Теоретико-множественная идеология приводит, например, к таким уродствам, как замена термина “равенство” геометрических фигур термином “конгруэнтность” и определение вектора как “параллельный сдвиг пространства”.
>
> Л.С.Понтрягин[71]

> Одиноко брожу средь толпы я
> И не вижу мне равного в ней.
> До чего же все люди тупые,
> До чего же их всех я умней.
>
> Все другие гораздо тупее,
> Нет такого, чтоб равен был мне.
> Лишь один себе равен в толпе я.
> Лишь один. **Да и то не вполне**.
>
> Игорь Иртеньев, Стихи разных лет

1. Внематематические примеры ‘множеств’. Во многих элементарных руководствах приводятся примеры ‘множеств’, ‘функций’ и ‘отношений’, якобы возникающие в ‘реальной жизни’. Так для наглядности поступаем и мы. Следует, однако иметь в виду, что все эти примеры носят метафорический характер: в окружающем нас мире нет ничего, что можно было бы воспринимать как множества **буквально** – множества принадлежат нашим **моделям** внешнего мира. Впрочем, то же самое относится ко всем математическим понятиям: в действительности они говорят нечто не о внешнем мире, а о нашем восприятии этого мира. В материальном мире как таковом нет не только никакого прямого аналога таких понятий, как ‘натуральное число’ (забудем про ‘вещественные числа’!), ‘точка’ или ‘прямая’, но и ничего, что бы делало необходимым введение именно этих понятий. Именно эта черта математики подчеркнута в замечательно точном определении фон Лейбница[72]: “Математика изучает все в области чистого умозрения, что поддается точному определению”.

---

[71] Л.С.Понтрягин, Анализ бесконечно малых, Наука, М., 1980, с.1–256.

[72] **Готтфрид Вильгельм фон Лейбниц** (01.07.1646, Лейпциг – 14.11.1716, Ганновер) – ключевая фигура в развитии математики и всей Европейской культуры. Кроме математики он занимался лингвистикой, историей, философией, геологией, был юристом, дипломатом и

2. Что такое ‘равенство’ элементов? Проблема с внешним миром состоит именно в том, что он не относится, по всей видимости, к области ‘чистого умозрения’ и мало что в нем ‘поддается точному определению’. Трудности возникают уже на уровне самых простых (и, поэтому, самых фундаментальных!) понятий, таких как равенство двух элементов или принадлежность элемента множеству. Понятие ‘равенства’, в смысле, передаваемом также словами ‘тождественность’, ‘идентичность’, ‘одинаковость’ не обладает свойствами, которые мы приписываем ему в математике. По-видимому, в макромире ни один объект ‘не равен самому себе’. Обычным выражением этого является фраза Гераклита ‘нельзя дважды войти в одну и ту же реку’. Впрочем, человек подсознательно воспринимает происходящие в природе процессы как непрерывные и поэтому Кратил возразил ему, что ‘нельзя войти и один раз’. Напротив, в микромире все объекты одного типа следует в самом строгом смысле рассматривать как ‘один и тот же’ объект. С этой точки зрения абсолютно бессмысленны примеры типа ‘множество атомов водорода на Солнце’.

В самой математике ‘равенство’ двух вещей есть **продукт соглашения** (“согласие есть продукт непротивления сторон”) и может в разных ситуациях пониматься по-разному. Достаточно вспомнить контроверзию об употреблении слов ‘равный’ и ‘конгруэнтный’ в школьной геометрии: что такое две ‘равные’ фигуры? Вскоре мы встретимся с употреблением слов ‘отображение’ и ‘семейство’, которые отличаются лишь используемым понятием равенства. В более продвинутых областях алгебры понятие ‘равенства’ объектов утрачивает всякое значение, и на первый план выдвигается понятие другое понятие ‘одинаковости’, а именно, ‘изоморфизм’. Еще на шаг дальше понятие ‘изоморфизма’ становится столь же бессмысленным, как понятие ‘равенства’, и на первый план выдвигается понятие ‘эквивалентности’ или ‘гомотопии’ и так далее.

3. Пример неопределенности, связанный с величиной множества. Рассмотрим различные издания одной и той же классической книги объемом, скажем, 500 страниц. Предположим, что в этой книге сделана 1000 опечаток (вполне реалистическая оценка снизу). Будем ли мы по прежнему воспринимать два различных экземпляра книги, с разными опечатками, как ‘одну и ту же’ книгу? (Эта проблема подробно обсуждается в рассказе Борхеса “Библиотека”). Возьмем какой-нибудь текст, который, с одной стороны, еще достаточно близок к современному языку, чтобы быть полностью понятным и не нуждаться в переводе, а, с другой стороны, существенно расходится с нормами современного языка орфографически (для большинства основных европейских языков временной границей является начало XVI века, хорошими примерами могут служить книги Рабле или Маргариты Наваррской, конечно, существуют гораздо более консервативные языки, чем русский, английский, немецкий или французский). Будет ли издание “Гаргантюа и Пантагрюэля” в оригинальной орфографии ‘той же самой’ книгой, что издание с модернизированной орфографией?

4. Примеры неопределенности, не связанные с величиной множеств. Может показаться, что все примеры неопределенности связаны с большой величиной рассматриваемых объектов. Однако даже на уровне самых маленьких ‘множеств’ совершенно неясно, какие элементы принадлежат им и сколько этих элементов. Мы уже приводили пример неопределенности, связанный с пониманием выражения ‘множество букв латинского алфавита’. Можно указать много других ситуаций, где неопределенность вовсе не связана с величиной, а возникает по совершенно другим причинам. Хрестоматийным является пример ‘множество великих русских романов XX века’ (принадлежит ли ‘Лолита’ этому множеству? – и если нет, то почему?). Даже такое невинное – и, по видимости, точное – выражение как ‘множество падежей современного русского языка’ моментально приводит к неразрешимой проблеме, что

архивистом Ганноверской фамилии. Учениками Лейбница были братья Бернулли, в свою очередь Леонард Эйлер был непосредственным учеником Иоганна Бернулли. Таким образом, Петербургская математика восходит к школе Лейбница. В 1663–1676 годах он развил дифференциальное и интегральное исчисление и ввел обозначения такие как $\int$ и dx, которые используются и сегодня. В 1679 в связи с поисками ‘универсального метода’, который должен свести рассуждения к вычислениям, он развил двоичную арифметику. К Лейбницу восходят десятки понятий, терминов и обозначений в университетских курсах, в том числе функция, определитель, дифференцирования колец, производная, дифференциальные уравнения, алгоритм, координаты, алгебраическое versus трансцендентного, круги Эйлера и т.д. Только очень немногие из этих понятий официально носят его имя: формула Лейбница, признак Лейбница ...

именно следует считать различными элементами этого множества (следует ли отличать вокатив от номинатива, партитив от генитива, и аблатив от предложного падежа?). Конечно, можно *постулировать* (как это делают авторы школьных учебников), что это множество состоит из 6 элементов, но любой непредвзятый морфологический анализ показывает, что в современном русском языке имеется по крайней мере 9 падежей с различными формами.

§ 6. Подмножества, включение

1. Включение, подмножества. В терминах отношения принадлежности можно определить несколько других отношений между множествами, важнейшее из них – это отношение **включения**.

Определение. *Если каждый элемент x множества A принадлежит множеству B, то говорят, что множество A* **содержится** *в множестве B, или что множество A является* **подмножеством** *в B и пишут $A \subseteq B$.*

Введенный в этом определении знак $\subseteq$ называется знаком **включения**, его TEXническое название `\subseteq`. По определению $A \subseteq B$ означает, что $x \in A \Longrightarrow x \in B$. Так же, как и знак принадлежности $\in$, знак включения $\subseteq$ часто пишется в другую сторону, а именно, $B \supseteq A$, TEXнически `\supseteq`, означает то же самое, что и $A \subseteq B$, но читается 'B является **надмножеством** A', 'B **включает** A' или 'B **содержит** A в качестве подмножества'. Заметим, что знак $\subset$ тоже был введен Пеано и сегодня обычно воспринимается как слегка деформированный знак неравенства $<$.

Комментарий. Впрочем, сам Пеано использовал его в противоположном смысле и записывал включение A в B как $A \supset B$ (из A следует B). Вероятно, это указывает на происходившую в его сознании борьбу экстенсиональной и интенсиональной точек зрения. Дело в том, что если P и Q два предиката, то

$$(P \Longrightarrow Q) \quad \Longrightarrow \quad \{x \in X \mid P(x)\} \subseteq \{x \in X \mid Q(x)\}.$$

Для отрицания включения знак $\subseteq$ перечеркивается. Таким образом, $A \not\subseteq B$ означает, что A не является подмножеством в B, т.е. что найдется такое $x \in A$, что $x \notin B$. Если $A \subseteq B$, но при этом $B \not\subseteq A$, то говорят, что A **строго (собственно) содержится** в B или что A является **собственным подмножеством** в B и пишут $A \subset B$. Знак $\subset$ называется знаком **строгого включения**, TEXнически `\subset`. Точно так же $B \supset A$, означает, что B является **собственным надмножеством** A или, что то же самое, B **строго (собственно) содержит** A. Знак $\supset$ TEXнически называется `\supset`.

2. Свойства включения. Знак $\subseteq$ должен напоминать, что отношение включения аналогично отношению неравенства $\leq$. Перечислим наиболее важные свойства включения.

- **Рефлексивность**: $A \subseteq A$;
- **Антисимметричность**: если $A \subseteq B$ и $B \subseteq A$, то $A = B$;
- **Транзитивность**: если $A \subseteq B$ и $B \subseteq C$, то $A \subseteq C$.

Свойства отношений $\supseteq$, $\subset$ и $\supset$ аналогичны свойствам $\geq$, $<$ и $>$, соответственно.

Рефлексивность означает, что каждое множество A является подмножеством себя самого. Подмножество $A \subseteq A$ называется обычно **несобственным** подмножеством множества A. В § 6 будет определено пустое множество $\varnothing$. Так как у пустого множества вообще нет элементов, то любой элемент пустого

множества является также элементом любого другого множества A и, значит, $\varnothing \subseteq A$. Это подмножество обычно называется **тривиальным**. Таким образом, каждое множество A имеет по крайней мере два подмножества, тривиальное и несобственное (которые могут, впрочем, совпадать между собой).

Комментарий: Равенство множеств. Антисимметричность в действительности является *определением* равенства множеств: два множества называются **равными**, если каждое из них является подмножеством другого. Это определение представляет собой переформулировку аксиомы объемности **ZF1**, которую мы подробно обсуждаем в § 5.

Отступление: Силлогизм Barbara. Транзитивность включения известна в традиционной логике под названием силлогизма Barbara: если любое A есть B и любое B есть C, то любое A есть C. Подобная цепочка включений обычно записывается как $A \subseteq B \subseteq C$. Вот классический пример верного рассуждения, основанного на этом силлогизме: "любая жаба есть млекопитающее, любое млекопитающее есть животное, следовательно, любая жаба есть животное". Обратите внимание, что мы не обсуждаем здесь справедливость посылок и заключения, а говорим лишь, что *если* посылки оценены как истинные, *то* и заключение должно быть оценено как истинное. А вот как использовал этот силлогизм Льюис Кэрролл: "Мясо, которое я ем на обед, – это мясо, которое я покупаю на рынке; мясо, которое я покупаю на рынке, – это сырое мясо. Поэтому мясо, которое я ем на обед, – это сырое мясо". Заметим, впрочем, что традиционная логика не отличала это рассуждение от рассуждения вида: если $x \in A$ и $A \subseteq B$, то $x \in B$.

3. Первые примеры подмножеств. Приведем несколько очевидных примеров подмножеств.

• Имеют место включения $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \overline{\mathbb{Q}}, \mathbb{R} \subseteq \mathbb{C}$. Из множеств $\overline{\mathbb{Q}}$ и $\mathbb{R}$ ни одно не содержится в другом;

• $2\mathbb{N}, \mathbb{P} \subseteq \mathbb{N}$;

• $\{1, 3, 5, 7\} \subseteq \mathrm{Digit}$;

• $\{a, b, c\} \subseteq \mathrm{Lat}$;

• Включение $\underline{m} \subseteq \underline{n}$ имеет место в том и только том случае, когда $m \leq n$;

§ 7. Логические парадоксы, антиномии и фанфрелюшки

> Votre conseil, dist Panurge, soubs correction, semble à la chanson de Ricochet: ce ne sont que sarcasmes, moqueries, paronomasies, épanalepses et redictes contradictoires. Les unes destruisent les aultres. Je ne sçai esquelles me tenir. — Aussi, repondit Pantagruel, en vos propositions tant y ha de Si et de Mais, que je n'y sçaurons rien fonder, ne rien résouldre.
>
> François Rabelais[73]

> Когда Больцман почти столетие назад сформулировал H-теорему, то против нее были выдвинуты возражения на том основании, что она ведет к "парадоксам". Мы упоминаем об этих "парадоксах" только ввиду их исторического интереса. Парадокса здесь нет, поскольку утверждение, на которое он опирается, ошибочно.
>
> Керзон Хуанг[74].

[73] 'Ваши советы, сказал Панург, если не ошибаюсь, напоминают песенку о Рикоше: одни лишь сарказмы, насмешки, парономазии, эпаналепсии и нескончаемые противоречия. Одни из них разрушают другие. Я не знаю, какого из них придерживаться. — Точно также, ответил Пантагрюэль, и в ваших предложениях содержится столько 'Если' и столько 'Но', что я не смог бы ни одного из них обосновать и ничего доказать.' — Книга III, Глава X. **Парономазия** — сопоставление или смешение **паронимов** (различных по значению, но близких по звучанию слов), игра слов, основанная на созвучии, каламбур; **эпаналепсия** — повторение слов.

[74] К.Хуанг, Статистическая механика – М., Мир, 1966, 520с.

Epimenides to Buddha: I have come to ask a question. What is the best question to be asked, and what is the best answer to be given?

Buddha: The best question that can be asked is the question you are asking, ans the best answer that can be given is the answer I am giving.

R.Smullyan

Множество чайных ложек само не есть чайная ложка, а множество вещей, не являющихся чайными ложками, есть одна из вещей, не являющихся чайной ложкой.

Бертран Рассел, 'Мое философское развитие'

Острие критики логических парадоксов было нацелено на содержащееся в них допущение, что для любого свойства $P(x)$ существует соответствующее множество всех элементов x, обладающих свойством $P(x)$. Стоит лишь отвергнуть это допущение, и логические парадоксы становятся невозможными.

Эллиот Мендельсон[75]

Точно так же и в наши дни маленькие шутки вносят беспорядок в математические теории. Мы называем их парадоксами. Парадокс Перрона состоит в следующем. Пусть N наибольшее положительное целое число. Тогда для $N \neq 1$ мы имеем $N^2 > N$, что противоречит определению N как наибольшего. Следовательно, $N = 1$. Последствия этого парадокса разрушительны. Решая задачу мы теперь уже не можем предполагать, что решение существует. Странно, что столь очевидная логическая ошибка так долго оставалась незамеченной.

Лоренс Янг[76]

And the more he looked inside, the more Piglet wasn't there.

A.A.Milne, 'The house at Pooh corner'

Первую группу парадоксов[77,78,79], Рамсей назвал **логическими парадоксами**, это парадоксы, относящиеся к *форме* высказываний.

---

[75]Э.Мендельсон, Введение в математическую логику. – М., Наука, 1971, с.1–320, стр.10.

[76]Л.Янг, Лекции по вариационному исчислению и теории оптимального управления. – Мир, М., 1974, с.1–488. стр.41–42.

[77]**Парадокс** — справедливое высказывание или суждение, *кажущееся* неожиданным, нелепым или противоречивым (но в действительности не являющееся таковым!!): 'A statement seemingly absurd or contradictory, yet in fact true' — FW. Большинство парадоксов основано на использовании неявных предположений (hidden assumptions) и сразу снимаются, как только мы эксплицируем эти предположения и поймем, что в действительности утверждается. Сократический метод обучения состоит в том, чтобы ставить ученика перед парадоксом, обдумывая который ученик должен самостоятельно прийти к новым идеям. Примерно такую же роль играют коаны в методе дзенских учителей.

[78]Парадоксы следует отличать от антиномий. **Антиномия** — беззаконие, противоречие, особенно противоречие в законе или между законами. В противоположность парадоксу, который лишь *кажется* противоречием, антиномия указывает на *действительное* противоречие. Поскольку никаких противоречий в теории множеств никогда не было, в дальнейшем я вообще не упоминаю об антиномиях. В частности, я говорю о **парадоксе** Рассела, хотя сам Рассел ошибочно считал его **антиномией**, т.е. подлинным противоречием. В народном языке часто допускается метатеза, приводящая к смешению слов **антиномия** и **антимония** (**антимония** — сурьма, рвотный порошок), откуда **разводить антимонии**. Как указывает Фасмер, правильно говорить **разводить антиномии**. Это выражение как нельзя лучше описывает деятельность некоторых философов и логиков.

[79]Парадоксы следует отличать также и от фанфрелюшек, таких как, скажем, софизмы.

1. Парадокс Рассела. Напомним, в чем именно состояли эти так называемые 'парадоксы теории множеств'. Все эти парадоксы связаны с принятием следующего абсурдного предположения.

Аксиома Фреге. *Для любого свойства P существует множество $\{x \mid P(x)\}$ всех объектов x, обладающих свойством P.*

В 1902 году Рассел заметил, что принятие этой аксиомы ведет к противорию[80]. Рассмотрим предикат $P(x) = (x \notin x)$. Аксиома Фреге утверждает, что существует множество $X = \{x \mid x \notin x\}$.

Парадокс Рассела. *Пусть X – множество всех множеств, которые не являются собственными элементами. Тогда X в том и только том случае является собственным элементом, когда оно не является собственным элементом.*

Доказательство. Предположим, что $X \in X$. Тогда X является собственным элементом и, значит, не входит в X по определению X. Таким образом, $X \in X \Longrightarrow X \notin X$. С другой стороны, если $X \notin X$, то X не является собственным элементом и, значит, входит в X по определению X. Таким образом, $X \notin X \Longrightarrow X \in X$.

По этому поводу стоит заметить, что сам Кантор не только **никогда** не пользовался предположениями, подобным аксиоме Фреге, но уже лет за 20 до парадокса Рассела *тщательнейшим образом* различал **множества** (Mengen) и **совокупности**[81] (Gesamtheiten, Vielheiten, Totalitäten, Unmengen), которые слишком велики для того, чтобы быть множествами и чтобы к ним можно было применять стандартные процедуры образования новых множеств. Совокупности, к которым неприменима его теория **трансфинитных** множеств, Кантор называл **абсолютно бесконечными**. Иными словами, уже в 1880-х годах Кантору были известны не только сами парадоксы, но и способ их преодоления, по существу эквивалентный предложенной Дж.фон Нейманом теории классов.

2. Классические формулировки парадокса Рассела. Парадокс Рассела можно сформулировать и не используя теорию множеств, Этот парадокс является одной из удачных рефлексивных шуток и с незапамятных времен известны десятки рефлексивных шуток на тему 'Every rule has an exception, except this one', etc. Вот три классические формулировки этого парадокса.

Парадокс парикмахера. Вождь афинской демократии Клисфен повелел, чтобы единственный парикмахер города брил тех и только тех граждан Афин, которые не бреются сами. Должен ли парикмахер брить себя?

Парадокс каталога. Библиотека Борхеса[82] решила составить библиографический каталог ('каталог каталогов'), в который входят те и только те каталоги, которые не включают себя. Включает ли такой каталог[83] себя?

Фанфрелюшка — мелочь, пустяк, безделушка, безделица, дешевое украшение. В следующем параграфе примерно в том же значении используется кодовое слово **лаппалия**. Лаппалия указывает на отсутствие смысла и бесполезность, в то время как фанфрелюшка — на суетность, легкомыслие и безвкусие. **Софизм** — *заведомо* ложное высказывание (ложность которого известна говорящему!), доказываемое при помощи рассуждений, *кажущихся* правильными: 'a false argument intentionally used to deceive' — FW.

[80]Письмо Рассела Фреге можно найти в книге J.van Heijenoort, From Frege to Gödel, a source book in Mathematical Logic, 1879–1931. – Harvard Univ. Press, Cambridge, Mass., 1967. Кроме того, эта книга содержит переводы оригинальных статей Бурали-Форти, Цермело и других с подробными комментариями.

[81]Такие, например, как совокупность всех множеств, совокупность всех ординальных чисел, совокупность всех алефов и т.д.

[82]'Вселенная, некоторые называют ее Библиотекой, состоит из огромного, возможно, бесконечного числа шестигранных галерей' – Х.Л.Борхес, 'Вавилонская библиотека', – Собр. Соч., т.1, Полярис, М., 1997, с.341–348.

[83]Это не парадокс, а исторический факт: в 1765 году в Вене был опубликован каталог запрещенных публикаций, однако публика использовала его как руководство к поиску интересных книг, поэтому через 12 лет этот каталог был включен в себя.

Парадокс самоуважения. Имеет ли профессор Конте самоуважение, если он уважает только тех, кто не уважает себя?

3. Парадоксы Кантора и Бурали-Форти. Другими близкими парадоксами являются парадоксы Кантора и Бурали-Форти.

Парадокс Кантора. *Как известно, мощность множества 2^X подмножеств любого множества X строго больше, чем мощность самого множества X. Но если X - множество всех множеств, то 2^X является подмножеством X и, следовательно, мощность 2^X не превосходит мощности X.*

Парадокс Бурали-Форти[84] – это версия парадокса Кантора, в которой рассматриваются ординальные числа вместо кардинальных. Заметим, что это первый из *опубликованных* парадоксов – статья Бурали-Форти появилась за 6 лет до книги Рассела[85]. Однако в действительности, как ясно из текста одного из писем Кантора Гильберту 1896 года этот парадокс был известен самому Кантору не позже 1895 года ("То, что получил Бурали-Форти – сущая чепуха."). Напомним, что ординалом называется вполне упорядоченное множество.

Парадокс Бурали-Форти. *Является ли множество X всех ординалов, упорядоченное по включению, ординалом? Если ответ положительный, то X должно быть своим собственным элементом и, значит, $X < X$.*

4. Объяснение логических парадоксов. Легко видеть, что в действительности все эти парадоксы не содержат в себе ничего парадоксального и математики повседневно сталкиваются с подобными ситуациями. Чтобы обьяснить, в чем тут дело, дадим еще одну эквивалентную переформулировку парадокса Рассела.

Парадокс Пиглета. Пусть n – такое целое число, которое одновременно больше и меньше нуля. Тогда n в том и только том случае является положительным, когда оно является отрицательным.

Но ведь такого числа не существует, воскликнет здесь каждый. Вот именно! **Все** "логические парадоксы" (не путать с "лингвистическими" или "семантическими" парадоксами, типа парадокса лжеца) построены по следующей схеме: предположим, что **существует** некоторый обьект X, тогда этот обьект X одновременно обладает и не обладает некоторым свойством. Но это в точности и значит, что требуемого обьекта X **не существует**, именно так устроены доказательства **от противного**, например, доказательство иррациональности числа $\sqrt{2}$ или бесконечности множества простых чисел. **Единственная** разница состоит в том, что в парадоксе Пиглета противоречивость условия очевидна сразу, а в парадоксе Рассела условие **не кажется** противоречивым – хотя и является таковым! Таким образом, парадокс Рассела всего лишь доказывает (от противного), что **не существует** множества $y = \{x \mid x \notin x\}$ всех множеств, не являющихся собственными элементами, и, тем самым, **не для любого** свойства P обязано существовать множество $\{x \mid P(x)\}$. Но никто из серьезных математиков никогда и не утверждал, что **любое** свойство должно определять множество, во всяком случае, Канторовское определение говорит нечто совершенно другое! В действительности, для любого свойства P из двух свойств P и $\neg P$ не более одного является коллективизирующим. Таким образом, не более чем одна из формул $\{x \mid P(x)\}$ и $\{x \mid \neg P(x)\}$ может определять некоторое множество. Пока начинающий не в состоянии судить, какая из этих формул имеет смысл, он должен полностью избегать обозначение $\{x \mid P(x)\}$.

5. Теорема Кантора-Рассела. Таким образом, 'парадокс' Рассела есть в действительности никакой не парадокс, а *теорема*, показывающая, что *не существует* множества всех множеств. В действительности этот факт был известен еще самому Кантору и, конечно, не является никаким 'парадоксом' (Бурбаки [Бу] и не называет этот факт парадоксом).

Теорема. *Никакое множество не может содержать все множества в качестве элементов.*

Доказательство. Допустим, что существует множество всех множеств x. Тогда по аксиоме **ZF6′** существует множество $y = \{z \in x \mid z \notin z\}$, и, как мы только что видели, $y \in y$ в том и только том случае, когда $y \notin y$, так что y, а вместе с тем и x не существует.

---

[84] **Бурали-Форти** (1861–1931)

[85] C.Burali-Forti, Una questione sui numeri transfiniti. – Rend. Circolo Mat. Palermo, 1897, vol.11, p.154–164.

6. Существование бога. В действительности парадокс полностью аналогичный парадоксу Рассела – и решающийся таким же образом – широко обсуждался средневековыми софистами.

Парадокс всемогущества. Допустим, бог всемогущ. Может ли он создать камень, который он не может поднять?

Разумеется, любой ответ показывает, что бог не всемогущ и, значит, условие всемогущества бога (а, тем самым, и определение бога христианскими теологами, включающее это условие) является внутренне противоречивым. Теологи возражали на это, что бог не обязан подчиняться человеческой логике[86].

§ 8. Семантические парадоксы

Rien ne m'est seur que la chose incertaine;
Obscur, fors ce qui est tout evident;
Doubte ne fais, fors en chose certaine;
Science tiens a soudain accident.

François Villon[87]

Les fanfreluches antidotées ...

François Rabelais[88]

'I don't think –' 'then you shouldn't talk'.

Lewis Carroll,

And the more he looked inside, the more Piglet wasn't there.

A.A.Milne, 'The house at Pooh corner'

Вторую группу парадоксов Рамсей[89] назвал **семантическими парадоксами**, это парадоксы, связанные со *смыслом* высказываний. По существу все они относятся к тому языку, на котором сформулированы и поэтому называются также **лингвистическими парадоксами**.

1. Парадокс лжеца. Наиболее древний из языковых парадоксов – знаменитый **парадокс лжеца**, который известен в нескольких различных формах.

---

[86] Я, конечно, не знаком с литературой по вопросу, но отголоски этой дискуссии отчетливо слышны на многих страницах книг Рабле и Стерна: ''Tis above reason, cried the doctors on one side. — 'Tis below reason, cried the others. — 'Tis faith, cried one. — 'Tis a fiddlestick, said the other. — 'Tis possible, cried the one. — 'Tis impossible, said the other. — God's **power** is infinite, cried the Nosarians; he can do anything. — He can do nothing, replied the Antinosarians, which **implies contradictions**.' — Lawrence Sterne, The life and opinions of Tristram Shandy, gentleman, vol. IV, Slawkenbergius's tale. С точки зрения теории множеств наибольший интерес в этом отрывке представляют следующие два момента: замечание о том что **мощность** Бога бесконечна и утверждение, что Бог не может создать ничего, что **влечет противоречия**.

[87] F.Villon, Oeuvres. – Радуга, М., 1984, с.1–512; стр.274. Все известные мне русские поэтические переводы **грубо** искажают смысл именно этого фрагмента, поэтому даю свой русский подстрочник: '1) Я ни в чем не уверен, кроме сомнительных фактов; 2) ничто не является темным, кроме того, что совершенно очевидно; 3) я ни в чем не сомневаюсь, кроме бесспорных фактов; 4) знание представляется мне неожиданной случайностью'. Для сравнения, вот как соответствующие строки передает Эренбург, в том порядке, как они появляются в его переводе: '2) мне темен свет, ясны и близки тени; 3) я сомневаюсь в явном, верю чуду; 1) мне постоянство видится в измене; 4) и случай мне важнее всех учений'. Здесь, как и всюду, Эренбург пытается *улучшить* Вийона, внося чуждые оригиналу слезливость и экзальтацию. Между тем, интонация самого Вийона ироническая и отстраненная.

[88] '... безвредные (обезвреженные) фанфрелюшки ...'

[89] **Ф.Рамсей** (1903–1930)

Парадокс Эвбулида. *Некто произносит следующую фразу: "Высказывание, которое я сейчас произношу, ложно". Это высказывание в том и только том случае истинно, когда оно ложно.*

Парадокс Эпименида. *"Все утверждения, сделанные критянами, ложны". Следует иметь в виду, что автор этого высказывания, Эпименид, сам критянин, так что если это высказывание истинно, то оно ложно. С другой стороны, если оно ложно, то это означает, что некий критянин некогда произнес истинное утверждение. Само по себе это не является логически невозможным, но представляется довольно удивительным, как произнесение Эпименидом этого ложного высказывания может повлечь некий эмпирический факт, а именно, существование критянина, который не лжет.*

Эти парадоксы произвели громадное впечатление на греков, согласно легенде они привели к самоубийству Филита Косского. Идея этих парадоксов положена в основу доказательства **теоремы Геделя о неполноте**. Парадоксу Эвбулида можно придать и следующую более драматическую форму, тоже известную с древности.

Дилемма[90] **крокодила.** Крокодил украл ребенка и обещал вернуть его отцу, если тот отгадает, вернет ли ему крокодил ребенка. Как должен поступить крокодил, если отец скажет, что крокодил не вернет ребенка?

Если Вы поняли механизм этих парадоксов, то Вам ничего не стоит решить следующую задачу.

Задача: Миссионер и людоеды. Людоеды решили, что миссионер надоел им своими проповедями и давно пора использовать его по прямому назначению. Однако, поскольку они уже прониклись духом христианского милосердия, они разрешают миссионеру произнести какое-нибудь высказывание с тем условием, что если высказывание окажется истинным, его сварят, а если ложным – зажарят. Что должен сказать миссионер?

Очень похожая задача содержится в "Приключениях хитроумного идальго дон Кихота из ла Манчи", Часть 2, Глава 51. Эта задача по-существу эквивалентна предыдущей, но людоеды называются в ней по-испански чиновниками.

Задача Санчо Пансы. Вот, что говорится в тексте: "Señor, un caudaloso río dividía dos términos de un mismo señorío. Y esté vuestra merced atento, porque el caso es de importancia y algo dificultoso. Digo, pues, que sobre este río estaba un puente, y al cabo de él, una horca y una como casa de audiencia, en la cual, de ordinario, había cuatro jueces que juzgaban la ley que puso el dueño del río, del puente y del señorío, que era en esta forma: "Si alguno pasare por esta puente de una parte a otra, ha de jurar primero adónde y a qué va; y si jurare verdad, déjenlo pasar, y si dijere mentira, muera por ello ahorcado en la horca que allí se muestra, sin remisión alguna." ... Sucedió, pues, que tomando juramento a un hombre, juró y dijo que para el juramento que hacía, que iba a morir en aquella horca que allí estaba, y no a otra cosa." Русский пересказ: "Некое поместье разделяется на две половины рекой, через которую переброшен мост, рядом с которым стоит виселица. Под этой виселицей четыре чиновника тщательно следят за соблюдением закона, согласно которому всякий, проходящий по мосту через реку, должен под присягой объявить, куда и зачем он идет. При этом тех, кто говорит правду, следует беспрепятственно пропускать, а тех, кто солжет, тут же отправлять на стоящую рядом виселицу. Что следует сделать с человеком, который под присягой заявил, что пришел затем, чтобы его вздернули на эту самую виселицу и ни за чем другим?"

Отступление: история парадокса лжеца. Герман Вейль дает следующее вдохновенное описание истории этих парадоксов: "Сократические философы мегарской школы – Эвклид, Эвбулид и другие – упивались парадоксами этого сорта, принадлежавшими, очевидно, к другому сорту утверждений, чем парадоксы движения элеатов, сформулированные Зеноном.

---

[90] **Дилемма** — выбор из *двух* взаимоисключающих возможностей. Примерно то же самое, что альтернатива, но с обертонами. Дилемма подразумевает невозможность, насильственность или затрудненность выбора: обе возможности представляются одинаково неприятными, пугающими или зловещими. Вен.Ерофеев иллюстрирует понятие дилеммы следующими примерами: 'Дилемма: лежать–ночевать в болоте с лягушками или в крапиве', 'Идешь направо — дурь находит, налево — Брежнев говорит'; 'Прямо пойдешь — жить не будешь, налево пойдешь — жизнь потеряешь, вправо пойдешь — умрешь, назад пойдешь — околеешь'.

Аристотель посвящает им целую книгу “De Sophisticis Elenchis”, интенсивно занимается ими стоик Хрисипп. Во времена Римской империи они образовывали составную часть школьного курса диалектики. Средневековое схоластическое развитие достигает кульминации у Павла Венетуса, умершего в 1428 году ... Типичным для отношения более современных философов является презрительное замечание К.Прандтля в его классической “Истории логики на Западе”: “Lappalien, wie die Mehrzeit der Fangschlüsse sind, wird die wahre Logik überhaupt nicht berücksichtigt” ”.

2. Парадоксы самоприменимости. Еще одна группа рефлексивных парадоксов была придумана в начале XX века в период дискуссии об основаниях математики. Следующий парадокс был замечен К.Греллингом и Л.Нельсоном в 1908 году, причем сами они считали его просто вариацией на тему Рассела.

Парадокс Греллинга. *Некоторые русские прилагательные сами обладают тем свойством, которое они описывают. Например, прилагательное ‘русский’ само является русским, прилагательное ‘многосложный’ само является многосложным, прилагательное ‘абстрактный’ само является абстрактным, и т.д. Назовем такие прилагательные* **автологичными**. *В то же время большинство прилагательных не обрадает этим свойством, так, например, прилагательное ‘английский’ само не является английским, прилагательное ‘односложный’ само не является односложным, прилагательное ‘конкретный’ само не является конкретным, прилагательное ‘рыжий’ само не является рыжим. Назовем такие прилагательные* **гетерологичными**. *Является прилагательное ‘гетерологичный’ автологичным или гетерологичным?*

Этот парадокс аналогичен парадоксу Рассела, но, разумеется, не может быть решен таким образом, поскольку прилагательное ‘гетерологичный’ существует. Ниже мы объясним, в чем тут дело. Следующий парадокс[91], является упрощенной версией **парадокса Ришара**[92,93].

Парадокс Берри. *Выражение “наименьшее целое число, которое не может быть описано по-русски менее, чем четырнадцатью словами” само содержит 13 слов и описывает некоторое целое число.*

Приведем теперь первоначальную формулировку опубликованного в 1905 году парадокса Ришара[94], так как она хорошо иллюстрирует идею Канторовского диагонального процесса (в действительности, в первоначальном варианте, принадлежащем самому Ж.Ришару, речь как раз и шла о вещественных числах).

Парадокс Ришара. *Рассмотрим всевозможные арифметические функции $f : \mathbb{N} \longrightarrow \mathbb{N}$, которые можно описать конечной фразой на русском математическом языке. Так как используемый при этом алфавит конечен, то имеется лишь счетное число таких функций, перенумеруем их: $f_1, f_2, \ldots$. Рассмотрим теперь функцию f, значение которой в $n \in \mathbb{N}$ определяется $f(n) = f_n(n) + 1$. Эта фраза описывает некоторую функцию, так что найдется такой номер n, что $f = f_n$. Но это невозможно, так как $f(n) \neq f_n(n)$.*

Конечно, при чуть более внимательном рассмотрении выясняется, что парадокс Ришара вообще не является парадоксом[95], так как в действительности приведенная в нем фраза не определяет никакой арифметической функции, по крайней мере до тех пор, пока не указан способ нумерации функций $f_1, \ldots, f_n, \ldots$ – на это обстоятельство обратил внимание сам Ришар. Эмиль Борель[96] предложил более глубокое объяснение. А именно, он указал, что нет никаких оснований полагать, что бесконечное подмножество счетного множества само счетно: множество всех фраз счетно, но это еще совершенно не значит, что и множество тех из них, которые действительно определяют какую-то арифметическую функцию, тоже счетно.

---

[91] B.Russell, Les paradoxes de la logique. – Revue de la metaphysique et de la morale, 1906, vol.14, p.627–650; page 645.

[92] Х.Карри, Основания математической логики. – М,, Мир, 1969, с.1–568; стр.24.

[93] С.Клини, Математическая логика. – М., Мир, 1973, с.1–480; стр.222–223.

[94] J.Richard, Les principes des mathématiques et le problème des ensembles. – Acta Math., 1905, vol.30, p.295–296.

[95] ‘Exemplo de Richard non pertinet ad mathematica, sed ad linguistica’ – G.Peano.

[96] E.Borel, Les “paradoxes” de la théorie des ensembles. – Ann. Sci. Ecole Norm. Sup., 1908, vol.25, p.443–448.

Как мы узнаем в главе 4, это можно доказать только используя аксиому выбора. Тем самым, функции, которые можно описать конечной фразой, вообще невозможно занумеровать.

Традиционные объяснения семантических парадоксов. Согласно мнению Рамсея, в формулировки семантических парадоксов входят понятия, не принадлежащие математике и логике, например, понятие истинности, поэтому их вообще незачем рассматривать. Рассел считал, что причиной возникновения всех перечисленных выше парадоксов является **самоприменимость** (self-reference), иными словами, все эти парадоксы являются **рефлексивными**. В **теории типов**, предложенной им и Уайтхедом в качестве основания математики, введен специальный механизм, позволяющий избежать самоприменимость. Однако в математике было бы нежелательно совсем отказываться от конструкций, использующих самоприменимость.

3. Объяснение семантических парадоксов. Легко видеть, что в действительности и все эти парадоксы не содержат в себе ничего парадоксального, а возникают в результате присущего естественному языку смешения понятий. Сформулируем еще один парадокс, в котором никакой самоприменимости нет, так что механизм возникновения семантических парадоксов становится более явным.

Парадокс Жихаря. *Рассмотрим два высказывания. "Жихарь светловолос и голубоглаз" и "Жихарь – мужское имя из шести букв". Из них с очевидностью следует, что существует светловолосое и голубоглазое мужское имя из шести букв.*

Но ведь здесь спутаны два значения слова 'Жихарь' – в первом из них речь идет о конкретном богатыре по имени Жихарь, а во втором – об имени 'Жихарь' как таковом. Вот именно! Ровно то же самое происходит во **всех** семантических парадоксах. В них одно и то же слово понимается в двух разных смыслах: как *имя* некоторого объекта и как *имя имени* этого объекта. Действительно, в естественных языках нет механизма, позволяющего различать уровни высказываний, например, отличать высказывания о реальности от высказываний о языке, которым мы описываем эту реальность, а их в свою очередь от высказываний о языке, которым мы описываем этот язык и так далее.

Предметный язык, метаязык, арго. Четкое различие между **предметным языком**, которым мы описываем неторый круг явлений, **метаязыком**, которым мы описываем этот предметный язык, **метаметаязыком**, которым мы описываем этот метаязык, и так далее, моментально устраняет все языковые парадоксы. Например, в парадоксе Греллинга помещенное в кавычки слово 'гетерологичный' относится к языку, описывающему язык, описывающий реальность, а не помещенное в кавычки – к языку, описывающему язык, описывающему язык, описывающий реальность. Однако последовательное проведение подобных различений не всегда удобно и, поэтому, в противоположность логикам, работающие математики редко строго его придерживаются, а пользуются общепринятым **арго** (термин Юрия Ивановича Манина из [Ma]) и полагаются на здравый смысл.

§ 9. Еще один рефлексивный парадокс

A new paradox offers the opportunity to recapture the sense of confusion and uncertainty that faced mathematicians in the early part of the twentieth century.

W.S.Zwicker[97]

— Пардон! — отозвался Фагот, — я извиняюсь, здесь разоблачать нечего, все ясно.

— Нет, виноват! Разоблачение совершенно необходимо. Без этого ваши блестящие номера оставят тягостное впечатление. Зрительская масса требует объяснения.

Михаил Булгаков, 'Мастер и Маргарита'

And the more he looked inside, the more Piglet wasn't there.

[97] W.S.Zwicker, Playing games with games: the hypergame paradox. – Amer. Math. Monthly, 1987, June-July, p.507–514.

A.A.Milne, 'The house at Pooh corner'

За прошедшие 100 с лишним лет описанные в двух предыдущих параграфах парадоксы порядком подрастеряли свою парадоксальность и воспринимаются сегодняшними математиками как общие места, привычные банальности, пригодные только для развлечения 'детей, народных масс и философов'. Однако нет ничего такого, что нельзя было бы назвать другим именем. Вот более свежий парадокс, который позволит даже профессионалу секунд на 30 ощутить ту растерянность, которая охватила математический мир в начале XX века[98,99,30].

1. Парадокс гиперигры. Рассмотрим детерминированную пошаговую антагонистическую игру двух лиц с полной информацией G. Это значит, что в эту игру играют два игрока A и B, которые по очереди делают ходы, причем A ходит первым. Каждый из них знает все ходы другого. В игре G нет никакого места случаю (типа выбрасывания костей и т.д.). В игре G невозможна ничья: когда игра закончена, в ней ровно один победитель. Назовем игру G **почти конечной**, если она удовлетворяет следующему условию:

i) Каждая партия заканчивается через конечное число ходов.

Назовем игру G **конечной**, если, кроме того,

ii) В каждый момент партии имеется лишь конечное число возможных ходов.

С учетом этих определений мы можем рассмотреть **суперигру**, правила которой таковы: игрок A делает первый ход, которым он выбирает любую конечную игру G. После этого A и B играют в игру G, первый ход в которой делает игрок B. Победитель в этой игре G провозглашается победителем суперигры. Может ли игрок A своим первым ходом передать ход игроку B, т.е. назвать суперигру? Нет, так как суперигра не является конечной: в начале игры у игрока A имеется бесконечное число возможных ходов, так как имеется бесконечное число конечных игр. Однако суперигра очевидным образом почти конечна.

Теперь рассмотрим **гиперигру**, которая играется по тем же правилам, что и суперигра, за исключением того, что первым ходом игрок A может назвать любую *почти* конечную игру G. Очевидный вопрос, является ли гиперигра почти конечной? С одной стороны, она, очевидно, удовлетворяет тому же условию i), что и суперигра, так что она должна быть почти конечной. С другой стороны, если она почти конечна, то в качестве первого хода игрок A может сказать 'гиперигра!'. После этого игрок B может ответить 'гиперигра!' и т.д. Таким образом, гиперигра не может быть почти конечной.

2. Пример разоблачения. Описание этого парадокса в книгах Шмульяна и Гарднера содержит неточность, так как там говорится, что если гиперигра не является почти конечной, то ее нельзя использовать в качестве первого хода, так что она является слабо конечной. Однако это рассуждение ошибочно, так как оно игнорирует возможность существования других почти конечных игр, которые могут приводить к бесконечным партиям в гиперигре. Правильное описание сущности этого парадокса приведено в статье Цвикера.

Постараемся, прежде всего, придать точный математический смысл тому, что описано в предыдущем пункте. Как проще всего промоделировать почти конечную игру G в теории множеств? Обычным способом изображения таких игр являются **укорененные деревья** (rooted trees), которые обычно изображаются растущими от корня вниз. В начале игры мы находимся в корне дерева, первый ход состоит в том, что мы выбираем одно из растущих из корня ребер и спускаемся по нему на один уровень в следующую вершину. После этого второй ход состоит в том, что мы выбираем ребро растущее вниз из этой вершины и спускаемся по нему еще на один уровень, и т.д. Терминальные вершины помечены A и B, чтобы указать на то, кто выиграл. Слабая конечность игры означает в точности, что это дерево **фундировано**, т.е. в нем нет бесконечных ведущих вниз путей. Конечность игры означает, кроме того, что каждая вершина этого дерева имеет конечную валентность, т.е. из нее выходит конечное число ребер.

Суперигра состоит в том, что мы склеиваем представители классов изоморфизма (**порядковые типы**) *конечных* укорененных деревьев. (В действительности, требуется еще

[98]R.Smullyan, 5000 B.C. and other philosophical fantasies. – St. Martin's Press, N.Y., 1983, pages 40–41.

[99]M.Gardner, Puzzles from other worlds: fantastical brainteasers from Isaac Asimov's science fiction magazine. – Randam House, N.Y., 1984, pages 60–61, 163.

поставить на терминальных вершинах метки A и B, так что типов игр больше, чем порядковых типов, но это не влияет на вопросы существования). Так как эти порядковые типы образовывают множество, такая операция возможна.

С другой стороны, гипериграа состоит в том, что мы склеиваем порядковые типы *всех* фундированных деревьев. Однако парадокс Бурали-Форти запрещает даже рассмотрение множества всех ординалов, которые соответствуют порядковым типам *линейно упорядоченных* фундированных множеств! А гипериграа включает порядковые типы *всех* (а не только линейно упорядоченных!) фундированных множеств. Значит никакой гипериграы не может существовать[100]. В действительности даже совокупность почти конечных игр, заканчивающихся победой игрока A на *первом шаге*, не образует множества, так как такие игры описываются кардинальными числами (алефами), которые не могут образовывать множества в силу парадокса Кантора. Таким образом, парадокс гипериграы является просто слегка завуалированной формой парадоксов Кантора и Бурали-Форти.

Все так называемые 'противоречия' снимаются как только мы готовы признать, акт именования не является одновременно актом творения: не все, что мы можем назвать, существует. 'Гипериграа' является таким же оксюмороном[101] как 'множество всех множеств', 'множество всех множеств, не являющихся собственными элементами', 'честный политик' и существует лишь как имя для обозначения фикции, которая не только не существует, но и не может существовать в действительности[102].

§ 10. Аксиоматика Цермело-Френкеля **ZFC**

> В мире все вещи рождаются в бытии, а бытие рождается в небытии.
>
> Дао дэ цзин, § 40.

> Существует начало и то, что еще не начало быть началом, а также то, что еще не начало быть тем, что еще не начало быть началом. Существует бытие, существует небытие, существует то, что еще не начало быть небытием, а также то, что еще не начало быть тем, что еще не начало быть небытием. Внезапно появляется небытие, и неизвестно, что же на самом деле существует, а что же не существует, бытие или небытие.
>
> Чжуан-цзы, Гл. 2.

> 1. Ни бытия не было тогда, ни небытия. Ни воздушного пространства, ни неба. Что двигалось? Где? Под чьей защитой? Состояла ли из воды глубокая бездна?
> 2. Ни смерти не было тогда, ни не-смерти; день и ночь не различались тогда. Само по себе, без дуновения, дышало лишь Это; и ничего не было, кроме Этого.

---

[100]По поводу этого утверждения Цвикер (ibid., page 510) замечает: "It is easy to have a strong gut reaction against this claim. How can a certain game fail to exist when the rules for playing are clear (but are they clear?). I have actually played Hypergame (or so I thought at the time) so how can it not have existed? These reactions show that achieving the shift in perspective in our gut is not so easy even when the mathematics is transparent. The reader might wish to sound his or her own heart on this question: does it seem *natural* that Hypergame is not a game? If not, do you feel a little more sympathy with those to whom Russell's paradox was baffling and important even after the publication of Zermelo's paper."

[101]Оксюморон – заведомая глупость, от греческого $o\xi\upsilon\varsigma$ – резкий, острый, кислый (откуда русское 'уксус') и $\mu o\rho o\varsigma$ – глупый (откуда русское 'морон'). Обычно употребляется в специальном техническом смысле, указывающем на сочетание заведомо противоречивых понятий: 'христианская наука', 'научный коммунизм', 'свобода и равенство', 'законность и справедливость', ...

[102]'Логическое направление является источником неисчерпаемого количества сущностей, существование которых в действительности лишь словесно' (Н.Н.Лузин, Собрание сочинений, т.2. Дескриптивная теория множеств. – Изд-во АН СССР, М., 1958, стр.23).

Ригведа, Гимн X, 129

В старину мудрые цари прозрели общую основу Неба и Земли в чередовании сил Инь и Ян. Но ежели все обладающее формой родилось из бесформенного, от чего же родились Небо и Земля? Я отвечаю: вначале была Великая Пустота, потом появилось Великое Начало, затем появилась Великая Основа, после чего появилась Великая Вещественность. В Великой Пустоте еще не было Логоса. Великое Начало было началом Логоса. Великая Основа была началом всех форм. Великая Вещественность — начало всех вещей. Логос, форма и вещь еще не отделились друг от друга, посему такое состояние зовется хаосом. Хаос означает смешение всех вещей, еще не отделившихся друг от друга. Всматривайся в него — и не увидишь, вслушивайся в него — и не услышишь. Посему он зовется Пустотой. Пустое не имеет ни формы, ни границ. Претерпев превращение, оно стало Единым, а из Единого оно стало семью, семь же превратилось в девять. На девятке превращения исчерпываются и снова приходят к единице. А это Единое есть начало превращений всех форм.

Ле Цзы, Гл. I, Небесная доля

Вначале был логос и логос был у бога и логос был бог.

Евангелие от Иоанна

Сначала не было ничего: ни земли, ни песка, ни холодных волн. Была лишь одна черная бездна Гиннунгагап.

Сказания о богах

В *ортодоксальной* теории Цермело-Френкеля **ZFC** существует единственный тип объектов – множества и единственный предикат $\in$. Множества и отношение принадлежности подчинены следующим девяти аксиомам **ZF1**–**ZF9**.

ZF1 (Аксиома экстенсиональности). *Два множества равны, $x = y$, если они содержат одни и те же элементы, т.е. если $z \in x \iff z \in y$.*

Определим отношения включения $x \subseteq y$ как $z \in x \Longrightarrow z \in y$. В этих обозначениях $x = y$ в том и только том случае, когда $x \subseteq y$ и $x \supseteq y$.

Замечание 1. Эта парадоксальная аксиома, называемая также **аксиомой объемности**, является *квинтэссенцией* теоретико-множественной точки зрения. Ее нетривиальность состоит, конечно, не в том, что два равных множества имеют одинаковые элементы, а в том, что два множества, имеющие одинаковые элементы, полагаются равными. Поясним это следующим примером, принадлежащим Расселу: множество двуногих без перьев равно множеству людей, но всякое рассуждение о том, будет ли двуногий без перьев (например, попавший в ощип петух) более способен, чем человек, развить оперение, находится вне сферы теории множеств, так как аксиома **ZF1 запрещает** различать два эти описания. Даже в самой математике это часто слишком суровое ограничение.

Замечание 2. Иногда приходится слышать, что вещь равна только себе самой. В действительности равенство, как и все остальное, является результатом соглашения, продуктом **непротивления сторон**. В качестве иллюстрации этого можно упомянуть, что в системе **NF** Куайна равенство множеств определяется не по Кантору, а по Лейбницу, т.е. двойственным образом как identitas indiscernibilium. А именно, два множества равны, если они содержатся в качестве элементов в одних и тех же множествах: $x = y$ если и только если $x \in z \iff y \in z$.

Множество, не содержащее ни одного элемента, называется **пустым множеством** и обозначается $\varnothing$. Это обозначение было введено Бурбаки (по предложению Андре Вейля), и представляет собой датскую (и норвежскую) букву ö. До сих пор мы не знаем, существует ли хотя бы одно множество. Следующая аксиома гарантирует, что одно множество определенно существует.

ZF2 (Аксиома существования). *Существует пустое множество.*

Заметим, что согласно аксиоме **ZF1** существует ровно одно пустое множество. По определению утверждение $x \in \varnothing$ ложно для любого x. Поэтому утверждение $x \in \varnothing \Longrightarrow P(x)$ или, что то же самое, $\forall x \in \varnothing, P(x)$ истинно для любого свойства P. Таким образом, **любой** элемент пустого множества обладает **любым** свойством (а также отрицанием этого свойства).

Комментарий. О том, что понятие пустого множества совершенно не очевидно, говорит хотя бы тот факт, что оно было введено лишь в конце XVII века фон Лейбницем под именем 'non Ens' ('небытие', 'не сущее'). Вся традиционная логика, следуя Аристотелю, признавала **правило конверсии**: "если всякое A есть B, то некоторое A есть B", явным образом подразумевающее, что A непусто. На нашем языке это означает, что из $A \subseteq B$ делается вывод, что $A \cap B \neq \varnothing$. Например, из посылки "все кентавры лысы" Аристотель делает вывод "существует лысый кентавр". Может быть лысый кентавр действительно существует (это не противоречит известным сегодня физическим законам), но с нашей сегодняшней точки зрения это никак не следует из посылки. Именно на игре с этим правилом построено большинство так называемых 'логических парадоксов' (парадокс Рассела и его родственники). Берется произвольный элемент пустого множества и выводится, что он обладает как свойством P, так и свойством $\neg P$, после чего все долго в недоумении смотрят на получившееся противоречие. Однако в действительности противоречие получается только при дополнительном предположении, что в пустом множестве есть хотя бы один элемент. Как говорится по этому поводу в 'Син-син-мей', "пустой ум свободен от противоречий".

Три следующие аксиомы и аксиома **ZF7** являются аксиомами свертывания, утверждающими, что существуют некоторые множества, построенные по строго определенным правилам.

ZF3 (Аксиома неупорядоченных пар). *Для любых двух вещей x и y существует множество $\{x, y\}$, единственными элементами которого являются x и y.*

В случае, когда $x \neq y$ множество $\{x, y\}$, существование которого утверждается в этой аксиоме, называется **неупорядоченной парой** с элементами x и y или просто **парой**. Такая пара называется неупорядоченной, потому что, согласно аксиоме **ZF1** пара $\{y, x\}$ равна паре $\{x, y\}$. В случае же, когда $x = y$, в силу той же аксиомы $\{x, x\} = \{x\}$, так что из **ZF3** вытекает, что для любого объекта x существует одноэлементное множество $\{x\}$, называемое еще **синглетоном**. Заметим, что в стандартной теории множеств ни для одной вещи x одноэлементное множество $\{x\}$ не может совпадать с x.

Комментарий: Зависимость аксиомы пары от остальных аксиом ZF. Как заметил Ян Мычельски, аксиома **ZF3** моментально вытекает из аксиом существования **ZF2**, степени **ZF7** и подстановки **ZF6**. В самом деле, $2^{2^{\varnothing}} = \{\varnothing, \{\varnothing\}\}$, после чего существование *любой* пары $\{a, b\}$ следует из аксиомы подстановки. Мы, однако, не будем заниматься такой ерундой, как исключение **ZF3** из списка аксиом **ZF**. В самом деле, аксиома **ZF3** носит гораздо более наглядный характер, чем каждая из аксиом **ZF6** и **ZF7**, достаточна для многих приложений и была введена для системы **Z**, где вместо аксиомы **ZF6** фигурировала лишь значительно более слабая аксиома подмножеств **ZF6′**, не позволяющая вывести **ZF3** из остальных аксиом. Вообще, навязчивое стремление логиков формулировать *независимые* системы аксиом представляется мне родом агрессивного безумия. С точки зрения математика гораздо важнее иметь удобные и наглядные системы аксиом, чем независимые.

Если x – любое множество множеств, то **объединением** его элементов называется множество $z = \bigcup y$, $y \in x$, состоящее из тех и только тех элементов, которые принадлежат по крайней мере одному из множеств $y \in x$. Согласно

этому определению для любого множества множеств X имеем

$$u \in z = \bigcup_{y \in x} y \quad \Longleftrightarrow \quad \exists y \in x, u \in y.$$

Однако пока совершенно непонятно, почему описанное в этом определении множество обязано *существовать*.

ZF4 (Аксиома объединения). *Для любого множества множеств x существует объединение $\bigcup y$, $y \in x$.*

Существование конечных множеств. Аксиомы **ZF3** и аксиомы объединения **ZF4**, утверждающей, что объединение любого множества множеств само является множеством (см. Глава 2) уже достаточно, чтобы доказать существование любых конечных множеств.

Задача. Докажите, что для любых трех вещей x, y, z существует множество $\{x, y, z\}$, единственными элементами которого являются x, y и z. Вообще, пусть $x_1, \ldots, x_n$ – любые n вещей, где $n \in \mathbb{N}$. Докажите, что существует множество $\{x_1, \ldots, x_n\}$, единственными элементами которого являются $x_1, \ldots, x_n$.

Решение. Пользуясь аксиомой **ZF3**, образуем пару $\{x, y\}$ и одноэлементное множество $\{z\}$. Тогда по аксиоме **ZF4** существует их объединение, которое равно $\{x, y, z\}$. Продолжим действовать рекурсивно. Допустим, мы уже знаем, что существует множество $\{x_1, \ldots, x_{n-1}\}$. По аксиоме **ZF4** можно образовать его объединение с одноэлементным множеством $\{x_n\}$.

Итак, из аксиом **ZF3** и **ZF4** вытекает, что любая конечная совокупность вещей образует множество. Смысл следующей аксиомы состоит в том, что существует хотя бы одно бесконечное множество. Разумеется, так как бесконечные множества еще не были нами определены внутри системы **ZF**, обычно эта аксиома формулируется как существование натурального ряда. При этом логики обычно считают, что натуральный ряд начинается с 0, т.е. фактически строят множество $\mathbb{N}_0$, которое они, к тому же, обычно обозначают через ω.

ZF5 (Аксиома бесконечности). *Существует такое множество ω, что $\varnothing \in \omega$ и для любого $x \in \omega$ имеем $\{x, \{x\}\} \in \omega$.*

Замечание. Эта аксиома – существование **актуально** бесконечных множеств – есть 'альфа' (но еще не 'омега', вопреки обозначению) Канторовской теории множеств и всей Канторовской математики. В окружающей нас действительности (и, тем более, в человеческом опыте) нет, по-видимому, **ничего** бесконечного. Концепция актуальной бесконечности представляет собой **свободное творение человеческого разума**, причем, как показывает вся история науки, совершенно не очевидное. Вот что пишет по этому поводу известный критик Канторовской математики Петр Вопенка: "В настоящее время существование актуально бесконечных множеств превратилось в догму, в которую верит большинство математиков; более того, математики пытаются внушить веру в эту догму и другим людям. В то же время мы не можем указать какое-либо актуально бесконечное множество в реальном мире – здесь мы имеем дело с конструкцией, расширяющей реальный мир и качественно превосходящей пределы наших наблюдений." Видимо, большинство профессиональных математиков согласится с фактической стороной этого замечания, но они видят в этом силу математики. Величие математики как раз и заключается в том, что она использует придуманные ей конструкции, использующие бесконечность, и, тем самым, **нетривиальным образом расширяющие реальный мир**, чтобы с их помощью решать вопросы, по самой своей сути относящиеся к конечному.

Следующая аксиома, называемая аксиомой подстановки, была введена Абрахамом Френкелем. С содержательной точки зрения ее смысл состоит в том,

что образ функции на множестве является множеством. Разумеется, так как понятие функции еще определено в рамках теории **ZF**, мы должны придать этому утверждению точный смысл.

ZF6 (Аксиома подстановки). *Допустим, что для любого x существует единственный y такой, что $F(x,y)$. Тогда для любого множества z существует единственное множество u, состоящее из всех y таких, что $x \in z$ и $F(x,y)$.*

Смысл аксиомы Френкеля состоит в следующем: если каждый элемент множества заменить некоторым множеством, то в результате снова получится множество. На самом деле, с учетом остальных аксиом, вместо аксиомы подстановки достаточно было бы сформулировать более слабое утверждение: любая совокупность, *эквивалентная* множеству, сама является множеством[103]. В сочетании с другими аксиомами, такими, как аксиома степени и аксиома объединения, аксиома подстановки позволяет строить громадные множества, представляющие интерес лишь для специалистов по аксиоматической теории множеств. Для всех приложений в обычной математике достаточно значительно более слабых предположений, например, следующей аксиомы, называемой **аксиомой подмножеств** (axiom of subsets) или **аксиомой выделения**, которая входила в первоначальную аксиоматику Цермело **Z**. Так как именно эта аксиома отличает **Z** как от аксиоматики Фреге, так и от аксиоматики Цермело-Френкеля **ZF**, именно ее (а вовсе не введенную Беппо Леви аксиому выбора!) естественно называть **аксиомой Цермело** (впрочем, на это название могли бы претендовать и остальные семь аксиом системы **Z**).

ZF6′ (Аксиома подмножеств). *Для любого множества x и любого свойства P существует множество всех $y \in x$ обладающих свойством P.*

Эта аксиома позволяет образовывать множество всех объектов, обладающих некоторым свойством, при условии, что они уже принадлежат некоторому множеству. Например, из нее немедленно следует существование пересечения $\bigcap y$, $y \in x$, любого множества множеств и разности $x \setminus y$ любых двух множеств. В сочетании с аксиомой объединения **ZF4** она позволяет образовать множество всех объектов, обладающих некоторым свойством, *при условии*, что они уже принадлежат каким-то (быть может различным) множествам.

Оказывается, даже аксиома бесконечности не позволяет строить сколь угодно большие множества. Ключевое открытие Кантора состояло в том, что множество всех подмножеств любого множества имеет мощность строго большую, чем само это множество. Однако пока мы не знаем, можно ли соединить все подмножества данного множества x в множество. Для бесконечного множества x это не вытекает из остальных аксиом, даже с учетом аксиомы подстановки **ZF6**. Поэтому возможность такого соединения должна постулироваться отдельно. Следующая удивительная аксиома была введена Кантором.

ZF7 (Аксиома степени). *Для любого множества x существует множество z такое, что $y \in z$ в том и только том случае, когда $y \subseteq x$.*

Множество z существование которого утверждается этой аксиомой, обычно обозначается 2^x и называется **булеаном** x. По определению, $y \in 2^x \iff y \subseteq x$.

[103]В действительности, в такой форме ее рассматривал сам Кантор в 1899 году.

Следующая аксиома – аксиома выбора – является наиболее известной из всех. По совершенно загадочным причинам это *единственная* аксиома, которая упоминается на первых страницах любого учебника по математическому анализу. Мы сформулируем аксиому выбора в исторически первой и наиболее простой форме – **аксиому Леви**[104]. В § ? мы дадим еще несколько эквивалентных формулировок этой аксиомы (в форме Цермело, в форме Рассела, в форме Хаусдорфа, в форме Куратовского-Цорна, в форме Тарского и т.д.). Напомним (подробнее по поводу отображений см. § ?), что отображение $f : X \longrightarrow Y$ называется **сюръективным**, если для любого $y \in Y$ существует $x \in X$ такое, что $f(x) = y$.

ZF8 (Аксиома выбора). *Пусть $f : X \longrightarrow Y$ – сюръективное отображение. Тогда существует отображение $g : Y \longrightarrow X$ такое, что для любого $y \in Y$ имеет место равенство $f(g(y)) = y$.*

Иными словами, эта аксиома утверждает, что существует такое подмножество $Z \subseteq X$, которое пересекается с каждым слоем отображения f ровно по одному элементу (т.е. такое, что ограничение $f|_Z$ отображения f на Z биективно).

ZF9 (Аксиома регулярности). *Пусть $y \neq \varnothing$. Тогда существует такой элемент $x \in y$, что для любого элемента $z \in y$ выполняется $z \notin x$.*

Аксиома регулярности запрещает существование множеств x таких, что $x \in\in x$. В самом деле, эта аксиома явным образом запрещает принадлежность $x \in x$, так как иначе в множестве $\{x\}$ не было бы элемента, который не содержит ни одного элемента этого множества. Кроме того, **ZF9** запрещает одновременное выполнение включений $x \in y \in x$. Точно так же, не существует трех вещей x, y и z, для которых $x \in y \in z \in x$, и так далее.

§ 11. Системы фон Неймана и Геделя-Бернайса **GB**

> В диаметре Алеф имел два-три сантиметра, но было в нем все пространство вселенной, причем ничуть не уменьшенное. Каждый предмет был бесконечным множеством предметов, потому что я его ясно видел со всех точек вселенной.
>
> Хорхе Луис Борхес, Алеф

Мы уже упоминали теорию **ZFU**, в которой существуют праэлементы. Есть много других теорий, которые заметно отличаются от **ZF**. Только одна из этих систем, а именно, система Геделя-Бернайса **GB**, получила такое же распространение как система **ZF**.

1. Аксиоматика фон Неймана, идея класса. В 1925–28 годах фон Нейман предложил[105] оригинальную аксиоматику теории множеств **N**, основанную не на понятиях множества и

[104] **Беппо Леви**

[105] **Джон (alias Янош, Иоганн) фон Нейман** (28.12.1903, Будапешт – 08.02.1957, Вашингтон) – один из самых замечательных и влиятельных математиков XX века, автор почти 200 статей и 10 книг по различным вопросам математики и ее приложений. С 1927 года преподавал в Берлине и Гамбурге, а в 1930 году эмигрировал в США, где работал в Принстоне, сначала в Принстонском Университете, а начиная с 1933 в Institute for Advanced Studies (вот полный список первых шести постоянных профессоров IAS: Дж.Александер, А.Эйнштейн, М.Морс, О.Веблен, Дж.фон Нейман, Г.Вейль). После ранних работ по основаниям теории множеств и логике фон Нейман заинтересовался функциональным анализом, в особенности в его алгебраических аспектах. Среди вершин его творчества в этом направлении можно упомянуть спектральную теорему для операторов в гильбертовом пространстве, эргодиче-

принадлежности, а на понятиях функции и упорядоченной пары[106]. Мы не будем пытаться здесь вопроизвести или прокомментировать эту чрезвычайно сложную систему. Однако одна из ключевых идей, положенных в основу этой системы, получила в дальнейшем развитие в другом направлении. Эта идея состоит в том, что парадоксы обусловлены не существованием "больших" множеств, а тем, что этим "большим" множествам разрешается входить как элементы в другие множества. Таким образом, фон Нейман предложил ввести новое понятие **класса**. При этом класс, который может входить в качестве элемента в какой-то другой класс, называется множеством, а классы, которые не входят как элементы ни в какой класс называются **собственно классами**. Собственно классы обладают всеми интуитивными свойствами множеств, кроме того, что они не могут быть элементами других классов и, тем самым, для них нельзя определить класс всех подклассов. Аксиома Фреге теперь справедлива для классов – т.е. для любого свойства можно образовать *класс*, состоящий из всех множеств, обладающих этим свойством, – но не ведет к противоречию. Например, можно непротиворечивым образом говорить о **классе всех множеств**.

2. Аксиоматика Геделя-Бернайса. Построенная в 1937 году **система Геделя-Бернайса**[107], обозначаемая обычно **GB**, как раз и является аксиоматической теорией множеств, реализующей эту идею[108,109]. Чтобы подчеркнуть преемственность основной идеи этой системы с системой фон Неймана, некоторые авторы называют ее системой **фон Неймана–Геделя–Бернайса** и обозначают **NBG**. Однако в действительности, как технически, так и по существу система **GB** гораздо ближе к системе **ZF**. В системе **GB** *два* типа объектов: классы (обозначаемые большими буквами) и множества (обозначаемые маленькими буквами) и одно отношение $\in$. С чисто логической точки зрения система Геделя–Бернайса обладает некоторыми преимуществами перед системой Цермело–Френкеля. Дело в том, что аксиома подстановки представляет собой фактически бесконечное число аксиом и можно показать,

---

скую теорему и теорию колец операторов (C^*-алгебры, факторы, ...). С большим успехом он применил эти понятия в классической и квантовой механике, и в настоящее время операторные методы стали одним из главных инструментов теоретической физики. Именно фон Нейману и Г.Вейлю принадлежит математическая формулировка квантовой механики в терминах операторов в гильбертовом пространстве. Другие работы фон Неймана относятся к топологическим группам, непрерывным геометриям и т.д. Помимо работ по чистой математике и физике Джон фон Нейман был основателем нескольких громадных направлений в computer science и прикладной математике, в том числе теории автоматов и теории игр. Начиная с 1940-х годов был одним из ключевых участников американского ядерного проекта, директором бюро по проектированию электронных вычислительных машин. На русский язык переведены его книги 'Теория самовоспроизводящихся автоматов', 'Теория игр и экономическое поведение' (совм. с О.Моргенштерном) и основные статьи по алгебрам операторов (Дж.фон Нейман, Избранные труды по функциональному анализу. – М., Наука, 1987, т.I, с.1–376; т.II, с.1–370.). Фон Нейман высказал много проникновенных мыслей по поводу математики, самая знаменитая среди которых звучит следующим образом: 'In Mathematics you don't understand things, you just get used to them'.

[106]J.von Neumann, Die Axiomatisierung der Mengenlehre. – Math. Z., 1928, Bd.27, S.669–752.

[107]**Isaak Paul Bernays** (17.10.1888, Лондон –) – один из крупнейших специалистов по теории множеств и математической логике. Был учеником Эдмунда Ландау в Геттингене, после чего до 1933 года работал там, вначале как ассистент Давида Гильберта, а потом до 1933 года как профессор. Начиная с 1945 работал в ETH в Цюрихе. На русский язык переведена его совместная с Д.Гильбертом двухтомная монография 'Основания математики', т.1, 'Логические исчисления и формализация арифметики', 1979, с.1–557; т.2, 'Теория доказательств', 1982, с.1–652.

[108]В действительности, в 1937 году была опубликована *первая* из семи статей Бернайса под общим названием 'A system of axiomatic set theory', в которых строилась эта система, последняя из которых появилась в 1954. А.Френкель и Бар-Хиллел характеризуют эти статьи Бернайса как 'самое обширное и глубокое из существующих исследований по аксиоматической теории множеств'. Детальное изложение системы **GB** можно найти в книге P.Bernays, Axiomatic set theory. – Amsterdam, 1958, p.1–225.

[109]К.Гедель, Совместимость аксиомы выбора и обобщенной континуум-гипотезы с аксиомами теории множеств. – Успехи Мат. Наук, 1948, т.3, N.1, с.96–149

что вся система **ZF** не может вытекать ни из какого конечного их числа[110]. В то же время, система Геделя–Бернайса **GB** содержит всего 18 или 19 аксиом – обычные аксиомы для множеств и аксиомы образования классов. Перечислим все эти аксиомы так, как они сформулированы в книге Коэна[111,112]:

GB1 Элементы классов являются множествами.

GB2 Аксиома экстенсиональности для классов.

GB3 Существование пустого множества.

GB4 Существование неупорядоченной пары (которая является множеством).

GB5 Аксиома объединения для множеств.

GB6 Аксиома бесконечности.

GB7 Аксиома степени для множеств.

GB8 Аксиома подстановки для классов (заменяя каждый элемент класса на некоторое множество, мы снова получаем класс).

Следующая группа аксиом относится к образованию классов.

GB9 Существует класс всех пар (x, y), где $x \in y$.

GB10 Существование пересечения для классов.

GB11 Существование дополнения для классов.

GB12 Существование проекции класса: элементы y такие, что существует x такое, что $(x, y) \in X$ образуют класс.

GB13 Существует класс пар (x, y) таких, что $y \in X$.

GB14 Существует класс пар (x, y) таких, что $(y, x) \in X$.

GB15 Существует класс троек (y, z, x) таких, что $(x, y, z) \in X$.

GB16 Существует класс троек (x, z, y) таких, что $(x, y, z) \in X$.

Последние две аксиомы являются сильными формами аксиомы выбора и аксиомы регулярности:

GB17 Существует класс всех пар вида (x, y), где $x \in y$, а y пробегает класс всех непустых множеств.

Иными словами, этот класс выбирает ровно по одному элементу из каждого непустого множества.

GB18 В любом непустом классе X существует элемент, который не содержит в качестве элемента ни одного другого элемента класса X.

Точное соотношение между системами **ZF** и **GB** дается следующим результом[113].

Теорема Мостовского. *Каждая теорема теории* **ZF** *является теоремой теории* **GB**. *Обратно, каждая теорема теории* **GB**, *в которой фигурируют только множества, является теоремой теории* **ZF**.

Таким образом, с точки зрения **всех** приложений в обычной математике теории **ZF** и **GB** эквивалентны и поэтому большинство работающих математиков предпочитает пользоваться более привычной системой **ZF**, лишь изредка упоминая “класс всех множеств”, “класс всех групп”, “класс всех колец” и т.д.

---

[110]П.Коэн, Теория множеств и континуум-гипотеза. – Мир, М., 1969, с.1–345. стр.163.
[111]П.Коэн, ibid., стр.143–145.
[112]К.Фейс, Алгебра: кольца, модули, категории. т.1. – М., 1977, 1–676.
[113]П.Коэн, ibid., стр.149.

§ 12. Теории типов: системы **PM**, **NF** и **ML**

> Как-то ночью, проснувшись с сильного похмелья, Федор очень захотел пить. Не зажигая света, он вышел на кухню, нащупал на полке бутыль и начал пить. Сделав первый глоток, он понял, что ошибся, и в бутыли не вода, как он предполагал, а керосин. Однако Федор с такой силой овладел дзен-буддизмом, что нашел в себе мужество не исправлять ошибки и спокойно допил бутыль до конца.
>
> Владимир Шинкарев, 'Максим и Федор'

Принципиально другой способ избавиться от антиномий – **теория типов** – был предложен Бертраном Расселом (см. популярное изложение этой идеи в[114,115]). В системах, основанных на этой идее, все математические объекты разделяются на **типы** и объекты более высокого типа могут содержать в качестве элементов только объекты более низкого типа, что автоматически устраняет возможность возникновения парадоксов аналогичных парадоксам Рассела или Кантора (так как в ней нельзя говорить о множестве всех объектов обладающих некоторым свойством, а только о множестве всех объектов **фиксированного типа** с этим свойством). Однако достигается это за счет того, что теория типов запрещает образование таких множеств как $\{x, \{x\}\}$.

1. Разветвленная теория типов. Титаническая попытка построить всю классическую математику на основе теории типов предпринята Расселом и Уайтхедом[116] в монументальном труде "Principia Mathematica"[117]. Использованная там чрезвычайно сложная система обозначается обычно **PM** и называется **разветвленной** (ramified) теорией типов. В этой теории нужно отдельно вводить **все** понятия на каждом уровне. Таким образом, понятия равенства, пустого множества, кардинального числа и т.д. расслаиваются на бесконечную иерархию понятий. Анри Пуанкаре поясняет сущность (разветвленной) теории типов следующей иллюстрацией[118]. "Возьмем пример Эпименида. Лжецом 1-го порядка будет тот, который лжет всегда, за исключением случая, когда он говорит: "я лжец 1-го порядка". Лжецом 2-го порядка будет тот, который лжет всегда, даже и тогда, когда говорит "я лжец 1-го порядка", но который не лжет, говоря "я лжец 2-го порядка", и т.д. Таким образом, когда Эпименид скажет нам "я лжец", мы можем его спросить, "какого порядка?". И только после того, как он ответит на этот законный вопрос, его утверждение будет иметь смысл." Это рассуждение хорошо показывает и то, каким образом теория типов снимает 'парадоксы' наивной теории множеств, и то, насколько тяжеловесно и далеко от обычной практики математиков подобное решение. Рассел и Уайтхед предприняли попытку избавиться от этой тяжеловесности, перестав ставить индексы и вводя фразу 'при условии, что все термы принадлежат соответствующим уровням', однако, как заметил в 1944 году Гедель, потерпели на этом пути сокрушительную неудачу.

2. Простая теория типов. Рамсей[119] предложил ограничиться **простой** теорией типов и все последующее развитие этой теории следовало по пути Рамсея[120]. В дальнейшем –

---

[114]B.Russell, Mathematical logic as based on the theory of types. – Amer. J. Math., 1908, vol.30, p.222–262.

[115]B.Russell, Introduction to Mathematical philosophy. – London, 1919.

[116]**Альфред Норт Уайтхед** (15.02.1861, Рамсгейт – 30.12.1947, Кембридж, Масс.) – английский логик и философ, профессор Лондонского Университета. Основные его работы относятся к попыткам логического обоснования математики. В 1924 году эмигрировал в США, в этот период его интересы окончательно сместились в область философии. В широких кругах Уайтхед знаменит главным образом своими bon mots – остроумными замечаниями о науке и ученых.

[117]A.N.Whitehead, B.Russell, Principia mathematica, vol.I–III. 2nd ed. – Cambridge, 1925–1927.

[118]А.Пуанкаре, "Логика бесконечности", с.455.

[119]E.P.Ramsey, The foundations of mathematics. – in The foundations of Mathematics and other logical essays. London, 1931, p.1–61.

[120]Впрочем, Герман Вейль считает, что идею разветвленной теории типов убил сам Рассел своей 'аксиомой сводимости' – см. Г.Вейль, Структура Математики. – Успехи Мат. Наук., 1976, т.31, N.1, с.220–238.

вплоть до сравнительно недавнего времени – предпринималось еще несколько попыток спасти и упростить теорию типов путем компромиса с идеями Цермело и фон Неймана. Наиболее известные из этих попыток – системы Тарского **T** и Куайна **NF** и **ML**, но было и много других – системы Карнапа, Лоренцена[121], Ван Хао, ...). В 1937 году Куайн[122] предложил упростить теорию типов следующим образом: лишь слегка ослабить аксиому Фреге, потребовав, чтобы *стратифицированные* по типам свойства являлись коллективизирующими. Эта система, известная как **NF** (New Foundations) была детально развита в чрезвычайно интересной книге Россера[123]. Как отметил Карри, система **NF** обладает рядом особенностей, которые делают ее абсолютно неприемлемыми для работающего математика (например, класс одноэлементных подмножеств любого множества не может считаться множеством!). В этой системе нельзя доказать теорему Кантора о мощности 2^X, так как в ее доказательство входят нестратифицированные формулы. Но – по той же причине – там нельзя доказать и большую часть обычных результатов теории чисел (ведь теперь принцип математической индукция справедлив только для стратифицированных формул!). В дальнейшем Куайн слегка видоизменил свою систему[124], чтобы согласовать ее с обычной математической практикой. Эта видоизмененная система получила название **ML** (Mathematical Logic). Однако, после выхода первого издания книги Куайна в 1940 году Линдон и Россер[125], независимо заметили, что эта система *противоречива*, так как в ней не устраняется парадокс Бурали-Форти. Это не помешало Куайну воспроизвести ту же систему во втором издании его книги в 1947 году! Только в третьем издании эта 'случайная оплошность' была исправлена Ван Хао.

Однако даже в простейших вариантах теории типов приводят к громоздкой символике и неестественным ограничениям математического языка, а, с другой стороны, все обычные варианты теории типов слабее теории Цермело. Существенным недостатком этих систем является их несовместимость с аксиомой выбора. Поэтому аксиоматики, основанные на этой идее, не приобрели *никакой* популярности среди работающих математиков и обсуждаются в основном логиками и философами. Последние авторы, придерживавшиеся принципов теории типов, жили и творили в ГДР[126] и с исчезновением этой страны теория типов окончательно прекратила свое существование.

§ 13. Универсумы, система Гротендика **ZFG**

> Это то, что называют **универсумом**. Это не постигается разумом, это можно либо принять, либо отвергнуть. Если мы приняли, в нас вдохнули новую жизнь. Если отвергли – мы хиреем. Что бы под этим ни подразумевалось, оно неуловимо; оно настолько огромно, что о нем никогда нельзя сказать последнего слова.
>
> Генри Миллер, "Сексус", Гл. I

Во многих разделах математики, особенно в теории категорий, и находящихся под ее влиянием областях (таких как гомологическая алгебра, алгебраическая геометрия и т.д.) обычно используется **система Гротендика** alias **система Цермело-Френкедя-Гротендика ZFG**. Это система Цермело-Френкеля **ZF** с дополнительной аксиомой Гротендика **G**, утверждающей существоване универсумов.

1. Универсумы. Сейчас мы введем множества настолько большие, что их можно представлять себе как формализацию наивного понятия 'множество всех множеств'. На самом деле, как мы знаем, понятие множества всех множеств противоречиво, однако *в самом строгом техническом смысле* каждый универсум можно представлять себе как **класс** всех множеств.

---

[121]P.Lorenzen, Einführung in die operative Logik und Mathematik. – Berlin et al., 1955.

[122]W.V.Quine, New foundations for mathematical logic. – Amer. Math. Monthly, 1937, vol.44, p.70–80. – расширенная версия перепечатана в W.V.Quine, From a logical point of view. – Cambridge, Mass., 1951, p.80–101.

[123]J.B.Rosser, Logic for mathematicians. – N.Y., 1953.

[124]W.V.Quine, Mathematical logic. – Cambridge, Mass., 1951.

[125]J.B.Rosser, The Burali-Forti paradox. – J. Symb. Logic., 1942, vol.7, p.1–17.

[126]G.Wunsch, Algebraische Grundbegriffe. – VEB Verlag für Technik, Berlin, 1970, S.1–212.

Определение. *Множество U называется* **универсумом**, *если оно удовлетворяет следующим условиям*

U1 $\omega \in U$,

U2 $A \in U \Longrightarrow A \subseteq U$,

U3 $A \in U \Longrightarrow 2^A \in U$,

U4 $A \in U \Longrightarrow \cup A \in U$,

U5 *для любого отображения* $f : A \longrightarrow U$ *имеем* $A \in U \Longrightarrow f(A) \in U$.

Легко убедиться, что все обычные теоретико-множественные конструкции с элементами U могут быть реализованы уже внутри U.

Задача. Покажите, что если U универсум, то

U6 $A \in U \ \ \& \ \ B \subseteq A \Longrightarrow B \in U$

U7 $A, B \in U \Longrightarrow \{A, B\} \in U$,

U8 если $I \in U \ \ \& \ \ A_i \in U$ для всех $i \in I$, то $\prod A_i \in U$, $i \in I$.

2. Универсумы как модели системы Геделя-Бернайса. Даже самый крошечный универсум чудовищно велик. В частности, он содержит в качестве элементов множество вещественных чисел $\mathbb{R}$ и все его подмножества, множество всех его подмножеств $2^{\mathbb{R}}$ и все его подмножества, множество $2^{2^{\mathbb{R}}}$ и все его подмножества и т.д. В действительности, каждый универсум можно рассматривать как модель системы Геделя-Бернайса. Назовем множество A **малым**, если $A \in U$, **большим**, если $A \subseteq U$, но $A \notin U$, и **экстраординарным**, если $A \not\subseteq U$. Теперь мы можем рассматривать малые множества как 'множества' модели, а большие множества как 'собственно классы', при этом сам U выступает в качестве 'класса всех множеств'. В такой модели можно осуществлять **все** конструкции над множествами и классами, допустимые в системе Геделя-Бернайса, и, *сверх того*, рассматривать множества классов, которые с точки зрения универсума будут экстраординарными множествами.

3. Аксиома Гротендика. Универсумы настолько велики, что существование хотя бы одного универсума не может вытекать из аксиом Цермело-Френкеля и должно гарантироваться специальной аксиомой. Следующую аксиому можно рассматривать как очень смелое обобщение аксиомы бесконечности.

G (Аксиома Гротендика). *Для каждого множества A существует такой универсум U, что $A \in U$.*

В частности, эта аксиома утверждает, что каждый универсум является элементом некоторого большего универсума! Тем самым, эта аксиома полностью устраняет необходимость рассмотрения классов. В самом деле, вместо множества всех множеств мы можем рассматривать множество всех множеств, содержащихся в данном универсуме – согласно аксиоме Гротендика это действительно множество! В действительности, для большинства практических целей эта аксиома слишком сильна, так как **всю** обычную математику можно строить на элементах *одного* какого-то универсума. Поэтому многие математики используют систему более слабую, чем система Гротендика[127], в которой вместо аксиомы **G** накладывается

[127]**Александр Гротендик** (род. 1928, Берлин) – Один из крупнейших математиков в истории, значение осуществленной им революции в математике можно сопоставить со вкладом Лейбница, Ньютона, Кантора, Гильберта. В 1933 году его родители попали в концентрационный лагерь, а он оказался в сиротском доме в Швейцарии. После войны учился во Франции и работал в Париже, Бюр-сюр-Ивет и Монпелье. Его ранние работы относятся к области функционального анализа и гомологической алгебры. После этого его основные интересы переключились на алгебраическую геометрию. Его многотомные 'Элементы алгебраической геометрии' (частично совместные с Дьедонне), 'Семинар по алгебраической геометрии' (частично совместные с Демазюром, Вердье и другими) и другие работы 1960-х годов стали библией для нескольких поколений математиков. Основал несколько больших направлений математики, в том числе K-теорию. На математическом конгрессе 1966 года в Москве награжден филдсовской премией. В начале 1970-х годов отошел от математики и занялся медитацией и литературной деятельностью. На русский переведена его статья 'О некоторых вопросах гомологической алгебры' и части книги 'Урожаи и посевы'.

лишь следующая значительно более слабая аксиома (см., например[128,129]).

G′ (Слабая аксиома Гротендика). *Существует хотя бы один универсум.*

С точки зрения всех обычных приложений универсум *чрезвычайно велик*, так как он содержит **бесконечную иерархию бесконечностей**, из которых в обычной математике редко используются больше, чем две или три. С другой стороны, с точки зрения Канторовской теории множеств универсум *безнадежно мал*, потому что бесконечно больше мощностей остаются вне универсума, чем попадают внутрь.

§ 14. Теория гипермножеств

> A well-known scientist (some say it was Bertrand Russell) once gave a public lecture on astronomy. He described how the earth orbits around the sun and how the sun, in turn, orbits around the centre of a vast collection of stars called our galaxy. At the end of the lecture, a little old lady at the back of the room got up and said: "What you have told us is rubbish. The world is really a flat plate supported on the back of a giant tortoise". The scientist gave a superior smile before replying, "What is the tortoise standing on?" – "You're very clever, young man, very clever", said the old lady, "But it's turtles all the way down!".
>
> Stephen W.Hawking, "A brief history of time".

1. Теория гипермножеств. Наиболее оспариваемой в настоящее время аксиомой теории **ZFC** является аксиома регулярности. Многие специалисты считают, что она внесена в **ZFC** по чисто техническим причинам, не отражает общепризнанного математического принципа и существенно ограничивает применимость теории множеств к моделированию циклических явлений (возникающих, скажем, в программировании или лингвистике). Эта аксиома *никогда* не использовалась в алгебре или топологии сознательно, а там, где ее использование носит неосознанный характер (например, определение упорядоченной пары (x, y) как $\{x, \{x, y\}\}$), его легко обойти, чуть подправив определения. Лично мне представляется, что ее принятие ведет к недопустимому обеднению нашей теоретико-множественной интуиции. Теория множеств без аксиомы **ZF9** обозначается $\mathbf{ZF}^-$ (или $\mathbf{ZFC}^-$, если хотят подчеркнуть наличие в ней аксиомы выбора) и называется теорией **гипермножеств**[130,131,132].

Разумеется, недостаточно просто отбросить **ZF9** и констатировать, что гипермножества *могут* существовать. Нужно добавить какую-то новую аксиому, которая позволит *строить* гипермножества, не являющиеся фундированными, наподобие того как мы строим множества при помощи обычных аксиом свертывания. Пусть x любое множество. Сопоставим ему **граф составляющих**, вершинами которого являются само множество x и все его составляющие, причем стрелка из вершины y в вершину z рисуется в том и только том случае, когда $y \in z$. Одна из наиболее популярных аксиом, **аксиома антифундирования AFA**, утверждает, что для *любого* ориентированного графа, удовлетворяющего очевидным необходимым условиям, существует гипермножество с данным графом составляющих.

Типичным примером гипермножества, не являющегося фундированным, служит

$$y = \{x, \{x, \{x, \{x \dots\}\}\}\}.$$

Ясно, что $y \in y$. В некотором смысле, который можно уточнить, множество y является *пределом* обычных хорошо фундированных множеств

$$\{x\}, \quad \{x, \{x\}\}, \quad \{x, \{x, \{x\}\}\}, \quad \{x, \{x, \{x, \{x\}\}\}\},$$

---

[128] S.MacLane, Categories for the working mathematicians. – Berlin, 1972.

[129] H.Herrlich, G.Strecker, Category theory. – Boston, 1973.

[130] P.Aczel, Non-well-founded sets. – SCLI Public., Stanford, 1988.

[131] J.Barwise, L.Moss, Hypersets. – Math. Int., 1991, vol 13, N.4, p.31–41.

[132] J.Barwise, L.Moss, Vicious circles and the mathematics of non-wellfounded Phenomena. – CSLI Public., Stanford, 1996, p.1–390.

которые становится все труднее отличать от y по мере продвижения по этой последовательности.

Таким образом, если обычная Канторовская теория множеств изучает экстенсивную бесконечность, уходящую вширь, теория гипермножеств добавляет к ней еще и интенсивную бесконечность, уходящую вглубь.

Легко привести пример гипермножества, которое не является своим собственным элементом, но является элементом своего элемента (и тем самым, входит в себя на всех четных уровнях). А именно, возьмем две различных вещи $u \neq v$ и положим

$$x = \{u, \{v, \{u, \{v \dots\}\}\}\}, \qquad y = \{v, \{u, \{v, \{u \dots\}\}\}\},$$

Легко видеть, что $x \neq y$, $x \in y$ и $y \in x$.

§ 15. Лягушачья икра

Профессор Чарльз Дарвин учит нас, что существует множество D объектов и линейное упорядочение этого множества такие, что первый элемент в этом множестве есть некая обезьянка Чарли, каждый не первый элемент есть сын непосредственно предшествующего элемента и последний элемент есть сам Дарвин. Совокупность A всех обезьян из множества D не является множеством; в противном случае A содержало бы последний элемент. Но, как знает всякий, сыновья обезьян суть обезьяны. Таким образом, оказалось бы, что все члены D, включая и Дарвина, были бы обезьянами.

Петр Вопенка[133]

На башне спорили химеры:
Которая из них урод?

Осип Мандельштам

1. Некантороская теория множеств. Конечно, все перечисленные в этом параграфе системы теории множеств можно было бы назвать *некантороскими*, но обычно, говоря о **некантороской теории множеств** имеют в виду теории *без аксиомы степени*, в которых нельзя говорить о множестве всех подмножеств фиксированного множества. Наиболее известной из таких систем является **система Цермело-Френкеля без аксиомы степени ZF-P**, в которой выполняются все аксиомы, кроме **ZF7**. Известно, что эта система не позволяет построить вещественные числа. Классической во французской литературе считается переписка Эмиля Бореля[134], Рене Бэра[135] и Анри Лебега[136] (именуемых в дальнейшем

[133]П.Вопенка, Математика в альтернативной теории множеств, М., Мир, 1983, с.1–150; стр.35.

[134]**Эмиль Борель** (07.01.1871, St Affrique – 03.02.1956, Париж) – знаменитый французский математик, основные работы которого относятся к теории меры, теории функций, теории вероятностей и теории игр. Учился в Париже и был профессором в Парижском Университете. В подходе к теории множеств занимал крайне сумбурную позицию. В нашем курсе упоминаются несколько классических теорем Бореля: теорема о свертке, теорема о ряде Тейлора и т.д. В курсе анализа встречается теорема Гейне-Бореля и борелевские множества. Кроме математики Борель успешно занимался политической деятельностью, до конца жизни был мэром Сен-Африк. Во время первой мировой войны был военно-морским министром в двух правительствах Пенлеве. Эмиля Бореля не следует путать с более знаменитым швейцарским математиком Арманом Борелем, одним из членов Бурбаки, в честь которого названы борелевские подгруппы, борелевские подалгебры и т.д.

[135]**Рене Бэр** (1874 – 1932)

[136]**Анри Леон Лебег** (Lebesgue) (28.06.1875, Beauvais (Oise) – 26.07.1941, Париж) – знаменитый французский аналитик, основные работы которого относятся к теории меры и интеграла, рядам Фурье и другим вопросам вещественного анализа. Кроме того, написал несколько статей в области топологии и геометрии. После окончания 1897 году Ecole Normale

академиками) с Жаком Адамаром[137]. Вначале академики считали, что в следствиях теории множеств, противоречащих их интуиции, виновата аксиома выбора. К их чести нужно заметить, что довольно скоро они разобрались, что истинная причина состоит в аксиоме степени. Когда Жак Адамар[138] указал академикам на то обстоятельство, что без аксиомы степени невозможно построить вещественные числа, они без колебаний отказались от понятия множества вещественных чисел (см. Бурбаки, с.338–339).

Наиболее радикальный отказ от канторовской математики (и от самой идеи актуальной бесконечности) происходит в **теории полумножеств**, развиваемой Петром Вопенкой и другими Пражскими логиками. Отчасти в этой теории (как и в ультраинтуиционизме Есенина-Вольпина) происходит возвращение к идеям Пуанкаре и Брауэра, но в гораздо более радикальной форме. А именно, Вопенка отрицает не только то, что все подмножества данного множества образуют множество, но даже и то, что подкласс множества обязан быть множеством! Именно подклассы множеств и называются **полумножествами**.

2. Нечеткие множества. Среди инженеров большую популярность получила так называемая теория нечетких множеств[139,140]. Пусть U – фиксированное множество. С точки зрения математики **нечеткое подмножество** в U это просто функция $f : U \longrightarrow \mathbb{I}$. В действительности, в этом случае инженеры обычно говорят о нечетком множестве X а функцию f называют **характеристической функцией** нечеткого множества X. При этом для элемента $x \in U$ значение $f(x)$ истолковывается как степень уверенности в том, что элемент x принадлежит X. Для обычного подмножества f принимает только значения 0 и 1.

Для нечетких множеств можно определить все обычные операции и конструкции над множествами, причем часто в нескольких различных вариантах. Например, **объединением** нечетких множеств называется множество с характеристической функцией $f \cup g$, определенной посредством $(f \cup g)(x) = \max(f(x), g(x))$, а их **пересечением** – множество с характеристической функцией $f \cap g$, определенной посредством $(f \cap g)(x) = \min(f(x), g(x))$.

В действительности, теория нечетких множеств представляет собой чисто словесную инновацию, предпринятую в коммерческих и рекламных целях (fuzzy logic и пр.). Она полностью моделируется в обычной теории множеств и не представляет собой **ничего нового** по сравнению с традиционной теорией вероятностей.

работал вначале школьным учителем, с 1910 года – профессором Парижского университета, а с 1912 года – в Collège de France. Один из немногих ученых пролетарского происхождения. Центральную роль в анализе играют мера Лебега и интеграл Лебега. В курсе анализа упоминается несколько теорем Лебега. Лебег много, охотно и, как правило, ошибочно высказывался по вопросам теории множеств. Последние 20 лет занимался главным образом педагогикой и историей математики. На русский язык переведена его книга ‘Об измерении величин’.

[137]R.Baire, E.Borel, J.Hadamard, H.Lebesgue, Cinq lettres sur la théorie des ensembles. – Bull. Soc. Math. France, 1905, v.33, p.261–273.

[138]**Жак Саломон Адамар** (Hadamard) (08.12.1865, Версаль – 17.10.1953, Париж) – замечательный французский аналитик. После окончания Ecole Normale работал в Сорбонне, College de France и l’Ecole Politechnique, на 1940/47 годы уезжал в США, после чего возвратился в Париж. Известен своими работами в области аналитической теории чисел, теории аналитических функций, теории дифференциальных уравнений в частных производных, вариационному исчислению и дифференциальной геометрии. В нашем курсе встречаются матрицы Адамара, произведение Адамара, неравенство Адамара. В области оснований математики занимал позицию безоговорочной поддержки аксиомы выбора. На русский язык переведены его книги ‘Неэвклидова геометрия в теории автоморфных функций’, ‘Психология изобретения в области математики’ и двухтомный учебник ‘Элементарная геометрия’.

[139]Л.Заде, Понятие лингвистической переменной и его применение к принятию приближенных решений. – М., Мир, 1976, с.1–165.

[140]А.Кофман, Введение в теорию нечетких множеств. – М., Радио и связь, 1982.

к

Глава 2. Булевы операции

> Изменения названий, соответствующие изменениям вещей и не соответствующие им, объединяются в пределах природы, свободно следуют бесконечным переменам и поэтому полностью исчерпывают естественный срок существования. Что означает 'объединяются в пределах природы'? Отвечу: существует истина и ложь, существует правда и неправда. Если истина действительно является истиной, то нечего спорить, насколько истина отличается от лжи. Если правда действительно является правдой, то нечего спорить, насколько правда отличается от неправды. Забудем о течении времени, забудем о суждениях о том, что такое правда и неправда, найдем радость в бесконечности и поселимся в бесконечном.
>
> Чжуан Чжоу, Гл. 2, Сглаживание противоположностей[141]

Здесь мы напоминаем определения и основные свойства *теоретико-множественных*, так называемых булевых[142] операций над множествами. Различные свойства этих операций были открыты еще в глубокой древности, но как целостная система они были изучены и систематизированы только в XVII–XIX веках.

§ 1. Булеан и внешние степени множества

1. Булеан. Через $2^U = P(U)$ будет обозначаться **множество** всех **подмножеств** множества U, называемое также **множеством частей** или **булеаном** множества U.

Заметим, что 'U' здесь является первой буквой слова universal (set) – универсальное множество. Дело в том, что если мы хотим добиться полной симметрии между свойствами пересечения и объединения, мы должны в каждый

---

[141] Имеется три русских перевода Чжуан-цзы, выполненных Л.Д.Позднеевой, С.Кучерой и В.В.Малявиным. Приведенный фрагмент является комбинацией перевода С.Кучеры (Древнекитайская философия, собрание текстов в двух томах. т.1. – Мысль., М., 1972, с.1–363., стр.261.) и перевода Л.Позднеевой, впервые опубликованного в 1967 году ('Атеисты, материалисты, диалектики древнего Китая. Ян Чжу, Ле-цзы, Чжуан-цзы. – М., 1967') и недавно переизданного (Чжуан-цзы. – Амфора, СПб, 2000, с.1–367., стр.34.) Новый перевод В.В.Малявина (Чжуан-цзы, – Астрель, М., 2002, с.1–429.) содержит массу интересного справочного материала, но, к сожалению, не передает симметрию оригинала и вносит в текст совершенно отсутствующую там вычурность. Вот, например, как там передается последняя фраза: 'Забудем о наших заботах, забудем о наших обязанностях, обретем беспредельность и будем вечно в ней пребывать'.

[142] **Джордж Буль** (02.11.1815, Линкольн – 08.12.1869, Корк) – английский логик и математик, основные работы которого относятся к алгебре логики и теории вероятностей. Вырос в крайней нищете, самостоятельно выучил несколько языков и работал частным преподавателем. В 1840-х годах он заметил аналогию между законами логики и законами операций над числами. Итогом этих наблюдений явились книги 'The mathematical analysis of logic' (1847 год) и 'An investigation of the laws of thought' (1854 год), в которых Буль ввел то, что теперь называется булевыми алгебрами. С 1849 года был профессором в Корке, Ирландия. В нашем курсе встречаются булеаны, булевы операции, булевы функции, булевы кольца, булевы решетки, булевы алгебры и т.д. Младшая дочь Буля Этель Лилиан в замужестве Войнич (11.05.1864, Корк – 28.07.1960, Нью Йорк), стала довольно известной писательницей, автором популярного в СССР романа 'Овод' (1897).

данный момент ограничиваться рассмотрением подмножеств некоторого фиксированного множества. Например, в качестве U можно взять какой-то универсум, если мы верим в его существование, но U совсем не обязательно должно быть *настолько* большим. С другой стороны, 'P' является первой буквой английского слова 'part'. В старинных книгах обычно пользовались готическими буквами, так что вместо $P(U)$ обычно писали $\mathfrak{P}(U)$. Следующий результат объясняет смысл используемого сегодня обозначения 2^U.

Теорема. *Если множество U конечно, то множество 2^U содержит $2^{|U|}$ элементов.*

Доказательство. Доказываем предложение индукцией по $n = |U|$. В качестве базы индукции можно взять случай $U = \varnothing$, когда $2^{\varnothing} = \{\varnothing\}$ состоит из одного элемента, что соответствует формуле $2^0 = 1$. Предположим теперь, что X непусто и фиксируем точку $x \in U$. Рассмотрим, как подмножества множества U расположены относительно x. Для подмножества $X \subseteq U$ имеет место следующая альтернатива: либо $x \in X$, либо $x \notin X$. Во втором случае множество X содержится в $(n-1)$-элементном множестве $U \setminus \{x\}$ и по индукционному предположению имеется ровно 2^{n-1} таких множеств. С другой стороны, в первом случае X имеет вид $X = Y \cup \{x\}$, для единственного $Y \subseteq U \setminus \{x\}$, так что таких множеств снова ровно 2^{n-1}. Но это и значит, что всего в U ровно $2^{n-1} + 2^{n-1} = 2^n$, как и утверждалось.

По аналогии и для бесконечных множеств 2^U обозначается через $2^{|U|}$. Например, мощность множества всех подмножеств $\mathbb{N}$ обозначается через $2^{\aleph_0}$, мощность всех подмножеств множества $\mathbb{R}$ обозначается через $2^{2^{\aleph_0}}$ и т.д.

Комментарий. Рассмотрение булеана как множества неизменно остается одним из самых оспариваемых пунктов всего канторовского учения. Однако, если в начале XX века оспаривалась *возможность* рассматривать булеан как множество (А.Лебег, Л.Брауер и др.), то сегодня оспаривается *целесообразность* так его рассматривать. В действительности, для любого множества U его булеан 2^U является не просто множеством, а множеством *упорядоченным* отношением включения. Современная точка зрения состоит в том, чтобы истолковывать булеан 2^U как *категорию*, объектами которой являются подмножества множества U, причем множество $\mathrm{Mor}(X, Y)$ пусто, если $X \not\subseteq Y$ и состоит из единственного элемента, если $X \subseteq Y$. Композиции морфизмов соответствуют цепочкам $X \subseteq Y \subseteq Z$. Теперь множество 2^{2^U} естественно истолковывать как 2-категорию и т.д. В частности, с этой точки зрения вещественные числа образуют категорию, а множество всех множеств вещественных чисел – 2-категорию.

2. Внешние степени множества. Множество m-элементных подмножеств множества U называется **m-й внешней степенью множества** U и обозначается через $\bigwedge^m(U)$ (в комбинаторике часто используется также обозначение $X^{(m)}$):

$$\bigwedge^m(U) = \{X \subseteq U \mid |X| = m\}.$$

Через $\bigwedge(U)$ обозначается множество всех **конечных** подмножеств множества U. Таким образом, для конечного множества $\bigwedge(U) = 2^U$.

Замечание. В действительности, для многих теоретико-множественных конструкций, в которых обычно происходит ссылка на аксиому степени **ZF7**, достаточно существования $\bigwedge(U)$. Поэтому в некоторых неканторовских теориях множеств вместо аксиомы **ZF7** принимается значительно более слабая аксиома **ZF7′**, утверждающая существование $\bigwedge(U)$ для любого множества U (**слабая**

аксиома степени). Эта аксиома никогда не подвергалось столь ожесточенным атакам, как аксиома Кантора о существовании булеана. Дело в том, что для бесконечных множеств $|\bigwedge(U)| = |U|$, так что в известном смысле $\bigwedge(U)$ не больше, чем U и его существование не позволяет, в отличие от аксиомы Кантора, строить бесконечную иерархию бесконечных мощностей.

Комментарий. Название и обозначение $\bigwedge^m(X)$ подсказаны аналогией с векторными пространствами. С точки зрения комбинаторики множества являются частным случаем векторных пространств, а именно, векторными пространствами над полем **из одного элемента** (того самого, про которое мы вскоре скажем, что его не существует). При этом множество совпадает со своим базисом, поэтому **все** отображения множеств линейны (над полем из одного элемента, разумеется). Таким образом, все комбинаторные задачи о множествах становятся частными случаями соответствующих задач о векторных пространствах, причем решение более общей задачи обычно проще. При этом подмножествам соответствуют подпространства, отображениям – линейные отображения и т.д. Все сказанное получает формальное истолкование в теории λ-колец, см., например [tD], Гл.3.

§ 2. Биномиальные коэффициенты

1. Биномиальные коэффициенты. Количество m-элементных подмножеств n-элементного множества называется **числом сочетаний из** n **по** m и обозначается $\binom{n}{m}$. Таким образом, по определению, $\binom{n}{m} = |\bigwedge^m(\underline{n})|$. Числа $\binom{n}{m}$ называются также **биномиальными коэффициентами**.

Шутка: О вкусах не спорят[143]**.** В одном учебнике математического анализа я встретил следующее определение биномиальных коэффициентов:

$$\binom{n}{m} = \frac{1}{m!}\frac{d^m}{dx^m}(1+x)^n|_{x=0}.$$

Желающие могут попробовать вывести из этого определения все свойства биномиальных коэффициентов, о которых пойдет речь далее.

Задача (Треугольник Паскаля[144]**).** Основным фактом про биномиальные коэффициенты является следующее **рекуррентное соотношение**. Для любых m и n имеет место равенство

$$\binom{n}{m} = \binom{n-1}{m-1} + \binom{n-1}{m}.$$

Теперь, чтобы полностью восстановить все биномиальные коэффициенты, достаточно воспользоваться ‘граничными условиями’

$$\binom{n}{0} = \binom{n}{n} = 1.$$

Указание. Действуйте так же, как в доказательстве предшествующей теоремы, а именно, фиксируйте точку $x \in X$.

---

[143]Впрочем, парафразируя Дарвина Ницше говорил, что жизнь как раз и есть спор о вкусах.

[144]**Блез Паскаль** (19.06.1623, Клермон-Ферран – 19.08.1662, Париж) – знаменитый французский математик и философ. В 16 лет открыл теорему Паскаля о шестиугольнике. В 1641 году сконструировал первый компьютер. Паскаль и Ферма были первыми математиками, которые получили серьезные результаты в области теории вероятностей. Отец Блеза Паскаля Этьен Паскаль тоже увлекался математикой, и улитка Паскаля названа в честь него.

Треугольник Паскаля, который на самом деле был известен в Китае не позже IX века, и в Европе не позже начала XVI века (в Италии треугольник Паскаля и сегодня называется **треугольником Тартальи**) допускает следующую эффектную формулировку. Биномиальный коэффициент равен числу маршрутов от вершины треугольника к точке, в которой расположен данный коэффициент (напомним, что **маршрут** – в отличие от **пути** – всегда идет в положительных направлениях, в данном случае вниз-влево и вниз-вправо).

Соотношение, определяющее треугольник Паскаля – это так называемое рекуррентное соотношение **треугольного типа**. Итерируя его, легко получить рекуррентное соотношение **вертикального типа**.

Задача. Докажите, что

$$\sum \binom{n}{i} = \binom{n+1}{m+1}, \qquad 0 \le i \le n.$$

Задача. Докажите, что

$$\binom{n}{m} = [n]_m/m!.$$

Подставляя сюда вместо убывающего факториала $[n]_m$ его выражение через обычный факториал, мы получаем привычную формулу $\binom{n}{m} = n!/m!(n-m)!$, но приведенная в задаче формула лучше, потому что она позволяет распространить определение биномиального коэффициента на случай, когда $n \in \mathbb{Z}$. Эту задачу можно сформулировать еще следующим образом.

Задача. Докажите, что произведение m последовательных целых чисел делится на $m!$.

Задача. Бриджевая рука представляет собой выбор 13 карт из колоды в 52 карты. Сколько существует различных бриджевых рук?

2. Некоторые важнейшие тождества. Имеются тысячи тождеств, связанных с биномиальными коэффициентами[145], и у нас нет ни возможности, ни желания обсуждать их здесь. Вбросим, тем не менее, пригоршню простейших тождеств, которыми мы будем постоянно пользоваться.

Задача. Докажите, что

$$\binom{n}{m} = \binom{n}{n-m}$$

не пользуясь формулой для $\binom{n}{m}$.

Задача. Вычислить сумму $\sum \binom{n}{m}$, $0 \le m \le n$, не пользуясь формулой для $\binom{n}{m}$.

Задача. Вычислить знакопеременную сумму $\sum (-1)^m \binom{n}{m}$, $0 \le m \le n$, не пользуясь формулой для $\binom{n}{m}$.

Все знают, что ответ в первой из этих задач равен 2^n, а во второй – 0, это очевидно из формулы бинома Ньютона для $(1+1)^n$ и $(1-1)^n$ в $\mathbb{Z}$ или

[145]Несколько десятков таких тождеств и много дальнейших ссылок можно найти в книге Р.Грэхем, Д.Кнут, О.Паташник, Конкретная математика. – Мир, М., 1998, с.1–703.

из непосредственного вычисления, использующего выражение биномиальных коэффициентов через факториалы. Однако мы хотим найти **априорные** доказательства, не зависящее от **вычисления** биномиальных коэффициентов. В первой задаче это очевидно, так как для конечного множества X имеем

$$2^X = \bigwedge(X) = \coprod_{m=0}^{n} \bigwedge^m(X).$$

Осталось вспомнить, что для n-элементного множества $|2^{\underline{n}}| = 2^n$. Во второй задаче требуется установить *априорное* соответствие между четными и нечетными подмножествами в $X = \underline{n}$. Если n само **нечетно**, то такое соответствие задается дополнением (если $Y \subseteq X$ имеет нечетный порядок, то порядок $\overline{Y} = X \setminus Y$ четен. В общем случае снова воспользуйтесь той же идеей, что в доказательстве теоремы!

Решение. Фиксируем точку $x \in X$ и рассмотрим отображение $\mathrm{inv}_x : X \longrightarrow X$, определенное посредством $\mathrm{inv}_x(Y) = Y \triangle \{x\}$. Ясно, что inv_x обратимо (в действительности inv_x является **инволюцией**, т.е. $(\mathrm{inv}_x)^2 = \mathrm{id}_X$) и переводит четные подмножества в нечетные.

Отступление: доказательство versus проверки. Большинство алгебраистов различает 'доказательство' и 'проверку'. Какой-то факт может быть 'проверен', но не 'доказан'. С этой точки зрения вычисление суммы, использующее выражение $\binom{m}{n}$ через факториалы, является 'проверкой', а то, что мы привели выше, 'доказательством', или, как сказали бы остальные математики, 'априорным доказательством', опирающимся только на определения. Это различие приобретает драматический характер в разделах алгебры, использующих нетривиальные классификационные теоремы. Многие классические проблемы теории групп (проблема Жордана, гипотеза Шрайера и т.д.) решены по модулю классификации конечных простых групп (называемой в дальнейшем просто **Классификацией**), т.е. проверено, что для всех (известных!) конечных простых групп соответствующее утверждение имеет место. В то же время никаких априорных (т.е. не использующих Классификацию) доказательств этих утверждений нет.

Задача (соотношение Вандермонда). Дайте априорное доказательство тождества

$$\binom{m+n}{l} = \sum \binom{m}{i}\binom{n}{l-i},$$

где сумма берется по всем $0 \leq i \leq l$.

Указание. Представьте множество порядка $m+n$ как копроизведение m-элементного множества X и n-элементного множества Y и посмотрите, какие пересечения его l-элементное множество Z имеет с X и Y. Некоторые авторы называют это тождество **тождеством Коши**.

Задача. Дайте априорное доказательство тождества

$$\binom{n}{m}\binom{m}{l} = \binom{n}{l}\binom{n-l}{n-m}.$$

Указание. Возьмите n-элементное множество X и посчитайте двумя способами (см. Главу V) количество таких пар (Y, Z), что $Y \in \bigwedge^m(X)$, $Z \in \bigwedge^l(X)$, $Y \supseteq Z$.

3. Биномиальные коэффициенты целого аргумента. Сейчас мы напишем формулу для числа m-элементных подмножеств в 'множестве отрицательной мощности'. Пусть $m, n \in \mathbb{N}_0$. Убывающий и возрастающий факториалы $[-n]_m$ и $[-n]^m$ определяются формулами: $[-n]_m = (-1)^m[n]^m$ и $[-n]^m =$

$(-1)^m[n]_m$, таким образом, убывающий и возрастающий факториалы находятся в двойственности. Теперь мы можем определить

$$\binom{-n}{m} = [-n]_m/m! = (-1)^m[n]^m/m!$$

Комментарий: Комбинаторные формулы versus знакопеременных. Мы распространили биномиальные коэффициенты на отрицательные значения аргументов, потому что получать формулы для $\mathbb{Z}$ обычно значительно проще, чем для $\mathbb{N}$. Однако в **знакопеременных** формулах (типа 'включения-исключения', см. § 4) не все слагаемые имеют комбинаторный смысл, написать их обычно просто, а реально считать при помощи них что-то очень долго и дорого. *Основным* содержанием комбинаторики является борьба за **комбинаторные формулы**, в которых все слагаемые положительны.

В Разделе IV мы обсуждаем еще одно важнейшее обобщение биномиальных коэффициентов: гауссовские коэффициенты $\binom{n}{m}_q$.

§ 3. Пересечение и объединение

Булевыми операциями обычно называются следующие четыре бинарные операции на множествах: пересечение, объединение, разность, симметрическая разность. Существование всех операций, *кроме* объединения, гарантируется аксиомой **ZF6′**, так как здесь результат операции возникает как подмножество уже имеющегося множества. С другой стороны, существование объединения нужно постулировать отдельно.

1. Пересечение. Первая важнейшая операция над множествами, пересечение (intersection, Durchschnitt) является просто переводом конъюнкции с интенционального на экстенсиональный язык.

Определение. Пересечением *двух множеств X и Y называется множество $X \cap Y$, состоящее из тех и только тех элементов, которые принадлежат обоим множествам X и Y,*

$$X \cap Y = \{x \in X \mid x \in Y\} = \{x \in Y \mid x \in X\}.$$

Упомянутая выше аналогия с конъюнкцией эксплицируется следующим образом: если X – подмножество множества U, выделенное свойством P, а Y – подмножество того же множества, выделяемое свойством Q, то

$$X \cap Y = \{x \in U \mid P(x)\} \cap \{x \in U \mid Q(x)\} = \{x \in U \mid P(x) \ \&\ Q(x)\}.$$

В терминах включения пересечение можно определить так: пересечение множеств X и Y – это инфимум пары $\{X, Y\}$, иными словами, *наибольшее* множество Z такое, что $Z \subseteq X$ и $Z \subseteq Y$. В частности, $X \cap Y = X \iff X \subseteq Y$ и, соответсвенно, $X \cap Y = Y \iff Y \subseteq X$.

2. Объединение. Точно так же вторая важнейшая операция, объединение (union, Vereinigung), является экстенсиональным аналогом дизъюнкции.

Определение. Объединением *множеств X и Y называется множество $X \cup Y$, состоящее из тех и только тех элементов, которые принадлежат по крайней мере одному из множеств X и Y,*

$$X \cup Y = \{x \mid x \in X \vee x \in Y\}.$$

Мы договорились, что запись $\{x \mid P(x)\}$ не имеет смысла (по крайней мере до тех пор, пока не проверено, что свойство P является коллективизирующим), но в данном случае существование $X \cup Y$ гарантируется аксиомой **ZF4**.

Контрольный вопрос в голову. Пересечение множества прямоугольников и множества ромбов есть множество квадратов. Верно ли, что их объединение есть множество параллелограммов?

К объединению применимо все, что было сказано выше о пересечении. Так, если, как и выше, X и Y – подмножества множества U, выделенные свойствами P и Q, соответственно, то

$$X \cup Y = \{x \in U \mid P(x)\} \cup \{x \in U \mid Q(x)\} = \{x \in U \mid P(x) \vee Q(x)\}.$$

В терминах включения объединение множеств X и Y определяется как супремум пары $\{X, Y\}$, иными словами, *наименьшее* множество Z такое, что $Z \supseteq X$ и $Z \supseteq Y$. В частности, $X \cup Y = X \iff X \supseteq Y$ и, соответсвенно, $X \cup Y = Y \iff Y \supseteq X$. Обратите внимание, что заменяя во всех формулах $\cap$ на $\cup$, $\&$ на $\vee$, а $\subseteq$ на $\supseteq$ мы снова получаем верные формулы. Эта двойственность между пересечением и объединением детально обсуждается в § ?.

В TEX'е знак пересечения $\cap$ называется `\cap`, а знак объединения $\cup$ – `\cup` (кепка и чашка[146]). Чтобы не путать, что есть что, начинающему достаточно запомнить одно из трех следующих мнемонических соображений:

• Знаки $\cap$ и $\cup$ являются графическими вариантами знаков $\wedge$ и $\vee$, соответственно (уже было объяснено, что $\vee$ это просто стилизованное начертание буквы 'V', первой буквы латинского союза 'vel' – или).

• Операция $\cap$ является аналогом произведения (в § ? мы придадим этому утверждению совершенно точный смысл!) и $\cap$ можно вопринимать как стилизованный знак произведения $\sqcap$.

• Знак $\cup$ является сокращением, происходящим от буквы 'U' – первой буквы английского слова union (в действительности, конечно, от итальянского unione!).

3. Примеры пересечений и объединений. Предполагая, что читатель уже знаком с этими операциями из школьного курса, ограничимся следующими элементарными примерами.

• Пусть $X = \{a, b, c\}$, $Y = \{a, c, d\}$. Тогда $X \cap Y = \{a, c\}$, а $X \cup Y = \{a, b, c, d\}$.

• Пусть $f, g \in \mathbb{R}[x, y]$ – два многочлена от переменных x, y. Решить уравнение $f(x, y) = 0$ означает найти уравнитель отображений $X = \mathrm{Eq}(f, 0)$ Точно так же, решить уравнение $g(x, y) = 0$ означает найти уравнитель $Y = \mathrm{Eq}(g, 0)$. Решить систему уравнений

$$\begin{cases} f(x, y) = 0 \\ g(x, y) = 0 \end{cases}$$

означает найти пересечение $X \cap Y$ этих уравнителей.

• В школьном курсе алгебры часто пользуются записью

$$\begin{bmatrix} f(x, y) = 0 \\ g(x, y) = 0 \end{bmatrix}$$

[146]Общепринятые сегодня в английском языке названия cap и cup были предложены Уитни.

указывающей на то, что мы ищем множество пар $(x, y) \in \mathbb{R}^2$, удовлетворяющих хотя бы одному из уравнений, $f(x, y) = 0$ и $g(x, y) = 0$, т.е. в обозначениях предыдущего примера ищется объединение $X \cup Y$.

• Во всех основных графических программах имплементированы операции $\cap$ и $\cup$ над плоскими фигурами. В `Adobe Illustrator` эти операции так и называются `Intersect` и `Unite`.

Задача. Чему равно пересечение двух интервалов вещественной оси?

Ответ. Пусть (a, b), $a < b$ и (c, d), $c < d$, два интервала. Если $b \leq c$ или $d \leq a$, то их пересечение пусто. Если же $b > c$ и $d > a$, то пересечение этих интервалов является интервалом $(\max(a, c), \min(b, d))$.

Задача. Рассмотрим два интервала вещественной оси (a, b), $a < b$, и (c, d), $c < d$. Когда их объединение снова является интервалом? Чему оно равно в этом случае?

Ответ. Тогда и только тогда, когда (a, b) и (c, d) пересекаются, т.е. когда $c < b$ и $a < d$. В этом случае их объединение равно $(\min(a, c), \max(b, d))$.

Задача. Докажите следующую **лемму Данжу**: если три интервала вещественной оси имеют общую точку, то по крайней мере один из них содержится в объединении двух других.

Решение. Пусть $I_i = (a_i, b_i)$, $a_i < b_i$, где $i = 1, 2, 3$ – три интервала. По условию найдется такая точка $x \in \mathbb{R}$, что $a_i < x < b_i$ для всех $i = 1, 2, 3$. Дважды применяя результат предыдущей задачи, получаем

$$I_1 \cup I_2 \cup I_3 = (\min(a_1, a_2, a_3), \max(b_1, b_2, b_3)).$$

Возьмем какое-то i такое, что $\min(a_1, a_2, a_3) = a_i$. Теперь возьмем какое-то $j \neq i$ такое, что $\max(b_1, b_2, b_3) = b_j$, либо, если такого j не существует (иначе говоря, если $b_i > b_j$ для $j \neq i$), то вообще любое $j \neq i$. Тогда $I_i \cup I_j = (a_i, b_j) = I_1 \cup I_2 \cup I_3$, так что, если h индекс такой, что $\{i, j, h\} = \{1, 2, 3\}$, то $I_h \subseteq I_i \cup I_j$.

§ 4. Тождества для объединения и пересечения: решетки

> Самую большую величину, вне которой ничего нет, я называю великим единством; самую малую малость, внутри которой ничего нет, я называю малым единством. То, что не обладает толщиной, не может быть накоплено и все же его громада простирается на тысячу ли[147]. Великое тождество отличается от малого тождества — это я называю малым различием тождеств. Вся тьма вещей абсолютно тождественна и абсолютно различна — это я называю большим различием тождеств.
>
> Ху(э)й Ши (цитируется по Чжуан-цзы, Гл. 33, Поднебесная)

В настоящем пункте мы установим, что булеан 2^U произвольного множества U является дистрибутивной решеткой с 0 и 1 относительно операций пересечения и объединения.

1. Основные тождества. Перечислим основные тождества, которым подчиняются операции пересечения и объединения. Все эти тождества, как и тождества возникающие в дальнейшем, легко доказать, пользуясь свойствами логических связок и аксиомой объемности. Иными словами, для того, чтобы

[147] **Ли** – китайская мера длины, в русском переводе обычно передается как **миля**. **Тысяча ли** или **десять тысяч ли** — устойчивые выражения, обозначающие огромное расстояние или протяженность, например, 'путь в тысячу ли начинается с одного шага' (Дао де цзин) или в 'скакуны Ци-цзи и Хуа-лю за день пробегали тысячу ли' (Чжуан-цзы, глава 17, 'Осенний разлив').

проверить, что $X = Y$ нужно проверить, что для любого $x \in X$ выполнено $x \in Y$, а для любого $y \in Y$ выполнено $y \in X$. Пример такой проверки, приводится в § ? при обсуждении свойств симметрической разности. Все остальные подобные проверки проводятся по такой же схеме и предоставляются читателю в качестве упражнения. Начинающему настоятельно рекомендуется провести три-четыре подобных доказательства самостоятельно.

L1 Ассоциативность

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

L2 Коммутативность

$$X \cup Y = Y \cup X, \qquad X \cap Y = Y \cap X.$$

L3 Идемпотентность

$$X \cup X = X, \qquad X \cap X = X.$$

L4 Поглощение

$$X \cap (X \cup Y) = X, \qquad X \cup (X \cap Y) = X.$$

Тождества ассоциативности и коммутативности для этих операций были явно сформулированы Булем. Ассоциативности позволяет определить объединение и пересечение любого конечного семейства множеств. А именно, мы можем положить $A \cup B \cup C = (A \cup B) \cup C$ и $A \cap B \cap C = (A \cap B) \cap C$. Идемпотентность была впервые в явной форме упомянута Лейбницем, а поглощение – Грассманом. В предыдущем параграфе мы уже встречались с поглощением в форме *условных* тождеств: $A \subseteq B \Longrightarrow A \cap B = A$ и, соответственно, $A \supseteq B \Longrightarrow A \cup B = A$.

2. Решетки. Введем один из важнейших классов алгебраических систем, впервые определенный *в таком виде* Эрнстом Шредером[148,149] и Рихардом Дедекиндом[150]. Дедекинд впервые отметил универсальность этого понятия и его возникновение за пределами логики и теории множеств, в теории чисел[151] и алгебре (решетка делителей, решетка идеалов, решетка подгрупп, решетка нормальных подгрупп и т.д.).

---

[148]E.Schröder, Algebra der Logik. Bd.I–III, Leipzig, 1890–1895. Именно в этой книге аксиомы L1–L4 впервые явно выделены из аксиом булевой алгебры.

[149]**Эрнст Шредер** (25.11.1841, Пфорцхайм – 16.06.1902, Карлсруэ) – немецкий логик и алгебраист. С 1874 года был профессором Политехнического Института в Дармштадте и Карслуэ. В отличие Буля и большинства его последователей Шредер первым начал явным образом выделять, что в алгебре логики принимается в качестве аксиом, и доказывать все остальное. Он первым явно сформулировал несколько важных принципов в этой области, в том числе принцип двойственности.

[150]R.Dedekind, Über Zerlegungen von Zahlen durch ihre grössten gemeinsamen Teiler. – Festschrift Techn. Hochschule Braunschweig, 1897.

[151]Впервые эти идеи были опубликованы в написанном Дедекиндом приложении к 4-му издании книги P.G.Lejeune Dirichlet, Vorlesungen über Zahlentheorie, Braunschweig, 1894, однако в русском переводе (П.Г.Лежен Дирихле, Лекции по теории чисел, ОНТИ, М.–Л., 1936, с.1–403) это приложение опущено!

Определение. *Непустое множество L, на котором заданы две операции $\cap$ и $\cup$, удовлетворяющие перечисленным выше тождествам* L1–L4*, называется* **решеткой**.

В действительности, решетки относятся к числу нескольких *самых* фундаментальных и часто встречающихся алгебраических структур. Кроме теории множеств, логики, алгебры и теории чисел решетки на каждом шагу возникают в теории вероятностей, теории функций, теории меры, топологии, функциональном анализе и т.д. К решеткам применимы все обычные алгебраические понятия и конструкции. В частности, непустое подмножество M решетки L называется **подрешеткой**, если M замкнуто относительно $\cap$ и $\cup$, т.е. из того, что $X, Y \in M$ вытекает, что $X \cap Y, X \cup Y \in M$. Отображение $f : L \longrightarrow M$ одной решетки в другую называется **гомоморфизмом**, если оно сохраняет операции $\cap$ и $\cup$, т.е. $f(X \cap Y) = f(X) \cap f(Y)$ и $f(X \cup Y) = f(X) \cup f(Y)$ для любых $X, Y \in L$. Отображение $f : L \longrightarrow M$ одной решетки в другую называется **дуальным гомоморфизмом**, если оно *переставляет* операции $\cap$ и $\cup$, т.е. $f(X \cap Y) = f(X) \cup f(Y)$ и $f(X \cup Y) = f(X) \cap f(Y)$ для любых $X, Y \in L$.

Сказанное в предыдущем пункте означает, что для любого множества U его булеан 2^U будет решеткой относительно обычных операций объединения и пересечения. Конечно, решеткой будет и любое непустое подмножество $L \subseteq 2^U$, замкнутое относительно $\cap$ и $\cup$. Вот два важнейших примера подрешеток в 2^U:

• Множество $\bigwedge(U)$ всех конечных подмножеств в U.

• Множество $\mathrm{Cof}(U)$ всех ко-конечных подмножеств в U. Подмножество в $X \subseteq U$ называется **ко-конечным**, если для всех элементов $x \in U$, кроме конечного числа, также $x \in X$.

Оказывается, решетки можно определить совершенно иначе. А именно, если L – произвольная решетка, мы можем определить на L частичный порядок полагая $X \leq Y$ в том и только том случае, когда $X \cap Y = X$ или, что то же самое, когда $X \cup Y = Y$.

Задача. Проверьте, что так введенное отношение $\leq$ превращает L в частично упорядоченное множество, в котором для любых двух элементов $X, Y \in L$ существует инфимум и супремум, причем $\inf(X, Y) = X \cup Y$ и $\sup(X, Y) = X \cup Y$.

Обратно (см. [Bi2], Теорема 8 на стр.23), если у нас имеется такое частично упорядоченное множество L, что для любых двух его элементов X, Y существуют $\inf(X, Y)$ и $\sup(X, Y)$, то мы можем превратить его в решетку в нашем смысле, полагая $X \cap Y = \inf(X, Y)$ и $X \cup Y = \sup(X, Y)$. Именно так решетки и были первоначально определены Пирсом в 1880 году[152]. В главе V мы вернемся к определению решеток как частично упорядоченных множеств.

[152]C.S.Peirce, On the algebra of logic. – Amer. J. Math., 1880, vol.3, p.17–57. При этом Пирс считал все решетки дистрибутивными, на ошибочность чего указал в 1894 году Э.Шредер. Однако Пирс продолжал настаивать на своем. Вот цитата из письма Пирса Хантингтону от 14.02.1904: "Дело в том, что упомянутая статья была написана в дни вынужденного досуга, предоставленного мне сильнейшим гриппом. Готовя работу к печати, я опустил доказательство, отметив, что оно "слишком длинное и неинтересное" и что оно кажется мне достаточно очевидным. Но когда Д-р Шредер усомнился в самой его возможности, я оказался не в состоянии восстановить ход его рассуждений и подумал, что, таким образом, обнаружена еще одна из многочисленных в этой работе нелепых ошибок, которыми я был обязан гриппу." – E.V.Huntington, Sets of independent postulates for the algebra of logic, Trans. Amer. Math. Soc., 1904, vol.5, p.288–309, см также [Sal], стр.48–50. Именно под влиянием этой дискуссии Дедекинд и начал изучать тождества дистрибутивности и модулярности решеток.

3. Решетка вещественных функций. В дальнейшем нам встретится много примеров решеток. Однако, чтобы сразу дать читателю мысленный образ решетки, которая (на первый взгляд!) отлична от решетки множеств, приведем следующий пример. Пусть $L = \mathbb{R}^{\mathbb{R}}$ – множество вещественнозначных функций вещественного аргумента. Операции $\cup$ и $\cap$ на этом множестве вводятся следующим образом[153]

$$(f \cup g)(x) = \max(f(x), g(x)), \qquad (f \cap g)(x) = \min(f(x), g(x)).$$

Функция $f \cup g$ называется **верхней огибающей** функций f и g, а функция $f \cap g$ – их **нижней огибающей**.

Задача. Покажите, что L образует (дистрибутивную) решетку относительно введенных операций.

Многие важные классы функций замкнуты относительно верхних и нижних огибающих, даже если они не замкнуты относительно других обычных операций, скажем, относительно произведения функций. Например, таким свойством обладает класс всех функций, интегрируемых по Лебегу[154].

Задача. Докажите, что отображение $L \longrightarrow L$, $f \mapsto -f$, где $(-f)(x) = -f(x)$ является дуальным автоморфизмом решетки $L = \mathbb{R}^{\mathbb{R}}$, т.е.

$$-(f \cup g) = (-f) \cap (-g), \qquad -(f \cap g) = (-f) \cup (-g).$$

Почему в элементарных курсах анализа не принято говорить об этой решетке? Дело в том, что там принято выражать все свойства этой решетки при помощи одной *унарной* операции $|\ | : L \longrightarrow L$, $f \mapsto |f|$, определенной посредством $|f| = f \cup (-f)$. Ясно, что $\cup$ и $\cap$ выражаются в терминах этой операции, хотя и не очень естественно:

$$f \cup g = \frac{1}{2}(f + g + |f - g|), \qquad f \cap g = \frac{1}{2}(f + g - |f - g|).$$

Но, конечно, более компетентные и алгебраически настроенные аналисты[155] явным образом вводят на L структуру, определенную операциями $\cup$ и $\cap$.

4. Нейтральные элементы. Продолжим рассмотрение решетки $L = 2^U$ всех подмножеств фиксированного множества U. В этой решетке есть элементы

L5′ Существование нуля

$$X \cap \varnothing = \varnothing, \qquad X \cup \varnothing = X.$$

L5″ Существование единицы

$$X \cap U = X, \qquad X \cup U = U.$$

В абстрактных решетках эти элементы обычно обозначаются через 0 и 1, что и объясняет их названия. Заметим, что, вообще говоря, они не обязаны существовать. Так, например, если множество U бесконечно, то в $\bigwedge(U)$ есть 0, но нет 1, а в $\mathrm{Cof}(U)$ есть 1, но нет 0. Решетка L называется **решеткой с 0 и 1**, если в ней существуют элементы, удовлетворяющие аксиомам L5′ и L5″, соответственно. Как только что отмечено, 2^U – решетка с 0 и 1.

Предостережение. Наша нумерация аксиом слегка отличается от принятой специалистами по теории решеток. А именно, во-первых, так как тождество ассоциативности представляется мне самым фундаментальным из всех, я переставил аксиомы L1 и L3, поставив его на первое место. Во-вторых, вместо существования 0 и 1 в [Bi2] в качестве аксиомы L5 фигурирует модулярность.

---

[153] См., например, K.Maurin, Analiza, I – Elementy. – PWN, Warszawa, 1971, p.1–486, стр. 311 и далее.

[154] Б.Гелбаум, Дж.Олмстед, Контрпримеры в анализе. – Мир, М., 1967, с.1–251. Глава 13.

[155] Некоторые **аналитики** возражают против недискриминированного использования формы **аналист**, однако эта форма вполне отвечает правилам русского языка, параллельна таким общеупотребительным словам, как **даосист**, **алгебраист**, **таксидермист** и многократно использовалась Набоковым, который говорил **психоаналист**, а не **психоаналитик**.

§ 5. Тождества, связывающие пересечение с объединением: дистрибутивные и модулярные решетки

До сих пор мы изучали $\cap$ и $\cup$ по отдельности. Сейчас мы посмотрим, как они связаны между собой.

1. Дистрибутивность. В действительности операции объединения и пересечения дистрибутивны друг относительно друга. Так как мы уже знаем, что эти операции коммутативны, достаточно записать тождества левой дистрибутивности.

L6 Дистрибутивность.

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C), \qquad A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$

Дистрибутивность пересечения относительно объединения была впервые явно сформулирована Булем, а объединения относительно пересечения – Пирсом. Вообще говоря, L6 не вытекает из остальных аксиом, решетка, для которой она выполняется, называется **дистрибутивной**. В дальнейшем нам встретится много решеток, которые не являются дистрибутивными, скажем, решетка подпространств векторного пространства, решетка подгрупп группы, и т.д. Оказывается, с учетом предыдущих аксиом достаточно проверять только один из фигурирующих в L6 законов дистрибутивности (см. [Bi2], Теорема 9 на стр.24).

Задача. Пусть L – абстрактная решетка. Проверьте, что каждый из законов дистрибутивности влечет второй закон.

Следующий замечательный результат утверждает, что в действительности никаких дистрибутивных решеток, кроме подрешеток в 2^U, нет.

Теорема Биркгофа. *Всякая дистрибутивная решетка изоморфна подрешетке в 2^U для подходящего множества U.*

Доказательство этой теоремы несложно, но использует некоторые конструкции общей алгебры (такие, скажем, как подпрямое произведение), поэтому мы не можем его здесь привести, см., например, [Sal], стр. 34–35.

2. Модулярность. В действительности, большинство реально возникающих в алгебре решеток не являются дистрибутивными, но удовлетворяют несколько более слабому условию модулярности, впервые отмеченному Дедекиндом.

Задача. Покажите, что если L дистрибутивная решетка, то для ее элементов выполнено следующее **тождество модулярности**

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

Однако чаще условие модулярности формулируют не в виде тождества, а в виде **условного тождества** (в общей алгебре условные тождества принято называть **квазитождествами**).

Задача. Докажите, что выполнение тождества модулярности эквивалентно выполнению следующего **квазитождества модулярности**

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

Решение. В самом деле, предположим, что выполняется тождество модулярности. Тогда, если $X \leq Z$, то

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

Обратно, если верно квазитождество модулярности, то, так как $X \cap Z \leq Z$, его можно применить к $(X \cap Z) \cup (Y \cap Z)$.

Решетка называется **модулярной** или **дедекиндовой**, если в ней выполняется тождество модулярности. Как только что было замечено, каждая дистрибутивная решетка модулярна. Однако обратное, вообще говоря, безнадежно неверно: решетки подпространств векторного пространства, идеалов кольца, нормальных подгрупп группы и т.д. модулярны, но не дистрибутивны! А решетка всех подгрупп группы, вообще говоря, не является даже модулярной.

§ 6. Медиана

В действительности обе операции $\cap$ и $\cup$ легко восстанавливаются по одной *тернарной* операции на подмножествах. Следующий цикл задач взят из книги Гаррета Биркгофа [Bi1], в особенности стр. 196–197.

Задача. Докажите, что если L – дистрибутивная решетка, то

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

Определим теперь **медиану** трех множеств равенством

$$M(X, Y, Z) = (X \cap Y) \cup (X \cap Z) \cup (Z \cap X)$$

Как показывает предыдущая задача, мы могли бы в этом определении поменять местами $\cap$ и $\cup$.

Задача. Убедитесь, что медиана X, Y, Z состоит из тех элементов, которые принадлежат по крайней мере двум из множеств X, Y, Z.

В частности, медиана симметрична относительно любых перестановок X, Y, Z:

$$M(X, Y, Z) = M(X, Z, Y) = M(Y, X, Z) = M(Y, Z, X) = M(X, Y, Z) = M(Z, Y, X).$$

Смысл введения медианы состоит в том, что она описывает теоретико-множественное отношение **лежать между** в том же самом духе, в каком $\cap$ и $\cup$ описывают отношения $\subseteq$ и $\supseteq$.

Задача. Докажите, что $M(X, Y, Z) = Z$ в том и только том случае, когда $X \cap Y \subseteq Z \subseteq X \cup Y$.

Задача. Докажите, что $M(X, Y, Z) = W$ в том и только том случае, когда

$$X \cap Y \subseteq W \subseteq X \cup Y, \qquad X \cap Y \subseteq W \subseteq X \cup Y, \qquad X \cap Y \subseteq W \subseteq X \cup Y.$$

Указание. Используйте результаты предыдущих задач!

Перейдем теперь к рассмотрению случая, когда все наши подмножества являются подмножествами фиксированного универсального множества U.

Задача. Убедитесь, что

$$X \cap Y = M(X, Y, \varnothing), \qquad X = M(\varnothing, X, U), \qquad X \cup Y = M(X, Y, U).$$

Задача. Докажите, что переход к дополнению является автоморфизмом относительно медианы, т.е. $M(X, Y, Z)' = M(X', Y', Z')$.

Эту задачу можно значительно усилить. В случае $|U| = n$ у алгебры $(2^U, \cap, \cup)$ имеется $n!$ автоморфизмов, которые образуют симметрическую группу $S_U \cong S_n$. Медиана замечательна тем, что она дает наиболее простой способ реализации октаэдральной группы Oct_n.

Задача. Пусть $|U| = n$. Докажите, что у алгебры $(2^U, M)$ ровно $2^n n!$ автомоморфизмов.

Вот на закуску несколько более экзотических тождеств, показывающих, что приходит на замену идемпотентности и ассоциативности для тернарных операций.

Задача. Докажите, что

1) $M(X, M(X, Y, Z), Z) = M(X, Y, Z)$;
2) $M(X, Y, M(Z, U, V)) = M(M(X, Y, Z), U, M(X, Y, V)$;
3) $M(M(X, Y, Z), U, V) = M(M(X, U, V), Y, M(Y, Z, V))$.

§ 7. Метод включения-исключения

Сейчас мы опишем важнейший комбинаторный инструмент, которым мы будем постоянно пользоваться в дальнейшем.

1. Формула включения-исключения для двух или трех множеств. Пусть вначале $X = \cup X_i$, $i \in I$, – покрытие множества X. Мы хотим вычислить $|X|$. В качестве первого приближения воспользуемся правилом суммы. Однако при этом элементы, принадлежащие более чем одному множеству X_i будут посчитаны несколько раз и для получения правильного ответа мы должны их исключить. При этом мы исключим те элементы, которые содержатся более, чем в двух множествах X_i слишком много раз, и нам придется их снова включить и т.д.

Посмотрим, прежде всего, как выглядит формула включения-исключения для небольшого количества множеств. Для двух множеств эта формула записывается в виде

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Для трех множеств она приобретает вид

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

И в том и в другом случае ее легко переписать в виде **комбинаторных формул** $|A \cup B| = |A| + |B \setminus A|$ и $|A \cup B \cup C| = |A \setminus B| + |B \setminus C| + |C \setminus A| + |A \cap B \cap C|$.

Задача. Напишите формулу включения-исключения в случае четырех множеств. Верно ли, что эту формулу можно переписать в виде комбинаторной формулы $|A \cup B \cup C \cup D| = |A \setminus B| + |B \setminus C| + |C \setminus D| + |D \setminus A| + |A \cap B \cap C \cap D|$?

Указание. Второй вопрос состоит из двух частей: верно ли, что $A \cup B \cup C \cup D = (A \setminus B) \cup (B \setminus C) \cup (C \setminus D) \cup (D \setminus A) \cup (A \cap B \cap C \cap D)$ и верно ли, что пять подмножеств в правой части этого выражения попарно дизъюнктны?

2. Общая формула включения-исключения. Часто нам дан порядок объединения множеств, порядки попарных разностей и т.д., а неизвестным является какой-то из порядков пересечений. На этой идее основано большое количество фольклорных задач.

Задача (формула включения-исключения). Докажите, что имеет место равенство

$$|\cup X_i| = \sum |X_i| - \sum |X_i \cap X_j| + \sum |X_i \cap X_j \cap X_h| - \dots$$

где первая сумма берется по всем i, вторая – по всем $i < j$, третья – по всем $i < j < h$ и т.д.

Указание. Используйте индукцию по n.

Следствие: формула решета. *Пусть теперь X_i, $i \in I$, – любая система подмножеств в X. Тогда из последней задачи следует, что число $|X \setminus \cup X_i|$ элементов множества X, не содержащихся ни в одном из множеств X_i равно*

$$|X \setminus \cup X_i| = |X| - \sum |X_i| + \sum |X_i \cap X_j| - \sum |X_i \cap X_j \cap X_h| + \dots .$$

Эта формула называется **формулой решета**. Несмотря на свою крайнюю простоту она позволяет дать замечательно простые доказательства некоторых чрезвычайно важных арифметических фактов.

Задача: формула для функции Эйлера Известно, что для любого натурального n количество $\varphi(n)$ чисел между 0 и $n-1$ взаимно простых с n равно

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_s}\right),$$

где $p_1,\dots,p_s$ пробегает все различные простые делители числа n. Докажите это используя формулу решета.

Указание. $|X \setminus \cup X_i|$, $1 \le i \le s$.

Задача. Пусть $|X| = m$, а $|Y| = n$. Докажите, что

$$|\operatorname{Sur}(X,Y)| = n^m - n(n-1)^m + \binom{n}{2}(n-2)^m - \dots + (-1)^{n-1}\binom{n}{n-1}.$$

Задача ('задача Монмора'). Найти число D_n **беспорядков**, т.е. таких перестановок из S_n, которые не оставляют на месте ни одного символа.

Ответ. По формуле решета получаем, что

$$D_n = n!(1 - 1/1! + 1/2! - \dots + (-1)^n 1/n!)$$

Интересно, что формула в скобках – это начало разложения в ряд для e^{-1}. Таким образом, для не слишком маленьких n число $e^{-1} > 1/3$ является **очень** хорошим приближением для отношения $D_n/n!$, т.е. вероятности того, что наугад взятая перестановка n символов не оставляет на месте ни одного символа. Совершенно удивительно, что эта вероятность практически не зависит от n! Как замечает по этому поводу Райзер [Ry], "для всех практических целей вероятность **равна** e^{-1}" ("для гренландских китов $\pi = 3$").

Задача. Сколькими способами можно расставить шахматной доске 8 ладей так, чтобы ни одна из них не била другие и чтобы ни одна не стояла на главной диагонали a8–h1.

§ 8. Разность множеств

В этом параграфе мы продолжим определять булевы операции, а именно, введем и изучим разность множеств.

1. Разность. Как всегда, начнем с определения.

Определение. Разностью *двух множеств X и Y называется множество $X \setminus Y$, состоящее из тех и только тех элементов, которые принадлежат множеству X, но не принадлежат множеству Y,*

$$X \setminus Y = \{x \in X \mid x \notin Y\}.$$

Если X – подмножество множества U, выделенное свойством P, а Y – подмножество того же множества, выделяемое свойством Q, то

$$X \setminus Y = \{x \in U \mid P(x)\} \setminus \{x \in U \mid Q(x)\} = \{x \in U \mid P(x) \ \&\ \neg Q(x)\}.$$

В терминах включения разность можно определить так: разность множеств X и Y – это наибольшее подмножество в X, которое не пересекается с Y. Операции пересечения и разности не являются независимыми, а именно, пересечение следующим образом выражается через разность: $A \cap B = A \setminus (A \setminus B)$. В TEX'е знак теоретико-множественной разности $\setminus$ называется `\setminus`.

2. Примеры разности. В школе мы сталкивались с разностью каждый раз, когда нужно было исключить 'лишние' решения.

• Пусть, $f, g \in \mathbb{R}[x, y]$. Как и в § 3, положим $X = \mathrm{Eq}(f, 0)$, $Y = \mathrm{Eq}(g, 0)$. Тогда множество решений уравнения $f(x, y)/g(x, y) = 0$ равно $X \setminus Y$.

• Пусть, теперь $f, g \in \mathbb{R}[x]$. Обычным методом решения уравнения $\sqrt{f(x)} = g(x)$ в школьной алгебре является возведение в квадрат и последующее решение уравнения $f(x) = g(x)^2$. Пусть $X = \mathrm{Eq}(f, g^2)$ – множество решений этого уравнения. Чтобы получить из X то, что считается множеством решений уравнения $\sqrt{f(x)} = g(x)$ согласно великим методистским премудростям, нужно рассмотреть $X \setminus Y$, где $Y = \{x \in \mathbb{R} \mid f(x) < 0\}$.

• В основных графических пакетах имплементирована и операция $\setminus$ над плоскими фигурами. В действительности, в `Adobe Illustrator` таких операций целых две, и называются они `MinusFront` и `MinusBack`. Как Вы думаете, почему? Ответ дается в следующем пункте.

Задача. Чему равно пересечение двух интервалов вещественной оси?

3. Свойства разности. Разность множеств, вообще говоря, не является ни коммутативной, ни ассоциативной.

Задача. Когда $A \setminus B = B \setminus A$?

Задача. (i) Докажите, что для любых трех множеств имеет место включение $(A \setminus B) \setminus C \subseteq A \setminus (B \setminus C)$.

(ii) Приведите пример трех множеств, для которых это включения является строгим.

(iii) Верно ли, что $(A \setminus B) \setminus C = (A \setminus C) \setminus B$?

(iv) Верно ли, что $(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C)$?

Решение. Левая часть i) состоит из тех $x \in A$, которые не лежат ни в B, ни в C, в то время как правая часть и, тем самым, содержится в $A \setminus B$. Правая же часть состоит из тех $x \in A$, который не лежат в $B \setminus C$ и, тем самым содержит $A \setminus B$. Можно объяснить это и по другому: левая часть состоит из тех x, для которых $x \in A \ \ \& \ \ x \notin B \ \ \& \ \ x \notin C$, в то время как правая часть – из тех x, для которых $(x \in A \ \ \& \ \ x \notin B) \vee (x \in A \ \ \& \ \ x \in C)$ (см. § ?). Таким образом, чтобы привести пример трех множеств, для которых здесь имеет место строгое неравенство, достаточно взять три любых множества, для которых $A \cap C$ не содержится в B. Что касается iii) и iv), эти тождества верны.

4. Формулы де Моргана[156]**.** Разность **дистрибутивна справа** относительно пересечения и объединения. Иными словами, для любых трех множеств имеют место равенства

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

[156]**Август де Морган** (1806 Индия –1871) – знаменитый английский логик и математик. После обучения в Кембридже с 1828 по 1866 годы (с небольшим перерывом) был профессором University College в Лондоне, где среди его учеников был, в частности, Дж.Сильвестр. Де Морган первым явно ввел понятие отношения и основные операции над отношениями, которые в дальнешем изучали Шредер, Кантор и Пеано. Он заметил аналогию тождеств, которым удовлетворяют операции над высказываниями в логике, числами в алгебре и событиями в теории вероятностей, которую потом детально обсуждали Буль и другие

Задача. Запишите правую дистрибутивность относительно пересечения как тождество, в котором фигурирует только разность.

Ответ. $(A \setminus (A \setminus B)) \setminus C = (A \setminus C) \setminus ((A \setminus C) \setminus (B \setminus C))$.

Задача. Верно ли, что разность множеств **дистрибутивна слева** относительно пересечения и объединения, т.е. что для любых трех множеств имеют место равенства $A \setminus (B \cap C) = (A \setminus B) \cap (A \setminus C)$ и $A \setminus (B \cup C) = (A \setminus B) \cup (A \setminus C)$?

Ответ. Нет, неверно! Приведите примеры, показывающие, что дистрибутивность слева не имеет места.

В действительности заменой левой дистрибутивности разности относительно пересечения и объединения являются **формулы де Моргана**, в которых пересечение и объединение меняются местами:

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

Кажется, что эти формулы были известны всегда и невозможно представить, чтобы их не знали Лейбниц и Эйлер, однако в действительности, они были впервые опубликованы лишь А.де Морганом в 1848 году и Ч.С.Пирсом в 1867 году.

Предоставим начинающему проверить еще несколько тождеств, в которые входят пересечение, объединение и разность.

Задача. Докажите, что

i) $A \setminus B = A \setminus (A \cap B)$;

ii) $A \cap (B \setminus C) = (A \cap B) \setminus C$;

iii) $A \cap (B \setminus C) = B \cap (A \setminus C)$;

iv) $A \cap (B \setminus A) = \varnothing$;

v) $(A \setminus B) \cap (C \setminus D) = (A \setminus D) \cap (C \setminus B)$.

Решение. Обе части i) состоят из тех x, для которых $x \in A \ \ \& \ \ x \notin B$. Обе части ii) состоят из тех x, для которых $x \in A \ \ \& \ \ x \in B \ \ \& \ \ x \notin C$. Заметим, что ii) представляет собой видоизменение правой дистрибутивности. Теперь iii) следует из ii) с учетом коммутативности пересечения, а iv) моментально вытекает из iii) и свойства поглощения для пересечения $A \cap (B \setminus A) = B \cap (A \setminus A) = B \cap \varnothing = \varnothing$. Наконец, в v) обе части состоят из тех x, для которых $x \in A \ \ \& \ \ x \notin B \ \ \& \ \ x \in C \ \ \& \ \ x \notin D$.

Задача. Докажите, что

i) $(A \setminus B) \setminus C = A \setminus (B \cup C)$;

ii) $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$;

iii) $(A \cap B) \setminus (C \cup D) = (A \setminus C) \cap (C \setminus D)$;

§ 9. Дополнение: булевы алгебры

В этом параграфе мы завершим описание алгебры множеств.

1. Дополнение. Мы продолжаем рассматривать булеан 2^U множества фиксированного множества U. Пусть $X \subseteq U$. Разность $X' = U \setminus X$ называется **дополнением** к X или, если нужна особая точность, дополнением X в множестве U. В частности, $\varnothing' = U$ и $U' = \varnothing$

Многие авторы обозначают дополнение к X через $\complement X$, или, если нужно явно указать множество U, через $\complement_U X$. Знак $\complement$ является просто стилизованной буквой C – первой буквой слова complement. В TEX'е знак пересечения $\complement$ так и называется `\complement`.

Теперь мы готовы закончить формулировку аксиом булевой алгебры:

L7 Дополнительность $X \cap X' = \varnothing,\ \ X \cup X' = U$.

L8 Инволютивность $X'' = X$.

L9 Тождества де Моргана

$$(X \cap Y)' = X' \cup Y', \qquad (X \cup Y)' = X' \cap Y'.$$

Задача. Докажите, что

1) $X \subseteq Y \iff X' \supseteq Y'$.

2) $X \cap Y = \varnothing \iff X \subseteq Y' \iff Y \subseteq X'$.

3) $X \cup Y = U \iff X \supseteq Y' \iff Y \supseteq X'$.

2. Решетки с дополнениями. Пусть L – решетка с 0 и 1. Элемент Y называется **дополнением** элемента X, если $X \cap Y = 0$, $X \cup Y = 1$. Следующий результат был фактически замечен Грассманом.

Задача. Докажите, что в дистрибутивной решетке с 0 и 1 каждый элемент имеет не более одного дополнения.

Решение. В принципе доказательство очень похоже на доказательство единственности обратного элемента в моноидах, только вместо ассоциативности в нем используется ассоциативность. А именно, пусть Y, Z – два различных дополнения к элементу X. Тогда $Y = Y \cap 1 = Y \cap (X \cup Z) = (Y \cap X) \cup (Y \cap Z) = (0 \cup (Y \cap Z) = Y \cap Z$. Совершенно аналогично доказывается и равенство $Z = Y \cap Z$.

Решетка L с 0 и 1 называется **решеткой с дополнениями**, если любой ее элемент имеет дополнение. Решетка L называется **решеткой с единственными дополнениями**, если каждый ее элемент имеет *единственное* дополнение. Как было только что замечено, в *дистрибутивной* решетке с дополнениями дополнение *единственно*. Очевидно, что из коммутативности пересечения и объединения вытекает, что $(X')' = X$.

Задача. Пусть L – дистрибутивная рещетка с дополнениями. Докажите, что отображение $L \longrightarrow L$, $X \mapsto X'$, является дуальным автоморфизмом решетки L, иными словами, выполняются формулы де Моргана $(X \cap Y)' = X' \cup Y'$ и $(X \cup Y)' = X' \cap Y'$.

Указание. Так как $\cap$ и $\cup$ характеризуются как inf и sup относительно порядка $\leq$ на L, достаточно показать, что отображение $X \mapsto X'$ антитонно, т.е. $X \leq Y \Longrightarrow X' \geq Y'$.

Решение. В самом деле, пусть $X \leq Y$. Тогда

$$Y' = (X \cup X') \cap Y' = (X \cap Y') \cup (X' \cap Y') \leq (Y \cap Y') \cup (X' \cap Y') = (X' \cap Y'),$$

здесь мы воспользовались дистрибутивностью и тем, что $X \cup X' = 1$ и $Y \cap Y' = 0$. Но это и значит, что $Y' \leq X'$.

Дистрибутивные решетки с дополнениями называются **булевыми решетками**[157]. Сказанное в § 4 и предыдущем пункте означает, что 2^U является булевой алгеброй относительно обычных операций $\cap$ и $\cup$.

3. Булева алгебра. Дадим теперь абстрактное описание булевых алгебр. Кроме поведения множеств относительно булевых операций это понятие аксиоматизирует поведение высказываний в математической логике и событий в теории вероятности.

Определение. *Непустое множество A с двумя бинарными операциями $\cap$ и $\cup$ и одной унарной операцией $'$ называется булевой алгеброй, если эти операции удовлетворяют аксиомам* L1 – L9.

Итак булева алгебра это *по сути* то же самое, что булева решетка. Поясним, в чем именно состоит отличие. На профессиональном языке в булевой алгебре операция $'$ входит в сигнатуру, а в булевой решетке – нет. Это значит, что в булевой решетке по определению *две* операции $\cap$, $\cup$, а в булевой алгебре – *три*, $\cap$, $\cup$ и $'$. Тем самым, булева подрешетка булевой решетки A вместе каждыми двумя своими элементами X и Y содержит также $X \cap Y$ и $X \cup Y$, в то время как подалгебра булевой алгебры еще и X'. Точно так же, гомоморфизм булевых алгебр должен обладать дополнительным свойством $f(X') = f(X)'$.

Комментарий. Некоторые авторы говорят о булевой алгебре как о множестве с *двумя* операциями, но в этом случае это операции $\cap$ и $'$, либо $\cup$ и $'$. В самом деле, при наличии дополнения $\cup$ выражается через $\cap$ по тождеству де Моргана как $X \cup Y = (X' \cap Y')'$ и, соответственно, наоборот, $\cap$ выражается через $\cup$ по тождеству де Моргана как $X \cap Y = (X' \cup Y')'$.

В произвольной булевой алгебре имеются аналоги всех рассмотренных до сих пор операций и выполняются все тождества, которые мы проверяли в 2^U. Доказательство всех этих тождеств легко вытекает из аксиом L1 – L9. Например, $X \setminus Y$ можно определить как $X \setminus Y = X \cap Y'$. Попробуйте вывести установленные в предыдущем параграфе свойства разности только на основе аксиом.

4. Алгебры множеств. В самых различных областях математики на каждом шагу возникает следующий основной пример булевых алгебр. **Алгеброй множеств** называется произвольная булева подалгебра A алгебры 2^U. Иными словами, непустое подмножество $A \subseteq 2^U$ является алгеброй подмножеств U, если для любых $X, Y \in A$ также $X \cap Y, X \cup Y, X' \in A$. Тогда автоматически также и $X \setminus Y \in A$.

Комментарий. Впрочем, после полуторавековых упражнений терминология здесь все еще не установилась. Многие авторы говорят о **кольцах**, **полях** и даже **телах** множеств! Конечно, если бы эта тема привлекла внимание великого специалиста по подмножествам абстрактного пустого множества Никола Бурбаки[158], мы бы знали, какой терминологии придерживаться. Однако у Бурбаки теория интеграла строится на основе теоремы Рисса (которая принимается за определение) независимо от меры множеств, поэтому даже алгебры множеств

---

[157]Гливенко (В.К.Гливенко, Курс теории вероятностей, М.–Л., 1939, стр.209) пишет, что дистрибутивные решетки с дополнениями рассматривались братьями Бернулли задолго до Буля, Пирса и Шредера!

[158]'Отметим, что множество подмножеств пустого множества $\varnothing$, сводящееся к единственному подмножеству $\varnothing$, есть алгебра' – Н.Бурбаки, Интегрирование (Меры на локально компактных пространствах, продолжение меры, интегрирование мер, меры на отделимых пространствах). – Наука, М., 1977, с.1–600, стр.152.

определяются им в терминах характеристических функций! Вот и приходится бродить каждому самому по себе: не смогли придти к согласию даже авторы статей в 'Математической энциклопедии', которые в статьях 'алгебра множеств', 'борелевские множества', 'булева алгебра' и 'мера' пользуются для обозначения одного и того же понятия *четырьмя* разными терминами! Мне, однако, терминология, связанная с 'кольцами' и 'полями' множеств с операциями $\cap$ и $\cup$, представляется **злостным** анахронизмом. Хочется, все же, чтобы хотя бы относительно какой-то из этих операций 'кольцо' образовывало группу, а этого, как раз, ни в одном случае, кроме детально изученного Бурбаки кольца подмножеств пустого множества, не наблюдается.

Приведем пример алгебры множеств, отличной от 2^U.

Задача. Докажите, что $\bigwedge(U) \cup \mathrm{Cof}(U) \subseteq 2^U$ образует алгебру множеств.

§ 10. Симметрическая разность множеств

Сейчас мы введем еще одну операцию над множествами, которая позводит нам превратить 2^U в ассоциативное кольцо.

1. Симметрическая разность. Следующая операция, несмотря на то, что мы вводим ее последней, является самой важной среди всех теоретико-множественных операций.

Определение. Симметрической разностью *двух множеств A и B называется множество $A \triangle B$, состоящее из тех и только тех элементов, которые принадлежат ровно одному из множеств A или B,*

$$A \triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$

В старинных книгах суммой множеств часто называется объединение, но в действительности настоящим аналогом суммы чисел является именно симметрическая разность. Поэтому в дальнейшем мы будем, как правило, обозначать симметрическую разность через $+$ и называть **булевой суммой**, чтобы подчеркнуть ее аналогию с суммой **по модулю 2**.

• В основных графических пакетах имплементирована и операция $\triangle$ над плоскими фигурами. В частности, в `Adobe Illustrator` эта операция называется `Exclude`.

Задача. Убедитесь, что $X \triangle Y = (X \cup Y) \triangle (X \cap Y)$.

Задача. Пусть $X, Y \subseteq U$. Докажите, что $X \triangle Y = (X \cup Y) \cap (X' \cup Y')$.

2. Свойства симметрической разности. Симметрическая разность обладает еще более замечательными свойствами, чем пересечение и объединение.

G1 Ассоциативность $(X \triangle Y) \triangle Z = X \triangle (Y \triangle Z)$.

G2 Существование нейтрального элемента $A \triangle \varnothing = A = \varnothing \triangle A$.

G3 Существование симметричного элемента $A \triangle B = \varnothing = B \triangle A$.

G4 Коммутативность $X \triangle Y = Y \triangle X$.

В действительности свойство G3 можно усилить.

G5 Инволютивность $A \triangle A = \varnothing$.

В следующем параграфе на понадобится следующее свойство, устанавливающее дистрибутивность пересечения относительно симметрической разности

D Дистрибутивность $A \cap (B \triangle C) = (A \triangle B) \cap (A \triangle C)$.

Именно свойства G3 и G5 отличают симметрическую разность от остальных булевых операций. Подобно симметрической разности объединение имеет нейтральный элемент $\varnothing$, но ни для одного $A \neq \varnothing$ не существует множества B **симметричного** к A по отношению к объединению, т.е. такого, что $A \cup B = \varnothing$. Для симметрической же разности каждое множество симметрично себе. Часто, особенно в случае использования аддитивной записи $A + B = A \triangle B$ говорят, что каждое множество **противоположно** себе по отношению к булевой сумме. Докажем для примера свойство G1, доказательство остальных свойств проводится по той же схеме, но гораздо проще.

Доказательство ассоциативности $\triangle$. Условие на принадлежность x левой части состоит в том, что $((x \in A \ \& \ x \notin B) \vee (x \notin A \ \& \ x \in B) \ \& \ x \notin C) \vee (\neg((x \in A \ \& \ x \notin B) \vee (x \notin A \ \& \ x \in B)) \ \& \ x \in C)$. Используя формулы де Моргана, дистрибутивность связок $\&$ и $\vee$ и отбрасывая пустые слагаемые, легко убедиться, что это условие эквивалентно $((x \in A \ \& \ x \notin B) \vee (x \notin A \ \& \ x \in B) \ \& \ x \notin C) \vee (((x \in A \ \& \ x \in B) \vee (x \notin A \ \& \ x \notin B)) \ \& \ x \in C)$. Снова воспользовавшись дистрибутивностью, получаем окончательно следующее условие $(x \in A \ \& \ x \notin B \ \& \ x \notin C) \vee (x \notin A \ \& \ x \in B \ \& \ x \notin C) \vee (x \notin A \ \& \ x \notin B \ \& \ x \in C) \vee (x \in A \ \& \ x \in B \ \& \ x \in C)$. Таким образом, x принадлежит левой части в том и только том случае, когда он принадлежит либо ровно одному из множеств A, B, C, либо всем трем. Воспользовавшись коммутативностью $A \triangle (B \triangle C) = (B \triangle C) \triangle A$, мы видим, что таково же и условие принадлежности x правой части.

Если бы можно было говорить о множестве всех множеств, условия G1 – G4 означали бы, что булева сумма задает на нем структуру абелевой группы, а условие G5, что порядок любого $A \neq \varnothing$ равен двум. Однако, как мы знаем, ничего похожего на множество всех множеств не может существовать. Поэтому в дальнейшем мы будем применять булеву сумму к подмножествам некоторого фиксированного множества U, где она действительно будет задавать структуру абелевой группы периода 2 на булеане 2^U. Мы можем пользоваться всеми обычными свойствами групп. Например, существование противоположного элемента позволяет решать уравнения вида $A + X = B$. Прибавляя к обеим частям X, мы видим, что $A = A + \varnothing = A + (X + X) = (A + X) + X = B + X$. В силу той же причины для равенств с симметрической разностью возможно **сокращение**, т.е. из $A + C = B + C$ следует $A = B$ (достаточно прибавить к обеим частям C).

3. Симметрическая разность конечного семейства множеств. Подобно пересечению и объединению симметрическую разность можно определить для любого конечного семейства множеств при помощи формулы $X \triangle Y \triangle Z = (X \triangle Y) \triangle Z$.

Задача. Верно ли, что $A \triangle B \triangle C = (A \cup B \cup C) \setminus (A \cap B \cap C)$?

Ответ. "Это вряд ли". Левая часть состоит из тех x, которые принадлежат ровно одному или трем из множеств A, B, C, а правая часть - из тех x, которые принадлежат ровно одному или двум из этих множеств.

Если X_i – попарно непересекающиеся множества, то $\triangle X_i = \coprod X_i$.

Обозначим симметрическую разность $X \triangle \ldots \triangle X$ множества X с собой m раз, через mX. Ясно, что mX зависит лишь от четности m. Если m четно, то $mX = \varnothing$, а если m нечетно, то $mX = X$.

Задача. Пусть X – n-элементное множество. Вычислить $\triangle Y$, $Y \in \bigwedge^{n-1}(X)$.

Решение. Ясно, что

$$nX \triangle (\triangle_{Y \in \bigwedge^{n-1}(X)} Y) = \triangle_{Y \in \bigwedge^{n-1}(X)} (X \triangle Y) = \triangle_{x \in X} \{x\} = X.$$

Прибавляя к обеим частям равенства nX, получаем $\triangle Y = (n+1)X$.

Задача. Докажите, что для любых четырех множеств A, B, C, D имеет место включение

$$(A \setminus B) \triangle (C \setminus D) ?? (A \triangle C) \cup (B \triangle D).$$

В отличие от пересечения и объединения симметрическую разность нельзя определить для бесконечного семейства множеств.

Задача. Докажите, что

i) $(A \triangle B) \setminus C = (A \cup B) \triangle (A \cup C)$;

ii) $A \setminus (B \triangle C) = (A \setminus (B \cup C)) \cup (A \cap B \cap C)$;

4. Выражение булевых операций через две их них. В действительности, булевы операции можно выразить через 2 из них.

• **Выражение через $\cap$ и $\triangle$.** Докажите, что операции $\cup$ и $\setminus$ выражаются через операции $\cap$ и $\triangle$ следующим образом:

$$A \cup B = (A \triangle B) \triangle (A \cap B), \qquad A \setminus B = A \triangle (A \cap B).$$

• **Выражение через $\cup$ и $\triangle$.** Докажите, что операции $\cap$ и $\setminus$ выражаются через операции $\cup$ и $\triangle$. Так как $\setminus$ уже выражен через $\triangle$ и $\cap$, достаточно выразить $\cap$ через $\cup$ и $\triangle$. Такое выражение дается следующей формулой:

$$A \cap B = (A \cup B) \triangle (A \triangle B),$$

• На самом деле, чтобы определить структуру булевой алгебры на 2^U не нужно и двух операций. Определим операцию **бинарного отклонения** (известную также как **штрих Шеффера**) формулой $X|Y = X' \cap Y'$. Тогда все операции выражаются в терминах этой одной операции:

$$X' = X|X, \qquad X \cap Y = (X|X)|(Y|Y), \qquad X \cup Y = (X|Y)|(X|Y).$$

§ 11. Булевы кольца

Теория решеток представляет собой *учение*, в значительной степени параллельное теориям других алгебраических структур, таких как группы или кольца. В то же время, теория булевых алгебр обычно не рассматривается как самостоятельная алгебраическая теория[159]. Дело в том, что в 1935 году Стоун заметил, что изучение булевых алгебр может быть включено как *очень* специальная глава в теорию ассоциативных колец[160]. В настоящем параграфе мы изложим основные моменты этой конструкции, оставляя читателю (тривиальные) проверки технических утверждений.

[159]Речь здесь идет о булевых алгебрах с *конечными* операциями. Когда говорят о *теории* булевых алгебр, имеют в виду булевы алгебры в которых существуют те или иные классы *бесконечных* пересечений и объединений [Vla], [RS], [Sik].

[160]M.H.Stone, The theory of representations for Boolean algebras. – Trans Amer. Math. Soc., 1936, vol.40, p.37–111.

Определение. *Ассоциативное кольцо A с 1 называется* **булевым**, *если все его элементы идемпотентны, т.е. $x^2 = x$ для всех $x \in A$.*

Сейчас мы покажем, что в любом булевом кольце выполняются тождества $2x = 0$ (характеристика 2) и $xy = yx$ (коммутативность).

Теорема. *Булево кольцо является коммутативным кольцом характеристики 2.*

Доказательство. Равенство $x^2 = x$ влечет

$$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y,$$

поэтому $xy + yx = 0$. Полагая здесь $y = 1$ (или $y = x$), мы получим $2x = 0$. Тем самым, равенство $xy + yx = 0$ можно переписать в виде $xy = yx$.

Теорема Стоуна. *Пусть A – булева алгебра с операциями $\cap$, $\cup$, $'$. Определим на ней умножение как $XY = X \cap Y$, а сложение формулой*

$$X + Y = (X \cap Y') \cup (X' \cap Y) = (X \cup Y) \cap (X' \cup Y').$$

Эти операции превращают алгебру A в булево кольцо.

Обратно, если R – булево кольцо с операциями $+$ и $\cdot$ и единицей 1, то полагая $X \cap Y = XY$, $X \cup Y = X + Y + XY$ и $X' = 1 - X$, мы определим на R структуру булевой алгебры.

Начнем с доказательства того, что булево кольцо является булевой алгеброй. Для этого введем на булевом кольце A порядок, полагая $X \leq Y \iff XY = X$. Проверьте, что 1) $0 \leq X \leq 1$, 2) $X \leq X$, 3) если $X \leq Y$, и $Y \leq X$, то $X = Y$, 4) если $X \leq Y$ и $Y \leq Z$, то $X \leq Z$. Таким образом, A превращается в частично упорядоченное множество с наименьшим и наибольшим элементами.

Проверьте, что относительно введенного порядка 5) $\inf(X, Y) = XY$ и 6) $\sup(X, Y) = X + Y + XY$, 7) отображение $X \mapsto X' = 1 - X$ является антиавтоморфизмом порядка $\leq$, причем 8) $X \cap X' = 0$, $X \cup X' = 1$. Все свойства булевых операций, кроме быть может, дистрибутивности 9) $X \cap (Y \cap Z) = (X \cap Y) \cup (X \cap Z)$ теперь очевидны.

Для доказательства теоремы в другую сторону проверьте, что определив сложение приведенной в теореме формулой, мы получаем 1) $0 + X = X$, 2) $X + X = 0$, 3) $X + Y = Y + X$. Труднее всего проверить ассоциативность сложения. Для этого нужно заметить, что 4) обе суммы $(X+Y)+Z$ и $X+(Y+Z)$ равны

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

Свойства умножения очевидны, так как они совпадают с соответствующими свойствами пересечения, а для проверки дистрибутивности достаточно проверить, что 5) оба выражения $X(Y+Z)$ и $XY+XZ$ равны $(X \cap Y \cap Z') \cup (Y' \cap X \cap Z)$.

§ 12. Пересечение и объединение произвольных семейств

Специфика операций пересечения и объединения состоит в том, что они могут быть определены для произвольных семейств множеств.

1. Объединения и пересечения семейств множеств. Следующие определения естественно обобщают определения конечных пересечений и объединений.

Определение. *Если Ω – любое множество множеств, то* **пересечением** *его элементов называется множество $\bigcap X$, $X \in \Omega$, состоящее из тех и только тех элементов, которые принадлежат каждому множеству $X \in \Omega$.*

Таким образом, согласно этому определению для любого множества множеств Ω имеем

$$x \in \bigcap_{X\in\Omega} X \quad \Longleftrightarrow \quad \forall X \in \Omega,\ x \in X.$$

Определение объединения совершенно аналогично.

Определение. *Если Ω – любое множество множеств, то* **объединением** *его элементов называется множество $\bigcup X$, $X \in \Omega$, состоящее из тех и только тех элементов, которые принадлежат по крайней мере одному из множеств $X \in \Omega$.*

Согласно этому определению для любого множества множеств X имеем

$$x \in \bigcup_{X\in\Omega} X \quad \Longleftrightarrow \quad \exists X \in \Omega,\ x \in X.$$

Существование произвольных пересечений сразу вытекает из аксиомы подмножеств **ZF6′**. В то же время, существование объединений не вытекает из остальных аксиом и должно постулироваться отдельно, что мы и сделали в аксиоме объединения **ZF4**.

Часто говорят о пересечении или объединении **семейства** множеств. Например, если $X = (X_i)_{i\in I}$ – такое семейство, то пересечение и объединение всех X_i из этого семейства обычно обозначается через $\bigcup X_i$, $i \in I$, и $\bigcap X_i$, $i \in I$, соответственно.

2. Свойства бесконечных объединений и пересечений. Объединения и пересечения семейств идеально согласованы с *объединением* индексных множеств:

$$\bigcap_{i\in I\cup J} X_i = \bigcap_{i\in I} X_i \cap \bigcap_{i\in J} X_i, \qquad \bigcup_{i\in I\cup J} X_i = \bigcup_{i\in I} X_i \cup \bigcup_{i\in J} X_i,$$

Эти тождества являются частными случаем **общего тождества ассоциативности**. В самом общем виде ассоциативность выглядит следуюшим образом

$$\bigcup_{i\in\bigcup_{j\in J} I_i} X_i = \bigcup_{j\in J}\bigcup_{i\in I_j} X_i, \qquad \bigcap_{i\in\bigcup_{j\in J} I_i} X_i = \bigcap_{j\in J}\bigcap_{i\in I_j} X_i,$$

В то же время, поведение этих операций по отношению к *пересечению* индексных множеств несколько сложнее, в этом случае можно утверждать лишь, что

$$\bigcap_{i\in I\cap J} X_i \supseteq \bigcap_{i\in I} X_i \cup \bigcap_{i\in J} X_i, \qquad \bigcup_{i\in I\cap J} X_i \subseteq \bigcup_{i\in I} X_i \cap \bigcup_{i\in J} X_i,$$

В действительности, правильным аналогом являются **тождества дистрибутивности**:

$$\bigcup_{i\in I} X_i \cap \bigcup_{j\in J} Y_j = \bigcup_{(i,j)\in I\times J} (X_i \cap Y_j), \qquad \bigcap_{i\in I} X_i \cup \bigcap_{j\in J} Y_j = \bigcap_{(i,j)\in I\times J} (X_i \cup Y_j).$$

Наконец, для бесконечных объединений и пересечений имеют место аналоги **тождеств де Моргана**:

$$X \setminus \bigcap_{i\in I} Y_i = \bigcup_{i\in I} (X \setminus Y_i), \qquad X \setminus \bigcup_{i\in I} Y_i = \bigcap_{i\in I} (X \setminus Y_i),$$

§ 13. Непересекающиеся множества, дизъюнктное объединение

1. Дизъюнктное объединение. В конкретных ситуациях очень часто возникает объединение попарно непересекающихся множеств и нам будет удобно ввести для него специальное обозначение.

Определение. *Говорят, что множества X и Y* **не пересекаются** (*alias,* **дизъюнктны**)*, если $X \cap Y = \varnothing$. В противном случае говорят, что они* **пересекаются** *или, если нужна особая точность, что они имеют* **нетривиальное пересечение**.

Вообще, пусть Ω – любое множество множеств. Говорят, что элементы Ω **не пересекаются** (или, если нужна особая точность, **не пересекаются в совокупности**), если $\bigcap X = \varnothing$, где пересечение берется по всем $X \in \Omega$. Говорят, что элементы W **попарно не пересекаются** (alias, **попарно дизъюнктны**), если любые два **различных** элемента $X, Y \in \Omega$ не пересекаются, т.е. если из того, что $X, Y \in \Omega$, $X \neq Y$, следует, что $X \cap Y = \varnothing$.

Возьмем три попарно различных вещи x, y, z и рассмотрим множество $U = \{X, Y, Z\}$, где $X = \{y, z\}$, $Y = \{x, z\}$ и $Z = \{x, y\}$. Тогда элементы U не пересекаются в совокупности, но любые два из них имеют нетривиальное пересечение.

Задача. Докажите, что если X и Y дизъюнктны, $U \subseteq X$, $V \subseteq Y$, то U и V тоже (*'тем более'*) дизъюнктны.

В случае, когда X и Y дизъюнктны, мы будем использовать для объединения $X \cup Y$ запись $X \sqcup Y$ и называть его **дизъюнктным объединением**. Таким образом, $U = X \sqcup Y$ по определению означает, что $U = X \cup Y$ и $X \cap Y = \varnothing$. Это определение распространяется на любое количество объединяемых множеств. Так, запись $U = X \sqcup Y \sqcup Z$ означает, что $U = X \cup Y \cup Z$, причем $X \cap Y, X \cap Z, Y \cap Z = \varnothing$. Вообще, если Ω – любое множество попарно не пересечкающихся множеств, мы будем использовать для $\bigcup X$, $X \in \Omega$, запись $\coprod X$, $X \in \Omega$.

В следующей главе мы придадим смысл выражению $X \sqcup Y$ и для общего случая, когда множества X и Y пересекаются. В этом случае $X \sqcup Y$ будет называться *копроизведением* множеств X и Y. Однако для случая дизъюнктных множеств этот новый смысл будет согласован только что описанным.

2. Бетховен и морские свинки. В XIX веке логики любили маскировать условия типа дизъюнктности двойными отрицаниями ("Hobbits delighted in such things"). Вот пример развлекательной задачи на эту тему из книги Льюиса Кэррола "Symbolic logic" (как пишет по этому поводу Келли, "из Льюиса Кэррола, с приветом Шредеру").

Задача. Рассмотрим следующие три высказывания:

(1) Nobody, who really appreciates Beethoven fails to keep silence while the Moonlight Sonata is being played.

(2) Guinea pigs are hopelessly ignorant of music.

(3) No one who is hopelessly ignorant of music ever keeps silence while the Moonlight Sonata is being played.

Верно ли, что из этих высказываний вытекает следующее:

(4) Guinea pigs do not really appreciate Beethoven.

Решение. См. предыдущую задачу.

§ 14. Алгебры и топологии

В действительности, во многих разделах математики принято рассматривать решетки и булевы алгебры, в которых существуют различные классы **бесконечных** пересечений и объединений.

1. Полные решетки. Вернемся к определению решетки. В § 4 мы объяснили, что решетку можно воспринимать как такое частично упорядоченное множество, в котором существуют супремум и инфимум любых двух элементов и, тем самым, любого конечного подмножества. Решетка называется **полной**, если в ней существуют супремум и инфимум *любого* подмножества. В этом случае $\inf\Omega$ обычно интерепретируется как бесконечное пересечение $\bigcap X$, $X\in\Omega$. Аналогично, $\sup\Omega$ интерпретируется как бесконечное объединение $\bigcup X$, $X\in\Omega$.

Задача. Пусть L – решетка с 0 и 1. Если в L существуют объединения произвольных семейств, то в L существуют и пересечения произвольных семейств, и наоборот.

Решение. В самом деле, пусть, например, в L существуют бесконечные объединения. Рассмотрим произвольное множество $\Omega\subseteq L$. Множество Θ его нижних граней содержит 0 и, значит, непусто. Пусть $Y=\bigcup X$, $X\in\Theta$. Тогда $Y=\inf(\Omega)$

2. σ-алгебры. Часто условие существования *произвольных* бесконечных пересечений и объединений является чересчур сильным. Пусть $\beth$ – какой-то бесконечный кардинал. Говорят, что решетка L является **$\beth$-полной**, если в ней существуют супремум и инфимум любого подмножества Ω такого, что $|\Omega|\leq\beth$. В случае, когда $\beth=\aleph_0$ аналисты обычно называют $\aleph_0$-полные решетки **σ-полными** или просто **σ-решетками**.

В случае, когда $\beth$-полная решетка $L=A$, *кроме того*, является булевой алгеброй, т.е. замкнута относительно перехода к *дополнению*, ее обычно называют **$\beth$-полной** булевой алгеброй. При этом $\aleph_0$-полные булевы алгебры обычно называются просто **σ-алгебрами**. Иными словами, σ-алгебра Ω подмножеств в U удовлетворяет следующим четырем аксиомам:

Σ1 T замкнуто относительно **счетных** пересечений: $V_i\in\Omega\Longrightarrow\bigcup V_i\in\Omega$;

Σ2 T замкнуто относительно **счетных** объединений: $V_i\in\Omega\Longrightarrow\bigcup V_i\in\Omega$;

Σ3 $\varnothing, U\in\Omega$;

Σ4 Ω замкнуто относительно дополнений: $X\in\Omega$, то $U\setminus X\in\Omega$.

Из формул де Моргана вытекает, что достаточно требовать только существования счетных пересечений **или** объединений. Некоторые авторы называют σ-алгебры **σ-кольцами**.

Понятие σ-алгебры является основным в теории меры. А именно, пусть Ω есть некоторая σ-подмножеств в U. **Мерой** μ, определенной на Ω, называется отображение $\Omega\longrightarrow\mathbb{R}_+$, такое, что $\mu(\varnothing)=0$, обладающее свойством **счетной аддитивности**:

$$\mu(\coprod X_i)=\sum\mu(X_i),$$

где объединение и сумма берутся по произвольному *счетному* семейству X_i *попарно дизъюнктных* множеств $X_i\in\Omega$. $i\in\mathbb{N}$.

3. Топология. Структура топологического пространства является одной из основных в математике. Ее можно задавать многими различными (но эквивалентными между собой) способами. Обычный способ, приводящий к наиболее элегантным определениям, состоит в выделении на U топологии.

Определение. *Подмножество $T\subseteq 2^U$ называется* **топологией** *на множестве U, если оно удовлетворяет следующим трем аксиомам:*

O1 *T замкнуто относительно* **произвольных** *объединений: $V_\alpha\in T\Longrightarrow\bigcup V_\alpha\in T$;*

O2 *T замкнуто относительно* **конечных** *пересечений: $V,W\in T\Longrightarrow V\cap W\in T$;*

O3 $\varnothing, U\in T$.

Множество U вместе с заданной на нем топологией называется **топологическим пространством**. При этом элементы $A\in T$, рассматриваемые как подмножества в U, называются **открытыми** множествами, а их дополнения в U – **замкнутыми** множествами.

• Среди всех топологий на X существует самая сильная топология $T=2^U$, называемая **дискретной**, в которой **все** подмножества U открыты и самая слабая топология $T=\{\varnothing,U\}$,

называемая **тривиальной**, единственными открытыми множествами в которой являются $\varnothing$ и само U.

• Топология на конечном множестве U это то же самое, что подрешетка с 0 и 1 в решетке множеств 2^U.

• Пусть теперь U – бесконечное множество, а $T = \mathrm{Cof}(U)$ множество всех ко-конечных подмножеств в U. Эта топология называется **коконечной**.

В действительности, алгебраисты обычно задают топологию двойственным образом, посредством задания системы **замкнутых** множеств.

Определение. *Подмножество $T \subseteq 2^X$ называется* **топологией** *на множестве X, если оно удовлетворяет следующим трем аксиомам:*

Z1 *T замкнуто относительно* **произвольных** *пересечений: $Z_\alpha \in T \Rightarrow \bigcap Z_\alpha \in T$;*

Z2 *T замкнуто относительно* **конечных** *объединений: $Y, Z \in T \Rightarrow Y \cup Z \in T$;*

Z3 *$\varnothing, X \in T$.*

Независимо от того, как мы определяем топологию, как алгебраисты, или как все остальное человечество, мы должны быть в состоянии заметить разницу между определением топологии и σ-алгебры. В σ-алгебре существуют как счетные пересечения, так и счетные объединения (поскольку она замкнута относительно дополнений!), с другой стороны в топологии, существуют *произвольные* объединения (или пересечения!) и *конечные* пересечения (или объединения!). Feel the difference!

4. Catch 666. Теперь читатель может проверить, понял ли он что-нибудь из прочитанного в этом параграфе.

Коан. Рассмотрим топологию $T \subseteq 2^U$. По определению в T существуют объединения произвольных семейств элементов. Как мы только что доказали, тогда там существуют и пересечения произвольных семейств. В хаусдорфовом пространстве (скажем в $\mathbb{R}$ с обычной топологией) пересечение всех окрестностей точки совпадает с этой точкой. Значит любая точка там открыта, так что на $\mathbb{R}$ нет никаких хаусдорфовых топологий, кроме дискретной.

Ответ для знатока. 'Прошу не читать помещенного далее решения для учащегося!'[161]

Решение для учащегося. Было бы *слишком* жестоко оставлять начинающего, который все же решил (вопреки явному запрету!) читать текст, набранный мелким шрифтом (и ненароком долетел до этого места) в таком положении. Поэтому я все же (хотя это и не в моих правилах: 'спасение начинающих – дело самих начинающих'[162]) поясню, в чем здесь дело. Действительно, решетка открытых множеств полна и является подрешеткой в 2^U. Это значит, что *конечные* пересечения и объединения в этой решетке совпадают с теоретико-множественными пересечениями и объединениями. Так как, кроме того, бесконечное объединение открытых множеств совпадает с их теоретико-множественным объединением, то топология представляет собой полную решетку. Тем самым, действительно, в топологии существуют произвольные бесконечные пересечения. Только вот ниоткуда не следует, что бесконечные пересечения открытых множеств в топологии, рассматриваемой как решетка, совпадают с теоретико-множественными пересечениями! В действительности, пересечением бесконечного семейства множеств в топологии является *внутренность* их теоретико-множественного пересечения. Это не должно вызывать удивления, ведь даже для конечноместных операций подобная ситуация нередка. Скажем, решетка подпростанств векторного пространства V является подрешеткой в множестве всех подмножеств этого пространства относительно *того же* порядка. Кроме того, пересечение подпространств совпадает с их теоретико-множественным пересечением. Но вот для объединения это уже совсем не так. Объединением подпространств *в решетке подпространств* является их *прямая сумма*. Что уж говорить о *бесконечноместных* операциях, где речь идет о продолжении конечноместных операций по непрерывности! Ясно, что результат такой операции просто *обязан* зависеть от способа продолжения!

---

[161] Э.Ландау, Основы анализа. т.I. – ИЛ, М., 1947, с.1–182, стр.7.

[162] 'Fabian ertrank. Er konnte leider nicht schwimmen.' – E.Kästner, Fabian, die Geschichte eines Moralisten. Kap.24.

Глава 3. Произведения и копроизведения

> Более всего он любил прямолинейный проспект; этот проспект напоминал ему о течении времени между двух жизненных точек; и еще об одном: иные все города представляют собой деревянную кучу домишек, и разительно от них всех отличается Петербург. Есть бесконечность в бесконечность бегущих проспектов с бесконечностью в бесконечность бегущих пересекающихся теней. Весь Петербург — бесконечность проспекта, возведенного в n-ю степень. За Петербургом же – ничего.
>
> Андрей Белый, Петербург, Глава I

Здесь мы напоминаем определения и основные свойства *теоретико-категорных* операций над множествами, таких как прямое произведение и копроизведение. Эти операции принципиально отличаются от рассмотренных в предыдущей главе булевых операций тем, что они определены не *на самом деле*, на уровне элементов, а лишь с точностью до *канонического изоморфизма*. Непонимание этого принципиального момента приводит всех авторов, стоящих на 'наивных' позициях, к грубейшим ошибкам.

Наиболее важная с точки зрения алгебраиста операция над множествами – это образование **прямого** или **декартова**[163] **произведения**. Эта конструкция является очень широким обобщением понятия системы координат с одной стороны и понятия множества X^I всех отображений из I в X с другой. Поскольку эта конструкция играет столь важную роль в дальнейшем, в этой главе мы детально и с большим количеством примеров изучаем прямые произведения двух множеств, конечного числа множеств и, наконец, произвольных семейств множеств. Кроме того, мы обсуждаем двойственную конструкцию копроизведения, а также несколько других конструкций, являющихся обобщениями или вариантами прямого произведения.

§ 1. Упорядоченные пары

> If it were not possible to represent ordered pairs in set theory, set theory would be of virtually no mathematical interest at all.
>
> Jon Barwise & Larry Moss[164]

> Содержит ли пара единицу? — Пара не содержит единицы. — Содержит ли пара правое? — Пара не содержит правого. — Содержит ли

[163] **Рене Декарт** (31.03.1596, La Haye (сегодня Descartes), Touraine – 11.02.1650, Стокгольм) – замечательный математик и мыслитель. С 1618 года он принял участие в нескольких военных походах в различных странах Европы, а с 1628 года осел в Нидерландах. В 1637 году вышла его главная книга 'Геометрия', где он связал геометрию с алгеброй и, тем самым, заложил основы алгебраической геометрии. Он сформулировал много теорем, касающихся алгебраических уравнений, которые были доказаны только много позже. Декарт был одним из прекурсоров дифференциального и интегрального исчисления, большое влияние на развитие которого оказали произведенные им вычисления длин кривых, площадей ограниченных ими фигур, уравнений касательных и т.д. Другие математические работы Декарта относятся к теории чисел. В нашем курсе встречаются декартовы координаты, декартовы произведения, теоремы Декарта и т.д. В других (кон)текстах встречаются также Декартов лист, овал Декарта, Декартовы квадраты, и т.д. С детства Декарт привык оставаться в кровати до 11 утра и предаваться размышлениям. В 1649 году королева Кристина убедила Декарта перебраться в Стокгольм. Однако она хотела заниматься с ним геометрией в 5 утра. Как известно, будить математика – преступление, поэтому через несколько месяцев такой жизни Декарт умер от пневмонии.

[164] J.Barwise, L.Moss, Hypersets – Math. Intelligencer, 1991, vol.13, N.1, p.31-41.

> пара левое? — Пара не содержит левого. — Можно ли дать правому название ‘пара’? — Нельзя. — Можно ли дать левому название ‘пара’? — Нельзя. — Когда левое соединяется с правым, можно ли этому дать название ‘пара’? — Можно. — Можно ли изменяющееся назвать ‘неизменяющимся’? — Можно. — Когда к правому имеется присоединение, можно ли дать название ‘изменяющееся’? — Можно. – Что же изменяется? — правое. — Но если правое изменяется, то как же можно назвать его ‘правым’? А если не изменяется, то как можно давать название ‘неизменяющегося’? Если пара не содержит ни левого, ни правого, то как же получается пара от соединения левого и правого?
>
> Гуньсун Лун-цзы, Гл. 3: О проникновении в изменения

Обычная в учебной литературе (‘наивная’) конструкция прямого произведения основана на понятии упорядоченной пары.

1. Упорядоченные пары. Наряду с неупорядоченными в математике очень часто применяются также **упорядоченные пары**. Упорядоченная пара, состоящая из **вещей** x и y, не обязательно различных, обозначается обычно через (x, y). При этом по причинам, которые вскоре станут понятны, x и y обычно называются не элементами, а **компонентами** или **координатами** упорядоченной пары (x, y). Некоторые авторы тем не менее называют x ‘первым элементом’ упорядоченной пары, а y – ее ‘вторым элементом’, но это с необходимостью приводит к высказываниям в духе Мо Ди и Гуньсун Луна: “первый элемент упорядоченной пары не является ее элементом” (“белая лошадь не является лошадью”).

Характеристическим свойством упорядоченных пар является то, что две упорядоченных пары равны если и только если равны их соответствующие компоненты, т.е. $(x, y) = (u, v)$ в том и только том случае, когда $x = u$ и $y = v$. В отличие от неупорядоченных пар, упорядоченные пары (x, y) и (y, x) различны, если $x \neq y$, и можно говорить об упорядоченной паре (x, x) с равными компонентами. Некоторые авторы обозначают упорядоченную пару (x, y) через $\langle x, y\rangle$, но в алгебре $\langle x, y\rangle$ обычно понимается иначе!

2. Почему философы не смогли определить упорядоченную пару? Начнем со случая прямого произведения двух множеств $X \times Y$. Прежде всего мы покажем, что аксиома **ZF3** позволяет ввести также упорядоченные пары. Это не совсем очевидно и возникшую здесь проблему очень живописно описывает Ян Стюарт[165]: “Трудность состояла здесь в том, чтобы избежать ссылок на способ изображения такой пары в виде (a, b). Нельзя говорить “a – левый элемент”, потому что “левый” не является понятием теории множеств. Ранние философы совершенно запутались в этом вопросе (см. [Russell]). “Является ли упорядочение свойством a?” Нет, оно зависит также и от b ибо, скажем, пары $(1, 2)$ и $(3, 1)$ различны. “Является ли оно свойством a?” Нет, по той же причине. “Тогда это свойство a и b?” Тоже нет, потому что a и b не отличается от b и a, и тогда получается, что (a, b) и (b, a) – одно и то же. Требуется как-то избавиться от симметрии между a и b. Философы оказались здесь бессильны, потому что не понимали разницы между x и $\{x\}$. Они не хотели различать эти вещи. Однако стоит только осознать эту разницу, как открывается целый ряд разнообразных путей решения задачи.”.

3. Представление упорядоченных пар в теории множеств. *Единственное* свойство упорядоченных пар, которое будет нас интересовать, выражается следующей аксиомой.

---

[165] Я.Стюарт, Концепции современной математики – Вышейшая школа, Минск, 1980, с.1–382. см. с.372.

ОР (Аксиома упорядоченных пар). *Равенство двух упорядоченных пар* $(x, y) = (u, v)$ *имеет место тогда и только тогда, когда* $x = u$ *и* $y = v$.

При этом x называется **первой компонентой**, а y – **второй компонентой** упорядоченной пары (x, y).

Можно ли промоделировать понятие упорядоченной пары в ортодоксальной теории множеств? Логики и философы начала XX века высказывали самые причудливые мнения по этому вопросу. Следующее определение упорядоченных пар называется определением Винера[166]–Куратовского.

Определение. Упорядоченной парой (x, y) *с первой компонентой* x *и второй компонентой* y*, называется множество* $(x, y) = \{\{x\}, \{x, y\}\}$.

Иногда, чтобы подчеркнуть, что используется именно это определение упорядоченной пары, говорят, что (x, y) упорядоченная пара x и y **по Куратовскому**[167]. В этом определении симметрия между x и y нарушается несколько больше, чем в записи (x, y), поэтому многие математики не считают его вполне убедительным и рассматривают понятие упорядоченной пары как **первичное**. Кроме того, отождествление пары (x, x) с множеством $\{\{x\}\}$ в определении Куратовского выглядит довольно странным – что такое тогда упорядоченная единица (x)?. Однако, как бы то ни было, сейчас мы убедимся, что это определение работает. После этого можно стандартным образом определить упорядоченные n-ки, декартовы произведения конечного числа множеств, отношения, отображения и пр.

Лемма. *Упорядоченная пара по Куратовскому удовлетворяет ОР.*

Доказательство. Пусть вначале $x = y$. Тогда $\{x\} = \{u\} = \{u, v\}$. Из первого равенства следует, что $x = u$ и теперь из второго равенства следует, что и $v = x$. Пусть теперь $x \neq y$. Тогда $\{x\}$ является одним из элементов $\{\{u\}, \{u, v\}\}$, но случай $\{x\} = \{u, v\}$ исключен, потому что это равенство влечет $x = u = v$ и тогда $\{u\} = \{u, v\}$ и, значит, $\{x, y\} = \{u\}$, так что $x = y = u$, вопреки предположению, что $x \neq y$. Это значит, что $\{x\} = \{u\}$ и, тем самым, $x = u$. С другой стороны, в этом случае $\{x, y\}$ обязано совпадать с $\{u\}$ или с $\{u, v\}$. Однако если $\{x, y\} = \{u\}$, то точно такое же рассуждение, как выше, показывает, что $x = y = u$, вопреки предположению. Это значит, что $\{x, y\} = \{u, v\}$ и, значит, $y = u$ или $y = v$. Случай $y = u = x$ исключен, поэтому, окончательно, $y = v$.

Впрочем, специальный вид множества $\{\{x\}, \{x, y\}\}$ в определении упорядоченной пары (x, y) не играет абсолютно никакой роли, мы могли бы определять ее как $\{\{y\}, \{x, y\}\}$ и множеством других образов. Возникает искушение определить упорядоченную пару (x, y) без затей, как $\{\{1, x\}, \{2, y\}\}$. Однако если x и/или y равны 1 и/или 2, здесь могут возникнуть трудности. Поскольку в большинстве конкретных задач приходится рассматривать лишь

---

[166]**Норберт Винер** (26.11.1894, Колумбия, Миссури – 19.03, Стокгольм) – знаменитый американский математик, основатель кибернетики. Сын Лео Винера (1862–1939), известного польского филолога. Семья Винеров происходит от выдающегося еврейского мыслителя Моисея Маймонида (1135–1204). Математический талант Винера проявился в очень раннем возрасте, уже в 18 лет он получил Ph.D. в MIT за работы по математической логике. Основные математические работы Винера относятся к гармоническому анализу и теории случайных процессов (тауберовы теоремы). Он интересовался и приложениями к физике (брауново движение, теория потенциала и т.д.). В 1948 году была опубликована его книга 'Cybernetics, or control and communication in the animal and the machine', которая стала культовой и дала название новой науке. На русский язык переведены его книги 'Преобразование Фурье в комплексной области' (совместная с Р.Пэли), 'Кибернетика' и автобиографические 'Бывший вундеркинд' и 'Я – математик'. Трудно резюмировать стиль Винера лучше, чем это сделал он сам: 'Каждый творчески работающий ученый волен ломать *любые* перегородки, если это нужно для успеха его работы'.

[167]**Казимеж Куратовский** (02.02.1896, Варшава – 1980) – польский математик, ученик Вацлава Серпиньского, основные работы которого относятся к теории множеств и топологии. С 1927 года профессор Львовского, а с 1934 – Варшавского университета. В 1948 стал первым директором основанного тогда Математического Института PAN. На русский язык переведен его двухтомник 'Топология' и 'Теория множеств' совм. с К.Мостовским.

пары (x, y), где x и y пробегают конкретные множества, то можно определить (x, y) как $\{\{©, x\}, \{¥, y\}\}$, где © и ¥ суть две **потусторонние** вещи, отличные от всех остальных вещей, с которыми нам в данный момент приходится иметь дело (существование потусторонних вещей следует из аксиомы подстановки **ZF6**).

Задача. Допустим, что упорядоченная пара (x, y) определяется как $(x, y) = \{\{©, x\}, \{¥, y\}\}$, где © и ¥ – две различные потусторонние вещи. Доказать, что так определенные упорядоченные пары удовлетворяет OP.

Привет Кудрявцеву. Интересно отметить, что (в отсутствие аксиомы **ZF9**) мы *не могли бы* определить упорядоченную пару (x, y) как $\{x, \{x, y\}\}$, так как могло бы оказаться, что $\{x, y\} \in x$. В качестве курьеза укажем, что именно так определяется упорядоченная пара в "Математической энциклопедии", т.V, с.713. При этом, уже совершенно анекдотическим образом, упорядоченная пара (a, b) определяется там только для *пары* $\{a, b\}$, так что автоматически $a \neq b$!

§ 2. Прямые произведения множеств: наивное определение

> Слово 'лошадь' обозначает форму, слово 'белый' обозначает цвет. То, что обозначает цвет, не есть то, что обозначает форму, Поэтому я утверждаю, что белая лошадь не есть лошадь.
>
> Гуньсун Лун-цзы, Гл. 2: Рассуждение о белой лошади

Мы начнем с наивного определения прямого произведения, которое в дальнейшем будет уточнено.

1. Прямое произведение двух множеств. Пусть вначале A и B – два множества.

Наивное определение. *Прямым произведением $A \times B$ множеств A и B называется множество*

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

всех упорядоченных пар, первый член которых принадлежит A, а второй – B.

Особенно важен для нас случай, когда $A = B$. Множество $A \times A = A^2$ называется **декартовым квадратом** множества A.

2. Существование прямого произведения. Разумеется, тот факт, что все пары (a, b) могут быть собраны в множество, совершенно не является самоочевидным и должен либо специально постулироваться, либо выводиться из остальных аксиом. Покажем, что если (a, b) определяется по Куратовскому, то существование $A \times B$ может быть выведено из аксиомы объединения, аксиомы степени и аксиомы подмножеств. В самом деле, элементы пары $\{\{a\}, \{a, b\}\}$ принадлежат множеству $2^{A \cup B}$ и, тем самым, все такие пары принадлежат множеству $2^{2^{A \cup B}}$, существование которого гарантируется аксиомами объединения и степени. Теперь $A \times B$ может быть определено как

$$A \times B = \left\{ X \in 2^{2^{A \cup B}} \mid X = \{\{a\}, \{a, b\}\},\ a \in A,\ b \in B \right\},$$

причем это множество существует в силу аксиомы подмножеств.

Заметим, что это доказательство весьма неконструктивно, потому что, оно апеллирует к выделению подмножеств из *чудовищно* большого множества $2^{2^{A \cup B}}$. Например, если множества A и B счетны, то множество $2^{2^{A \cup B}}$ имеет мощность, строго большую мощности континуума (см. § ?). В действительности на обоих шагах достаточно использовать лишь значительно более слабое утверждение, а именно, существование не самого булеана 2^X, а лишь его крошечной части $\bigwedge(X)$ – множества всех *конечных* подмножеств множества X.

3. Правило произведения. Если множества A и B конечны, причем A содержит m элементов, а B содержит n элементов, то множество $A \times B$ тоже конечно и содержит mn элементов. Вообще, для любых двух множеств A и B мощность их прямого произведения $A \times B$ равна **произведению** мощностей множеств A и B, $|A \times B| = |A||B|$, где через $|X|$ обозначена мощность множества X (см. § ?). В частности, декартово произведение непустых сомножителей непусто. Для двух сомножителей (но, разумеется, не в общем случае!) этот факт можно доказать *без использования* аксиомы выбора.

Например, если $\{0, 1, 2\}$ – трехэлементное множество, а $\{x, y\}$ – двухэлементное множество, то их прямое произведение

$$\{0, 1, 2\} \times \{x, y\} = \{(0, x), (0, y), (1, x), (1, y), (2, x), (2, y)\}$$

содержит $3 \cdot 2 = 6$ элементов.

4. Первые примеры. Вот несколько очевидных примеров прямых произведений двух множеств.

• **Декартовы координаты.** Наиболее знакомый частный случай декартова произведения – по аналогии с которым Куратовский и дал название общему случаю – это декартовы координаты на плоскости. При этом каждой точке плоскости сопоставляются ее проекции на две координатные оси, называемые *осью абсцисс* и *осью ординат*, соответственно. В свою очередь точка z плоскости однозначно определяется своими проекциями x и y на эти оси, называемыми в школьном курсе ее *абсциссой* и *ординатой*. Впрочем, профессиональные математики обычно используют менее вычурные названия x и y и говорят просто о *первой координате* и *второй координате* точки z. Таким образом, точка z плоскости может быть *отождествлена* с парой своих координат (x, y). При этом плоскость (вместе с проекциями на координатные оси!) отождествится с прямым произведением координатных осей, т.е. двух экземпляров $\mathbb{R}$. Таким образом, эвклидову плоскость можно рассматривать как декартов квадрат вещественной оси. Это оправдывает обычное обозначение эвклидовой плоскости через $\mathbb{R}^2$.

• **Полярные координаты.** Рассмотрим плоскость, из которой удалено начало координат 0. Каждой точке z плоскости сопоставляется ее *модуль* r, являющийся (эвклидовым) расстоянием между z и 0. Если $z = (x, y)$, то $r = \sqrt{x^2 + y^2}$. Ясно, что модуль точки $z \neq 0$ является положительным вещественным числом, т.е. элементом $\mathbb{R}_+$. С другой стороны, если $z \neq 0$, то существует единственный луч исходящий из начала координат 0 и проходящий через точку z. Таким образом, каждой точке $z \neq 0$ можно сопоставить ее *аргумент*, т.е. точку w пересечения этого луча с единичной окружностью с центром в начале координат. В предшествующих обозначениях $\phi = (x/r, y/r)$ (именно здесь используется, что $z \neq 0$ или, что то же самое, что $r \neq 0$). Легко видеть, что и обратно любая точка $z \neq 0$ однозначно определяется парой (r, ϕ). Запись точки $z \neq 0$ в виде $z = (r, \phi)$ называется ее записью в *полярных координатах*. Она теснейшим образом связана с *тригонометрической формой* комплексного числа z. Таким образом, $\mathbb{R}^2 \setminus \{0\}$ может быть отождествлена с прямым произведением $\mathbb{R}_+ \times \mathbb{T}$.

• **Прямоугольники:** пусть $a, b, c, d \in \mathbb{R}$. Ясно, что $[a, b] \times [c, d]$ можно отождествить с прямоугольником на плоскости, с вершинами (a, c), (a, d), (b, c),

(b, d):

$$[a, b] \times [c, d] = \{(x, y) \mid a \leq x \leq b,\ c \leq y \leq d\}.$$

Это **замкнутый** прямоугольник, включающий свою границу.

Задача. Как устроено множество всех нетривиальных интервалов на прямой?

Ответ. Каждый нетривиальный интервал имеет однозначно определенный левый конец a и длину $l > 0$, и обратно любая пара чисел (a, l), $a \in \mathbb{R}$ и $l \in \mathbb{R}_+$, задает нетривиальный интервал $]a, a + l[$. Поэтому множество нетривиальных интервалов можно отождествить с верхней полуплоскостью $\mathbb{R} \times \mathbb{R}_+$.

Задача. Разложите множество ненулевых вещественных чисел $\mathbb{R}^*$ в прямое произведение.

Ответ. Сопоставление вещественному числу $x \in \mathbb{R}^*$ пары $(|x|, \mathrm{sign}(x))$, состоящей из его абсолютной величины и знака, позволяет отождествить $\mathbb{R}^*$ с прямым произведением $\mathbb{R}_+ \times \{1, -1\}$.

Задача. Разложите $\mathbb{R}$ в прямое произведение двух множителей, один из которых $\mathbb{Z}$.

Ответ. Сопоставление вещественному числу $x \in \mathbb{R}$ пары $(\lfloor x \rfloor, \mathrm{Frac}(x))$ позволяет отождествить $\mathbb{R}$ с прямым произведением $\mathbb{Z} \times [0, 1[$.

§ 3. Дальнейшие примеры прямых произведений

> Элементарной ячейкой обычно называют параллелепипед, заполненный конкретным химическим содержанием.
>
> В.А.Франк-Каменецкий[168]

В настоящем параграфе мы приводим довольно много примеров прямых произведений. Пафос здесь состоит в том, что, во-первых, **всегда**, когда речь идет о двух независимо меняющихся величинах (абсцисса и ордината, модуль и аргумент, широта и долгота, целая и дробная часть, вертикали и горизонтали, ряд и место, масть и ранг, лицо и число и т.д.) мы имеем дело с прямым произведением и, во-вторых, что разложение множества в прямое произведение задает на нем *нетривиальную структуру*. Во всех рассмотренных ниже ситуациях структура прямого произведения очевидна для математика-профессионала, но начинающий не всегда смотрит на вещи под этим углом. Студент, считающий, что он владеет этими идеями, может смело пропустить этот параграф. Обобщим для примера разложение вещественного числа на целую и дробную часть на случай высших размерностей, Для этого нам понадобится еще два важных понятия.

• **Двумерная решетка.** Фиксируем два неколлинеарных вектора u и v на плоскости. Множество L точек плоскости, получающихся из начала координат 0 произвольными итерациями сдвигов на u и v и обратных к ним, называется **двумерной решеткой**, порожденной векторами u и v. При этом о паре векторов (u, v) говорят как о **базисе** решетки. Таким образом, $L = \{mu + nv \mid u, v \in \mathbb{Z}\}$. Кристаллографы обычно называют L **плоской сеткой** а элементы L – **узлами** этой сетки. Ясно, что сопоставление точке $x = mu + nv \in L$ пары ее координат (m, n) в базисе (u, v) задает изоморфизм L с прямым произведением $\mathbb{Z} \times \mathbb{Z}$. Заметим, что структура прямого произведения на L (т.е. задание проекций $\mathrm{pr}_1, \mathrm{pr}_2 : L \longrightarrow \mathbb{Z}$) зависит не только от самой решетки L, но и от выбора векторов u, v и, в свою очередь, определяет эти векторы.

• **Элементарные ячейки.** Пусть L – двумерная решетка, порожденная векторами u и v. Назовем **стандартной элементарной ячейкой** этой решетки множество $C = \{au + bv \mid 0 \leq$

[168] Редакционное примечание на стр.18 в книге Т.Пенкаля, Очерки кристаллохимии, Из-во “Химия”, Л., 1974, с.1–496

$a, b < 1\}$, **элементарной ячейкой** – любой сдвиг C при помощи целых кратных векторов u и v:

$$C_{mn} = C + mu + nv = \{x + mu + nv \mid x \in C\} =$$
$$\{au + bv \mid m \le a < m + 1,\ n \le b < n + 1\}.$$

Таким образом, каждая элементарная ячейка содержит ровно один узел решетки и, обратно, каждый узел решетки содержится в единственной элементарной ячейке. Ясно, что элементарная ячейка изоморфна декартову квадрату $[0, 1[^2$. Впрочем, в кристаллографии элементарной ячейкой часто называют **замыкание** нашей элементарной ячейки, т.е., например, множество $\overline{C} = \{au + bv \mid 0 \le a, b \le 1\}$, изоморфное декартову квадрату $[0, 1]^2$.

Теперь мы в состоянии обобщить представление числа в виде суммы целой и дробной частей на случай плоскости. При этом роль целых частей будут играть точки некоторой решетки L.

Задача. Постройте разложение эвклидовой плоскости $\mathbb{R}^2$ в прямое произведение двух множителей, один из которых L.

Ответ. Ну, конечно, это $\mathbb{R}^2 = L \times C$, где C – стандартная (в действительности, **какая-то**) элементарная ячейка.

• **Координаты на сфере.** Рассмотрим сферу $\mathbb{S}^2$ с двумя выделенными противоположными точками, называемыми *северным полюсом* z и *южным полюсом* z^*, соответственно. В географии и астрономии полюсы обычно обозначаются **NP** и **SP**, причем астрономы называют z *зенитом*, а z^* – *надиром*. Прямая, проходящая через полюсы, будет называться *полярной осью*. Пусть, далее, 0 – центр сферы. Большая окружность, лежащая в плоскости, ортогональной к полярной оси и проходящей через 0 называется *экватором* (в астрономии – *горизонтом*, *эклиптикой* и тому подобное, в зависимости от выбора полярной оси), сама эта плоскость называется *плоскостью экватора*. Пересечения сферы с плоскостями, параллельными плоскости экватора, называются *параллелями*, при этом каждая точка x лежит на единственной параллели. Любая дуга большого круга, опирающаяся на полюса называется **меридианом**, каждая точка $x \ne z, z^*$ лежит на единственном меридиане. Обычно один из меридианов фиксируется и провозглашается *нулевым меридианом*.

Тогда каждой точке $x \ne z, z^*$ на этой сфере сопоставляется пара (θ, ϕ), состоящая из двух углов, называемых, соответственно, *широтой* и *долготой* этой точки (а в астрономии – *склонением* и *прямым восхождением* и т.д.). Широта точки x определяется как проекция точки x на нулевой меридиан, т.е. точка пересечения нулевого меридиана с единственной параллелью, проходящей через точку x. Обычно широта отождествляется с углом $\theta \in]-\pi/2, \pi/2[$ между лучом $0x$ и плоскостью экватора. На самом деле, конечно, отрицательными широтами обычно не пользуется, в географии положительные широты называются *северными*, а отрицательные – *южными*, а в механике широтой обычно называется угол между осью $0x$ и осью $0z$, изменяющийся в интервале $]0, \pi[$. Долготой точки x называется ее проекция на экватор, т.е. точка пересечения экватора с меридианом, проходящим через точку x. При этом широта тоже обычно отождествляется с углом $\phi \in [0, 2\pi[$ между плоскостью нулевого меридиана и плоскостью меридиана, на котором лежит точка x. При этом положительным направлением обычно считается направление против часовой стрелки, если смотреть из z. Таким образом, долгота полюсов не определена, а любая другая точка сферы однозначно определяется парой (θ, ϕ). Это значит, что сфера с выколотыми полюсами $\mathbb{S}^2 \setminus \{z, z^*\}$ естественно отождествляется с прямым произведением $(-\pi/2, \pi/2) \times \mathbb{T}$ нулевого меридиана на экватор.

• **Нумерация билетов.** Типичный пример декартова произведения конечных множеств, с которым каждому приходится сталкиваться в жизни – это нумерация авиационных и театральных *билетов*. На билете обычно указывается *ряд* и *место*. В простейшем случае, когда в самолете только один класс, все ряды содержат одинаковое количество мест. Каждое место однозначно определяется заданием ряда, который обычно обозначается числом от 1 до n, в самолете среднего размера, скажем, $n = 30$ и заданием места в ряду, которое обычно обозначается латинской буквой, в самолете среднего размера A, B, C, D, E, F. Таким образом, место в самолете может быть отождествлено с парой (i, x), где $i \in \underline{n}$, $x \in \{A, B, C, D, E, F\}$. Также и в кинотеатрах и многих театрах на билете указывается номер ряда и номер места в ряду. В простейшем случае прямоугольного зала (скажем, в случае партера большого зала Петербургской Филармонии) множество мест может быть отождествлено с $\underline{m} \times \underline{n}$, где m –

число рядов, а n – число мест в ряду. Аналогичная система используется и при нумерации железнодорожных билетов, где на билете указывается номер вагона и номер места. Снова в предположении, что все вагоны имеют одинаковое количество мест, множество всех мест в поезде можно отождествить с множеством пар (i, j), где i – номер вагона, а j – номер места в вагоне.

• **Шахматная доска.** В первом приближении *шахматной доской* называется множество, состоящее из 64 *полей* (или *клеток*), расположеных в виде квадрата 8×8. Это множество может быть разбито на 8 вертикальных полос шириной в 1 клетку, называемых, *вертикалями* или 8 горизонтальных полос высотой в одну клетку, называемых *горизонталями*. Каждое поле однозначно определяет вертикаль и горизонталь, в которых оно расположено (на школьном жаргоне 'абсциссу' и 'ординату' этого поля). В свою очередь, поле однозначно определяется заданием своей вертикали и своей горизонтали. Это значит, что поле может быть *отождествлено* с упорядоченной парой, состоящей из вертикали и горизонтали. Традиционно вертикали нумеруются латинскими буквами от a до f, а горизонтали – арабскими цифрами от 1 до 8, поэтому мы введем множества $V = \{a, b, c, d, e, f, g, h\}$ и $H = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Таким образом, шахматную доску B можно отождествить с прямым произведением $V \times H$. При этом в обычной шахматной нотации вместо $(b, 4)$ пишут $b4$, но суть от этого, конечно, не меняется.

В действительности, кроме разложения в прямое произведение, шахматная доска имеет еще одну важнейшую структуру, которая будет чрезвычайно полезна при решении некоторых рассматриваемых в дальнейшем задач. А именно, шахматная доска обычно рассматривается вместе с разложением в дизъюнктное объединение четной и нечетной частей. При этом традиционно четные поля шахматной доски называются черными, а нечетные – белыми. Подобные системы координат для записи игры и сообщения ходов используются во многих играх: го, 100-клеточные шашки, морской бой и так далее. Например, шашки и морской бой используют доску, состоящую из $100 = 10 \times 10$ клеток, максишахматы – доску, состоящую из $144 = 12 \times 12$ клеток, а го – доску, состоящую из $361 = 19 \times 19$ узлов. В дальнейшем во всех подобных ситуациях мы будем говорить о 'шахматной доске' размера $n \times n$.

• **Стандартная карточная колода.** Большинство серьезных карточных игр, например, контрактный бридж, используют стандартную карточную колоду, состоящую из 52 карт. В книге[169]. приводится следующее определение: *стандартной карточной колодой* называется множество, состоящее из 52 *карт* 4 различных *мастей*, каждая из которых задается своим символом (pip): пики (♠), черви (♡), бубны (♢) и трефы (♣); и 13 карт каждой масти, определяемых своим *рангом*: туз (A), король (K), дама (D), валет (J), 10, 9, 8, 7, 6, 5, 4, 3, 2. Таким образом, стандартная карточная колода P (pack) может быть представлена как прямое произведение $S \times R$ множества мастей S (suits) и множества рангов R (rangs).

Комментарий. Мне доводилось слышать возражение, что 'пиковая дама' не есть пара $(♠, \mathrm{D})$. Конечно, философски настроенные индивидуумы могут считать, что существует некий *трансцендентный* объект 'пиковая дама', который обладает *внутренними характеристиками* (intrinsics), не сводящимися к ее масти и рангу, однако эти характеристики находятся вне обычных аксиоматик карточных игр. Поэтому с точки зрения всех обычных приложений 'пиковая дама' может быть **отождествлена** с парой $(♠, \mathrm{D})$.

§ 4. Упорядоченные n-ки

1. Аксиома упорядоченной n-ки. Все сказанное выше о декартовых произведениях двух множеств можно в действительности обобщить на произведения любых – в том числе и бесконечных – семейств множеств. Для конечного числа сомножителей сделать это совсем просто, нужно лишь говорить не об упорядоченных парах, а об упорядоченных тройках, четверках, ..., n-ках. При этом n-ка читается 'энка', аналогично 'm-ка' читается 'эмка', 'l-ка' – 'элька' и т.д.,

[169] Official rules of card games" - The U.S. Playing Card Company, Cincinatti, Ohio, 1998. – c.11

хотя для некоторых других букв подобное чтение несколько затруднительно[170] В тех случаях, когда мы не хотим явно указывать n, мы будем называть упорядоченную n-ку просто **тупелем**[171]. При этом упорядоченную пару естественно называть **дупелем**, упорядоченную тройку – **трипелем**, упорядоченную четверку – **квадрупелем**, упорядоченную пятерку – **квинтупелем**, упорядоченную шестерку – **секступелем** и т.д.

Комментарий. Программисты часто называют упорядоченную n-ку (линейным) **списком** (list) или (одномерным) **массивом** (array), эта терминология получает все большее распространение и в профессиональной математической литературе. С моей точки зрения оба эти термина не свободны от недостатков так как программисты разных деноминаций используют их в различных смыслах, отягощенных всевозможными коннотациями. Дело в том, что массив не обязательно одномерен, а списки, как правило, трактуются динамически и в разных языках программирования реализуются по разному, причем совершенно не обязательно как тупели. В `Mathematica` список действительно имеет структуру упорядоченной n-ки: $\{x_1,\dots,x_n\}$[172] Но в некоторых других языках, в частности в `Lisp`[173] и `Prolog` список *фактически* состоит из головы (head) и хвоста (tail), который сам является списком на единицу меньшей длины[174], иными словами список длины n истолковывается как $(x_1,(x_2,\dots,x_n))$. С другой стороны, массив не обязательно линеен, он может быть индексирован несколькими индексами. В языке `C` массивы отличаются от списков тем, что их размер изменить невозможно, так как выделяемая под массив память определяется в процессе компиляции, списки же носят динамический характер и их длина может меняться в процессе вычисления. Язык `C++` гораздо гибче и допускает динамические массивы, но различает списки и массивы по способу обращения к их элементам. Список упорядочен, но не индексирован и в нем можно обращаться только к первому, последнему и текущему элементу. С другой стороны, массив индексирован и допускает обращение к произвольному элементу. В свою очередь Кнут называет то, что мы называем просто списками, **`линейными списками`**, используя термин **`Список`**

---

[170]'По-русски чаще пользуются термином 'энка' (n-ка), а еще чаще (но в более широком смысле) – 'k-ка'' – примечание переводчика к [FBH], стр.144. В математических кружках для младших школьников $(x_1,\dots,x_k)$ обычно называется 'кашкой'.

[171]Предлагаемый нами термин **`тупель`** является калькой немецкого `Tupel`. Многие русские программисты используют то, что они считают английским чтением слова `tuple`, а именно, **`тупл`**. Однако дело в том, что по-английски `tuple` читается как **`тьюпл`**, а n-`tuple` как n-**`тапл`**. Я уже неоднократно объяснял свою точку зрения, что немецкое чтение терминов *всегда* дает более узнаваемые и правдоподобные результаты.

[172]Если быть совсем точным, список реализуется как укорененное *дерево* $\texttt{List}[x_1,\dots,x_n]$, с корнем `List` и соединенными с ним листьями $x_1,\dots,x_n$. Однако это относится к внутреннему представлению данных в программе, и при всех обычных приложениях остается невидимым большинству юзеров. Одномерные массивы имеет ту же структуру, что и списки, но отличается способом трактовки их имен и индексов членов. В математических терминах это соответствует записи списка как $x=\{x_1,\dots,x_n\}$, а массива как $x(\underline{n})=\{x(1),\dots,x(n)\}$. Разумеется, после того, как массив построен, он начинает трактоваться как список.

[173]`Lisp` — разработанный в 1958 году Джоном Маккарти весьма примитивный язык работы со списками, название которого значит **`шепелявить`** (не выговаривать звуки `с` и `з`) и читается как **`лишп`**. Впрочем, имеются и апокрифические расшифровки `LISP`, например, как сокращения от `Lots of Inane Stupid Parenthesis`. Это популярное название связано с тем, что в отличие от большинства языков высокого уровня в `Lisp` *отсутствуют* инструменты для работы со списками, так что каждый список приходится явно истолковывать через упорядоченные пары. Поэтому при образовании длинных списков в `Lisp` приходится ставить много лишних скобок, вводящих ненужную дополнительную структуру.

[174]Конечно, голова списка тоже может быть списком. Формально в руководствах по языку `Lisp` список изображается как $(x_1,\dots,x_n)$. Тем не менее, поскольку в чистом `Lisp` нет никаких операций со списками, кроме операций, выражающихся в `Mathematica` как `First`, `Rest` и `Prepend`, то на самом деле по умолчанию список с членами $x_1,\dots,x_n$ истолковывается в `Lisp` как правонормированный $(x_1,(x_2,(\dots,x_n)\dots))$. Конечно, в `Lisp` можно написать $((x,y),z)$. Но никакого аналога операции `Flatten`, позволяющей убрать лишние скобки, т.е. никакого способа написать просто (x,y,z), там нет.

(это не просто список, это список с большой буквы!) для *гораздо* более общей структуры, включающей в себя, *в частности*, деревья и леса. Но даже и линейные списки могут быть организованы как деки, стеки, очереди, циклические списки, дважды связанные списки и т.д. В то же время Вирт явно требует от массива не только свободного доступа, но и *однотипности*. Иными словами, все компоненты массива должны быть переменными одного и того же базисного типа, так что с точки зрения Вирта не только $((x, y), z)$, но даже $(1, \pi)$ не является массивом! Для тупелей с компонентами различных типов Вирт вводит специальный термин **запись** (record). Нежелание вдаваться в программистски-теологические дискуссии на тему о том, сколько демонов может поместиться на одном из концов списка, объясняет, почему мы не используем слова **список** и **массив** как *математические* термины. В русской *учебной* литературе, в частности, [Shi], n-ки иногда называются **кортежами**, но работающие математики **никогда** не пользуются этим термином.

Аксиома упорядоченной n-ки. *Равенство двух упорядоченных n-к*

$$(x_1 \dots, x_n) = (y_1, \dots, y_n)$$

имеет место тогда и только тогда, когда $x_i = y_i$ для всех i, $1 \leq i \leq n$.

2. Упорядоченная n-ка по Куратовскому. Упорядоченные n-ки можно определять по разному. В ортодоксальной теории множеств упорядоченную n-ку можно определить по Куратовскому. Например, в качестве упорядоченной тройки (x, y, z) можно взять $\{\{x\}, \{x, y\}, \{x, y, z\}\}$, в качестве упорядоченной четверки (x, y, z, u) можно взять $\{\{x\}, \{x, y\}, \{x, y, z\}, \{x, y, z, u\}\}$ и так далее.

Задача. Докажите, что $(x_1, \dots, x_n)$, определенная как

$$\{\{x_1\}, \{x_1, x_2\}, \dots, \{x_1, x_2, \dots, x_n\}\}$$

действительно удовлетворяет аксиоме упорядоченной n-ки.

3. Рекуррентное определение упорядоченной n-ки. Однако обычно упорядоченные n-ки определяются индуктивно как

$$(x_1, \dots, x_n) = ((x_1, \dots, x_{n-1}), x_n).$$

Например, упорядоченная тройка $(x, y, z) = ((x, y), z)$, упорядоченная четверка $(x, y, z, u) = ((x, y, z), u) = (((x, y), z), u)$ и так далее. Такая расстановка скобок называется **левонормированной**.

Задача. Докажите, что $(x_1, \dots, x_n)$, определенная как

$$((\dots(x_1, x_2), \dots, x_{n-1}), x_n)$$

удовлетворяет аксиоме упорядоченной n-ки.

Впрочем, опять специальное выражение упорядоченной n-ки в терминах упорядоченных пар не играет никакой роли. Мы могли бы определить упорядоченную n-ку при помощи правонормированной расстановки скобок, как $(x_1, \dots, x_n) = (x_1, (x_2, \dots, x_n))$ и многими другими способами. А ведь с точки зрения теории множеств упорядоченные n-ки, построенные при помощи левонормированной и **правонормированной** расстановки скобок – это совсем не одно и то же.

Задача. Что такое $((x, y), z)$ и $(x, (y, z))$ если упорядоченные пары интерпретируются по Куратовскому.

Впрочем, то, что упорядоченные n-ки можно определить по разному, не имеет никакого значения. Важно лишь, что между так определенными n-ками можно установить естественное взаимно однозначное соответствие. Например, $(x, y, z) \leftrightarrow ((x, y), z) \leftrightarrow (x, (y, z))$ устанавливает **каноническое** взаимно однозначное соответствие между тремя приведенными выше определениями упорядоченных троек. В более наивных изложениях в этом месте было бы написано $(x, y, z) = ((x, y), z) = (x, (y, z))$.

§ 5. Прямые произведения конечного семейства множеств

Понятие прямого произведения легко обобщается на любое конечное число сомножителей.

1. Прямое произведение конечного семейства множеств. Прямое произведение n множеств определяется точно так же, как прямое произведение двух множеств, но вместо упорядоченных пар нужно работать с упорядоченными n-ками. Пусть $X_1, \dots, X_n$ суть n множеств. Их декартово произведение определяется как

$$X_1 \times \dots \times X_n = \{(x_1, \dots, x_n) \mid x_i \in X_i\},$$

где $(x_1, \dots, x_n)$ обозначает упорядоченную n-ку, в которой первая компонента принадлежит X_1, вторая X_2, и т.д. Например,

$$\begin{aligned}\{0,1\} \times \{a,b\} \times \{@,\#\} =& \{(0,a,@),(0,a,\#),(0,b,@),(0,b,\#),\\ &(1,a,@),(1,a,\#),(1,b,@),(1,b,\#)\}.\end{aligned}$$

Для обозначения прямого произведения множеств часто используется знак $\prod$, известный под TEXническим именем `\prod`. Таким образом, вместо $X_1 \times \dots \times X_n$ пишут $\prod\limits_{i=1}^{n} X_i$. В частности, если $X_1 = \dots = X_n = X$, говорят об n-й **декартовой степени** множества X, а при $n = 3$ используется еще выражение **декартов куб**.

2. Ассоциативность прямого произведения. Во многих элементарных руководствах прямое произведение конечного числа множеств беззастенчиво определяется по индукции как $X_1 \times \dots \times X_n = (X_1 \times \dots \times X_{n+1}) \times X_n$. При этом те же авторы на той же странице говорят, что прямое произведение некоммутативно $X \times Y \neq Y \times X$. Оба эти утверждения не могут быть верными одновременно, так как статус коммутативности и ассоциативности для прямых произведений абсолютно одинаков: с точностью до равенства ни ассоциативность, ни коммутативность не имеют место, с точностью до эквивалентности обе они имеют место. В действительности, $(X \times Y) \times Z \neq X \times Y \times Z \neq X \times (Y \times Z)$, так как второе из них состоит из упорядоченных троек, в то время как первое и третье состоят из упорядоченных пар. В то же время с точностью до *канонических* изоморфизмов $(X \times Y) \times Z \approx X \times Y \times Z \approx X \times (Y \times Z)$, но, конечно, в том же самом смысле $X \times Y \approx Y \times X$.

3. Первые примеры. Вот несколько очевидных примеров прямых произведений трех множеств. Снова наиболее знакомый частный случай декартова произведения трех множеств – это координаты в пространстве. Эти примеры полностью параллельны соотвествующим примерам на плоскости и на сфере, но теперь имеется три координаты.

• **Декартовы координаты в пространстве.** В этой системе координат каждой точке пространства сопоставляются ее проекции на *три* координатные оси, называемые *осью абсцисс*, *осью ординат* и *осью аппликат*, соответственно. В свою очередь точка w пространства однозначно определяется своими проекциями x, y, z на эти оси, называемыми в школьном курсе ее *абсциссой*, *ординатой* и *аппликатой*. Таким образом, точка w трехмерного пространства может быть *отождествлена* с тройкой своих координат (x, y, z). При этом пространство (вместе с проекциями на координатные оси!) отождествится с прямым произведением координатных осей, т.е. *трех* экземпляров $\mathbb{R}$. Таким образом, трехмерное эвклидово пространство можно рассматривать как *декартов куб* вещественной оси. Это объясняет обычное обозначение эвклидова пространства через $\mathbb{R}^3$.

• **Цилиндрические координаты.** Удалим из пространства $\mathbb{R}^3$ ось аппликат:

$$X = \{(x, y, z) \mid x, y, z \in \mathbb{R}, z \neq 0\}.$$

В цилиндрических координатах точка в множестве X задается тремя координатами: полярными координатами (r, ϕ) ее проекции на плоскость xy и аппликатой z. Таким образом, $X = \mathbb{R}_{>0} \times \mathbb{T} \times \mathbb{R}$.

• **Сферические координаты.** Точка в множестве X описанном в предыдущем примере может быть задана еще и следующей тройкой координат: вначале укажем *полярный радиус* R точки $w = (x, y, z)$, т.е. ее расстояние до начала координат $R = \sqrt{x^2 + y^2 + z^2}$. Полярный радиус это радиус сферы с центром в начале координат, на которой лежит точка w. Как мы знаем из § ?, точка на сфере определяется своей *широтой* θ и *долготой* ϕ. Таким образом, точка $w \in X$ определяется набором координат (R, θ, ϕ) и, значит, $X = \mathbb{R}_{>0} \times (-\pi/2, \pi/2) \times \mathbb{T}$.

• **Двойная колода.** Некоторые игры (например, русский банк) требуют **двойную колоду**, состоящую из 2 стандартных колод с разными **рубашками**. Таким образом, двойная колода D представляется как прямое произведение $S \times R \times B$, где S и R имеют тот же смысл, что и выше, а B – множество рубашек (backs).

• **Кубик Рубика.** 27 маленьких кубиков, из которых составлен *умозрительный* кубик Рубика (включая несуществующий центральный кубик), можно мыслить себе как элементы декартова куба $\{-1, 0, 1\}^3$. Подобная координатизация фундаментальных областей часто применяется в теоретической кристаллографии.

• **Системы счисления.** Основная идея позиционной системы счисления состоит, как раз, в том, чтобы представить множество натуральных чисел – а потом и дробей – как объединение всевозможных конечных декартовых степеней множества цифр. Например, (не более, чем) трехзначное неотрицательное целое число можно мыслить себе как элемент декартова куба Digit^3 и так далее. Фактически эта система нуждается в некоторых модификациях, чтобы учесть знаки, положение запятой и т.д.

• **Автомобильные номера.** В большинстве европейских стран автомобильный номер состоит из комбинации латинских букв и арабских цифр (см. определение этих понятий в § 1.3).

Задача. Достаточно ли двух букв и четырех цифр для того, чтобы все автомобили в Германии получили различные номера?

Указание. Описанное в этой задаче множество изоморфно $\mathrm{Lat}^2 \times \mathrm{Digit}^4$. Найдите его порядок по правилу произведения.

Ответ. Нет, этого количества (6760000 комбинаций) недостаточно даже для того, чтобы различные номера получили уже все автомобили в земле Nordrhein-Westfalen, но вот *трех* букв и четырех цифр (175760000 комбинаций) более, чем достаточно.

4. Компьютерные примеры. Много конкретных примеров прямых произведений встречается в информатике и электронике.

• **Байт.** Один байт это элемент 8-й декартовой степени $\texttt{Byte} = \mathbb{F}_2^8$ двухэлементного поля $\mathbb{F}_2 = \{0, 1\}$. По правилу произведения $|\mathbb{F}_2^8| = 2^8 = 256$. Этого обычно достаточно, например,

для того, чтобы записывать буквы двух европейских алфавитов в двух регистрах, цифры, знаки препинания и некоторые управляющие символы.

• **Модель RBG.** Это основная *аддитивная* модель цвета, используемая в бытовом телевидении и большинстве компьютерных мониторов. Модель RBG описывает *излучаемые* цвета как комбинации *трех* основных цветов: красного (`Red`), синего (`Blue`), зеленого (`Green`). Именно эти цвета непосредственно воспринимаются человеческим глазом. В модели RBG передается интенсивность каждой из компонент, входящих в разложение данного цвета. Специалисты по электронике обычно называют компоненты **каналами**, причем в современных мониторах используется модель `TrueColor`, в которой на передачу каждого канала отведен один байт. Это значит, что градации каждого из основных цветов передаются числами от 0 (самый темный) до 255 (самый яркий). Таким образом, цвет в этой модели соответствует элементу декартова куба $\mathtt{RBG} = \mathtt{Byte}^3$. По формуле произведения общее количество цветов, отображаемых на экране монитора в режиме `TrueColor` равно $|\mathtt{RBG}| = 256^3 = 16777216$. Например, черный цвет в этой модели передается как $(0, 0, 0)$, а белый – как $(1, 1, 1)$.

• **Модель CMYK.** Это основная *субтрактивная* модель цвета, используемая в полиграфии и большинстве струйных принтеров. Модель CMYK описывает *отражаемые* цвета как комбинации *четырех* основных цветов: голубого (`Cyan`), пурпурного (`Magenta`), желтого (`Yellow`) и черного (`Key`). Конечно, для передачи цвета было бы достаточно *трех* цветов CMY, но фактически при печати темных оттенков использование модели, основанной на трех красках, вело бы к переувлажнению и деформации бумаги и избыточному расходу краски, поэтому темные оттенки печатаются с использованием черного цвета. Поэтому цвет в этой модели передается *четырьмя* байтами, так что $\mathtt{CMYK} = \mathtt{Byte}^4$. Снова количество каждой из четырех накладываемых красок передается числом от 0 (вообще не накладывается) до 255 (максимум). По формуле произведения общее количество полиграфических красок, передаваемых этой моделью, равно $|\mathtt{CMYK}| = 256^4 = 4294967296$, но, разумеется, не все они приводят к результатам различимым на глаз. Например, как $(1, 1, 1, 0)$, так и $(0, 0, 0, 1)$ по идее передают чистый черный цвет, но, разумеется, в первом случае для достижения того же результата нужно в три раза больше краски (в действительности, конечно, и сам результат в этом случае получится гораздо хуже, так как при смешении фактически используемых в принтере красок вместо чистого черного получится достаточно мерзкий темно-коричневый цвет).

• **Модель HSB.** Принципиально иначе устроена модель HSB, используемая в системах компьютерной графики. Как и в модели RBG в этой модели цвет описывается тремя компонентами, но это совершенно другие компоненты: тон (`Hue`), насыщенность (`Saturation`), яркость (`Brightness`). При этом тон передается положением в цветовом круге, измеряемом от 0^o (красный цвет) до 359^o (фактически, конечно, она все равно передается одним байтом, так что можно считать, что 2π радиан = 256 градусов!). Насыщенность описывает монохроматичность цвета, она меняется от 0 до 255 (в руководствах по компьютерной графике обычно пишут, что насыщенность меняется от 0% до 100%, но это, конечно, вранье). Чем меньше насыщенность, тем светлее цвет, при насыщенности 0 любой цвет становится белым. Яркость также меняется от 0 – самый темный, до 255 – самый яркий (конечно, специалисты по компьютерам опять попытаются Вас обмануть сказав, что она меняется от 0% до 100%). Чем меньше яркость, тем цвет темнее, при яркости 0 любой цвет становится черным. **Загадка:** какой цвет передается тройкой $(0, 0, 0)$ – красный, белый или черный? А теперь включите компьютер и проверьте!

§ 6. Лингвистические примеры

> Ибрахим аль-Каззаз формулировал суфийский метод в таких словах: “Демонстрируй неизвестное в терминах того, что называется “известным” в данной аудитории”.
>
> Идрис Шах, ‘Сказки дервишей’

За пределами собственно математики только язык (и письмо!), музыка и игра благодаря своей жесткой структуре в наибольшей степени поддаются математическому описанию.

• **Китайские циклические знаки.** Интересным примером прямого произведения двух

множеств являются китайские[175] циклические знаки, используемые в хронологии ('год дракона', 'год змеи', etc.). Первый ряд, `jikkan` состоит из 10 знаков,

Ji={`kinoe, kinoto, hinoe, hinoto, tsuchinoe, tsuchinoto, kanoe, kanoto, mizunoe,mizunoto`},

а второй ряд `junishi` – из 12 знаков

Ju={`ne=крыса, ushi=бык, tora=тигр, u=заяц, tatsu=дракон, mi=змея, uma=лошадь, hitsuji=овца, saru=обезьяна, tori=птица, inu=собака, i=боров`}.

По принятому в Китае и Японии календарю номер года внутри данной эпохи задается парой, состоящей из двух циклических знаков. Каждая эпоха состоит из 60 лет и начинается годом `kinoe ne`, следующий за ним год называется `kinoto ushi`, потом идет `hinoe tora` и т.д. Например, эпоха, в которой мы живем сегодня, началась в 1984 году, который был `kinoe ne`, 1985 год – `kinoto ushi` и т.д.

Естественно возникает вопрос, почему же эпоха состоит из 60 лет, если порядок произведения Ji × Ju равен 120? Дело в том, что фактически в качестве названия года фигурируют не все элементы Ji × Ju, а только те из них, для которых сумма номеров первого и второго знаков четна, т.е. ровно половина из них. Например, сочетание `kinoe ushi` невозможно, а сочетание `kinoto ushi` возможно. Названия знаков первого ряда сами являются составными, они идут парами, состоящими из старшего брата `e` и младшего брата `to`. Сами же пары отвечают пяти стихиям:

Go={`ki=огонь, hi=дерево, tsuchi=земля, ka=металл, mizu=вода`}.

Таким образом, в действительности с математической точки зрения год внутри данной эпохи полностью определяется парой, состоящей из стихии и циклического знака второй серии, т.е. каждая эпоха может быть отождествлена с Go × Ju.

• **Кана.** В отличие от китайского письма, в котором не используется ничего, кроме иероглифов, для записи японского языка, помимо того, применяется слоговое письмо, называемое *каной*. Базовой фонетической единицей японского языка является не фонема (как в русском, английском или немецком), а *слог*[176]. Основная таблица каны *годзюон* (от японского `gojûonzu` – таблица 50 звуков), изображается в виде матрицы, горизонтальные строки которой называются `dan` (ступени или уровни), а вертикальные столбцы – `gyô` (ряды)[177]. Строки этой таблицы соответствуют 5 гласным японского языка Dan={`a,i,u,e,o`}, а столбцы – 10 слогам Gyo={`a,ka,sa,ta,na,ha,ma,ya,ra,wa`}. *По идее*, на пересечении столбца и строки[178] стоит слог, первым звуком которого является согласный соответствующего элемента Gyo (в случае `a-gyô` – это, как принято говорить у лингвистов, ∅!), а вторым – элемент Dan. Таким образом, первый ряд годзюона, `a-gyô` выглядит так: {`a,i,u,e,o`}; второй ряд, `ka-gyô` – {`ka,ki,ku,ke,ko`}; а, скажем, пятый ряд, `na-gyô` – {`na,ni,nu,ne,no`}; седьмой ряд, `ma-gyô`

---

[175]Ввиду полной невозможности правдоподобно (или хотя бы узнаваемо) воспроизвести *китайские* названия циклических знаков европейским письмом, здесь и всюду в настоящем тексте в качестве чтений иероглифов приводятся их *японские* **куны**, записанные латиницей по системе Хепберна (`Hebonshiki-rômaji`), которая приблизительно передает *английское* произношение соответствующих согласных.

[176]"Если попросить японца сказать *сима* 'остров' наоборот, то он скажет не *амис*, а *маси*." – И.Фридрих, История письма. – Наука, М., 1979, с.1–463, стр.182.

[177]Вообще-то говоря, вопреки ожиданиям человека, пользующегося европейским письмом, в филологии, типографском деле и т.д., `dan` переводится как *столбец*, а `gyo` – как *строка*. Дело в том, что основное направление традиционного китайского и японского письма вертикальное. Естественно, когда китайские математики V века до нашей эры записывали матрицу системы линейных уравнений, при этом уравнения изображались в виде столбцов (в европейском понимании!), а не строк, как это делаем мы, так что при исключении неизвестных элементарные преобразования проводились над столбцами, а не над строками, причем нашему направлению сверху вниз соответствовало направление справа налево! Чтобы не путаться со строками и столбцами, русские филологи традиционно называют столбцы годзюона (в европейском понимании!) *рядами*.

[178]Как должно быть ясно из предыдущего примечания, в традиционном японском письме номер столбца указывается *перед* номером строки, кроме того, нумерация столбцов идет справа налево!

– {ma,mi,mu,me,mo}; а девятый ряд, ra-gyô – {ra,ri,ru,re,ro}. Фактически эта таблица существует в двух основных модификациях: *хирагана* и *катакана*. Хирагана *может* использоваться для записи собственно японских слов (в действительности, за исключением книг для самых маленьких детей она почти всегда используется в сочетании с *кандзи*) а катакана – для записи иностранных заимствований (слов наподобие aisu-kurimu). Таким образом, *в первом приближении*, японский силлабарий[179] можно рассматривать как 100-элементное произведение *трех* множеств Gyo × Dan × Var, где Var={hiragana, katakana}.

В действительности, конечно, кана устроена *гораздо* сложнее, чем описанная выше традиционная модель, так как на самом деле в современном японском языке не 10, а 17 согласных. Прежде всего, нужно учесть, сочетаемость фонем и позиционные аллофоны: скажем, в современном языке нет слога si, а есть только слог shi (этот отсутствующий в русском согласный произносится как польское ś или как немецкий ich-Laut). Таким образом, *фактически* третий ряд годзюона, sa-gyô читается так: {sa,shi,su,se,so}; четвертый ряд, ta-gyô – так: {ta,chi,tsu,te,to}; а шестой ряд, ha-gyô – так: {ha,hi,fu,he,ho}. Кроме того, это приводит к тому, что некоторые ряды не полны: а именно, в восьмом ряду, ya-gyô вместо обычных пяти всего три звука {ya,yu,yo}, а в десятом, wa-gyô – так и вовсе два {wa,(w)o}. С учетом этих поправок годзюон выглядит так

wa	ra	ya	ma	ha	na	ta	sa	ka	a
-	ri	-	mi	hi	ni	chi	shi	ki	i
-	ru	yu	mu	fu	nu	tsu	su	ku	u
-	re	-	me	he	ne	te	se	ke	e
(w)o	ro	yo	mo	ho	no	to	so	ko	o

Однако и это только часть правды. Дело в том, в этой таблице воспроизведены только ‘чистые звуки’ (choke-on). Фактически, кроме того, для второго, третьего, четвертого и шестого рядов существуют соответствующие ‘замутненные звуки’ (daku-on), а именно, {ga,gi,gu,ge,go}; {da,ji,du,de,do}; {za,ji,zu,ze,zo}; {ba,bi,bu,be,bo}; а для шестого ряда еще и ‘полузамутненные звуки’ (han-daku-on): {pa,pi,pu,pe,po}. Кроме того, имеется еще отдельный знак для n (это *единственная* согласная, которую японец может произнести не в составе слога!) и 33 ‘йотированных звука’ yô-on, {kya,kyu,. . . ,pyo}, для записи которых используется более одного знака каны.

• **Китайская грамота.** Как и в японском, основной фонетической единицей современного китайского языка является слог. Однако китайский слог устроен совершенно иначе, и значительно сложнее, чем японский. Ограничимся для простоты рассмотрением официального китайского ‘всеобщего языка’, известного как *путунхуа*[180]. В путунхуа каждая морфема представляет собой слог, который определяется четырьмя компонентами: *инициалью*, *медиалью*, *финалью* и *тоном*. Инициаль является согласной, может быть пустой; медиаль – гласной (в диалектах медиалью может быть и сонорный согласный), и, чтобы не утомлять читателя, мы не будем перечислять все возможные инициали и медиали путунхуа, а обозначим их множества через Init и Medi. Но вот перечислить все финали и тоны совсем просто. А именно, в отличие от южных диалектов в путунхуа имеется всего четыре финали Final={∅,n,ng,r}. Самым необычным в китайском слоге с точки зрения европейца является тон обозначающий повышение или понижение высоты звука. В путунхуа всего четыре тона Tone={¯,ˊ,ˇ,ˋ}, которые обычно называются, без затей, 1-м, 2-м, 3-м и 4-м. Таким образом, множество возможных китайских слогов является прямым произведением *четырех* множеств Init × Medi × Final × Tone. Однако в действительности, из примерно 1600 возможных слогов фактически в путунхуа встречаются лишь около 1200, которые и составляют полный фонетический состав китайского языка. С этим связана громадная синонимия и серьезные трудности в восприятии китайского языка на слух, которые испытывают не только иностранцы, но даже сами китайцы, в особенности уроженцы Юга, для которых путунхуа не является родным.

---

[179]см., например, E.Saito, H.Silberstein, Grundkurs der modernen Japanischen Sprache. – VEB Verlag Enziklopädie, Leipzig, 1981, S.1–646, таблица на стр.28.

[180]В первом приближении это пекинский диалект, обыватель называет его просто *китайским языком*, а переводчики американских фильмов – *мандариновым китайским* (Mandarin Chinese).

• **Четырехбуквенные слова.** Фиксируем алфавит X. Тогда множество $W_l(X)$ всех слов длины l в алфавите X можно отождествить с l-й декартовой степнью X^l этого алфавита. Для выражения несложных мыслей обычно удается обходиться небольшими подмножествами этих множеств. Например, основной словарный запас (Grundwortschatz) героев большинства американских фильмов образует подмножество в Lat^4, известное в просторечии как four-letter words.

• **Парадигмы.** Напомним, что парадигмой называется таблица флективных форм слова в индоевропейских и семитских языках. Например, в индоевропейских языках парадигма глагола определяется произведением лица Pers, числа Num, времени Temp, наклонения Modus, залога Vox и т.д. Что получается в результате, знает каждый, кто учился в классической гимназии и пытался проспрягать какой-нибудь простенький греческий глагол.

• **Гарнитуры.** Раньше типографское дело было вотчиной профессионалов, но теперь, в связи с распространением компьютерных типографских систем, стало всеобщим достоянием. *Гарнитурой* называется множество типографских шрифтов одинаковых по характеру рисунка, но различных начертаний и кеглей. *Шрифтом* называется множество *литер*, с буквами алфавита и всеми относящимися к нему знаками и цифрами. *Начертание* шрифта определяется его *наклоном* (прямой, курсив, наклонный), *шириной* (узкий, нормальный, широкий), *насыщенностью* (светлый, полужирный, жирный), *пропорциональностью* и т.д. *Кеглем* называется размер шрифта, измеряемый в типографских *пунктах* (сокращенно `pt`). Наиболее употребительны шрифты на следующие кегли: бриллиант (`3pt`), диамант (`4pt`), перль (`5pt`), нонпарель (`6pt`), миньон (`7pt`), петит (`8pt`), боргес (`9pt`), корпус (`10pt`) и цицеро (`12pt`). В газетах, плакатах и т.д. используются более крупные шрифты: терция (`16pt`), текст (`20pt`), миттель (`24pt`), малый канон (`36pt`) и большой канон (`48pt`).

Рассмотрим теперь какую-либо конкретную гарнитуру, для определенности гарнитуру CyrTimes, которой набран основной (русский!) текст настоящей книги. При этом, как обычно, возникают два регистра Case=`{Upper,Lower}`, и, чтобы не отвлекать внимание читателя, используются всего пять различных начертаний Type=`{\rm,\it,\bf,\tt,\smc}` и всего три кегля Size=`{8pt,10pt,12pt}`. Таким образом, *в первом приближении* использованную при наборе настоящего текста гарнитуру CyrTimes можно представлять себе как произведение

$$\mathrm{CyrTimes} = \mathrm{Cyr} \times \mathrm{Case} \times \mathrm{Type} \times \mathrm{Size}.$$

Разумеется, при этом русский алфавит Cyr нужно понимать не так, как он определен в Главе I, так как в него должны теперь входить цифры, знаки препинания и т.д. Не все элементы этого множества фактически различаются как *литеры* и далеко не все они были фактически использованы. Кроме того, для набора фрагментов на западных языках использовано аналогичное множество, основанное на Lat вместо Cyr. Все это, конечно, не относится к набору формул, где использованы несколько дополнительных кеглей, другие алфавиты (Greek и ивритская буква ‘алеф’), дополнительные начертания (фрактура `\frak`, рукописный `\Cal`, ажурный `\Bbb`, etc.), большое количество дополнительных знаков и т.д.

§ 7. Тождества, связывающие произведение с булевыми операциями

В этом параграфе мы рассмотрим поведение прямого произведения относительно булевых операций. Все фигурирующие в этом параграфе тождества верны и в наивном смысле, если, конечно, все входящие в них прямые произведения интерпретируются одинаковым образом, и в категорном смысле, как канонические изоморфизмы.

1. Дистрибутивность произведения относительно булевых операций.

Произведение множеств дистрибутивно относительно булевых операций:

$$X \times (Y \cup Z) = (X \times Y) \cup (X \times Z), \qquad (X \cup Y) \times Z = (X \times Z) \cup (Y \times Z).$$
$$X \times (Y \cap Z) = (X \times Y) \cap (X \times Z), \qquad (X \cap Y) \times Z = (X \times Z) \cap (Y \times Z).$$
$$X \times (Y \setminus Z) = (X \times Y) \setminus (X \times Z), \qquad (X \setminus Y) \times Z = (X \times Z) \setminus (Y \times Z).$$
$$X \times (Y \triangle Z) = (X \times Y) \triangle (X \times Z), \qquad (X \triangle Y) \times Z = (X \times Z) \triangle (Y \times Z).$$

Свойство дистрибутивности по отношению к пересечению множеств не так интересно, потому что в действительности для прямого произведения и пересечения выполняется *значительно* более сильное тождество **взаимной дистрибутивности**.

Задача. Докажите, что для любых четырех множеств X, Y, Z, W имеет место равенство

$$(X \cap Y) \times (Z \cap W) = (X \times Z) \cap (Y \times W) = (X \times W) \cap (Y \times Z).$$

Решение. Докажем, например, первое из этих равенств, равенство первого члена третьему проверяется совершенно аналогично. Совершенно ясно, что $(X \cap Y) \times (Z \cap W) \subseteq (X \times Z), (Y \times W)$, поэтому первый член содержится во втором. Обратно, пусть $(x, y) \in (X \times Z) \cap (Y \times W)$. Тогда, так как $(x, y) \in (X \times Z)$, то $x \in X$ и $y \in Z$, а так как $(x, y) \in (Y \times W)$, то $x \in Y$ и $y \in W$. Но это и значит, что $x \in X \cap Y$ и $y \in Z \cap W$, так что и второй член в свою очередь содержится в первом.

Задача. Нарисуйте двумерную картинку, изображающую это тождество.

Из той же картинки совершенно ясно, что для объединений ничего подобного не имеет места! Вообще говоря, дистрибутивность произведения относительно объединения дает лишь

$$(X \cup Y) \times (Z \cup W) = (X \times Z) \cup (Y \times W) \cup (X \times W) \cup (Y \times Z).$$

Задача. Верно ли, что

$$(X \cup Y) \times (Z \cup W) = (X \times (Z \cup W)) \cup ((X \cup Y) \times W) \cup (Y \times Z)?$$

Чему при этом равно $(X \times (Z \cup W)) \cap ((X \cup Y) \times W)$?

Задача. Верно ли, что

$$X \times Y \setminus Z \times W = (X \setminus Z) \times Y \cup X \times (Y \setminus W)?$$

Все содержание настоящего параграфа легко обобщается на бесконечноместные булевы операции. А именно, прямое произведение дистрибутивно относительно объединений и пересечений произвольных семейств:

$$\bigcup_{i \in I} X_i \times \bigcup_{j \in J} Y_j = \bigcup_{(i,j) \in I \times J} (X_i \times Y_j), \qquad \bigcap_{i \in I} X_i \times \bigcap_{j \in J} Y_j = \bigcap_{(i,j) \in I \times J} (X_i \times Y_j).$$

Для случая, когда $I = J$, вторую из этих формул можно усилить

$$\bigcap_{i \in I} X_i \times \bigcap_{i \in I} Y_I = \bigcap_{i \in I} (X_i \times Y_i).$$

§ 8. Диаграммы множеств и отображений

Мы будем очень часто пользоваться диаграммами множеств и отображений. Формальное определение диаграмм в общем случае требует введения понятий ориентированного графа и функтора, которые рассматриваются лишь в частях II и III, соответственно. Поэтому пока мы ограничимся лишь несколькими примерами, достаточными для наших ближайших целей. Впрочем, те соглашения, которые мы введем сейчас, будут без всяких изменений использоваться в общем случае, для диаграмм, состоящих из объектов и морфизмов произвольной категории.

1. Коммутативные треугольники. Одной из простейших диаграмм является треугольник. Пусть A, B, C – три множества, $f : A \longrightarrow B$, $g : A \longrightarrow C$ и $h : C \longrightarrow B$ – три отображения между этими множествами. Такая ситуация будет обычно изображаться в виде **треугольника**

$$\begin{array}{ccc} A & \xrightarrow{\ g\ } & C \\ & & \big\downarrow{\scriptstyle h} \\ & & B \end{array}$$

Мы будем говорить, что этот треугольник **коммутативен**, если отображение f равно композиции отображений g и h, т.е. если $f = h \circ g$.

Очень часто заданы не все отображения треугольника, а лишь часть из них, и требуется достроить эту диаграмму до *коммутативного* треугольника. Эта задача есть простейший случай задачи **дополнения** диаграммы до коммутативной диаграммы. В этом случае те отображения, которые заданы с самого начала, изображаются сплошными стрелками, а те, которые требуется построить, – пунктирными. Например, в треугольнике

$$\begin{array}{ccc} A & \xrightarrow{\ g\ } & C \\ & & \\ & & B \end{array}$$

отображения f и g заданы и требуется построить отображение h такое, что $f = h \circ g$. Это не всегда возможно и в Гл. ? мы найдем необходимое и достаточное условие возможности такого дополнения.

2. Коммутативные квадраты. Другой простейшей диаграммой является коммутативный квадрат. Имеется две интересующие нас возможности ориентировать стрелки в квадрате. Чаще всего встречаются квадраты вида

$$\begin{array}{ccc} A & \xrightarrow{\ \alpha\ } & B \\ {\scriptstyle\beta}\big\downarrow & & \big\downarrow{\scriptstyle\gamma} \\ C & \xrightarrow[\ \delta\ ]{} & D \end{array}$$

Как и раньше, это означает, что нам задано четыре множества A, B, C, D и четыре отображения $\alpha : A \longrightarrow B$, $\beta : A \longrightarrow C$, $\gamma : B \longrightarrow D$ и $\delta : C \longrightarrow D$.

Коммутативность этого квадрата означает, что два отображения из A в D, определенные этим квадратом, совпадают, т.е. $\gamma \circ \alpha = \delta \circ \beta$.

Другой тип коммутативных квадратов получается, если иначе ориентировать здесь стрелки. А именно, коммутативность квадрата

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ {\scriptstyle\beta}\uparrow & & \downarrow{\scriptstyle\gamma} \\ C & \xrightarrow[\delta]{} & D \end{array}$$

означает, что $\delta = \gamma \circ \alpha \circ \beta$.

§ 9. Прямое произведение множеств: проекции

В действительности прямое произведение это не просто множество, а множество вместе с проекциями на сомножители. Но если эти проекции заданы, то уже совершенно безразлично, как интерпретировать элементы произведения.

1. Проекции. Сопоставления $(a, b) \mapsto a$ и $(a, b) \mapsto b$ определяют отображения (см. § 2) $\mathrm{pr}_1 : A \times B \longrightarrow A$ и $\mathrm{pr}_2 : A \times B \longrightarrow B$, называемые, соответственно, **проекцией** $A \times B$ на первый и на второй сомножитель. Таким образом, *правильное* определение прямого произведения само требует понятия отображения и мы вернемся к нему в Главе 3 после того, как определим отображения. Однако уже сейчас подчеркнем, что прямое произведение двух множеств A и B это не просто некое множество $A \times B$, а множество $A \times B$ **вместе с отображениями** $\mathrm{pr}_1 : A \times B \longrightarrow A$, $(a, b) \mapsto a$ и $\mathrm{pr}_2 : A \times B \longrightarrow B$, $(a, b) \mapsto b$ называемыми **(каноническими) проекциями** $A \times B$ на первый и на второй сомножитель, соответственно. То же самое множество $A \times B$ вместе с *другой* парой отображений $f : A \times B \longrightarrow A$, $g : A \times B \longrightarrow B$ может уже *не быть* прямым произведением множеств A и B. Приведенное выше наивное определение игнорирует это ключевое обстоятельство.

2. Отличие прямого произведения от булевых операций. В стандартной теории множеств понятие прямого произведения является инструментальным для определения понятий отношения и отображения. Однако существуют другие подходы к обоснованию математики (скажем, система фон Неймана **N** или теория категорий), в которых понятие отображения (называемого функцией или морфизмом) является первичным. В этом случае не понятие отображения определяется через понятие прямого произведения, а, наоборот, прямое произведение определяется через отображения. В отличие от рассмотренных в предыдущем параграфе булевых операций, операция прямого произведение является не теоретико-множественной, а **теоретико-категорной**. Результат применения булевых операций определен **на самом деле**. В отличие от этого прямое произведение двух множеств определено не единственным образом, а лишь **с точностью до канонического изоморфизма**.

3. Пузлы. Математическое содержание головоломки, называемой по-английски jig-saw puzzle, а по-русски просто **пузл**[181], состоит в том, что прямое произведение двух множеств

[181] Набоков использует французское звучание **пузель** (с множественным числом **пузеля**!), а современный снобизм предписывает пытаться воспроизвести английское **пазл**. Однако мне представляется, что по-русски *всегда* следует ориентироваться на **немецкое** произношение

рассматривается просто как множество, *без указания канонических проекций на сомножители*, и требуется восстановить эти проекции. Элементы пузла называются обычно **писиками** (от английского pieces). Для восстановления канонических проекций используется дополнительная информация, состоящая в том, что пузл в целом является некоторой картинкой, а форма писиков строго индивидуальна (в хорошо изготовленном пузле нет двух одинаковых писиков, так что, в принципе, его можно собрать и без помощи картинки, просто по форме писиков). Каждый, кто пытался собрать пузл средних размеров, скажем, состоящий из $1000 = 40 \times 25$ писиков, знает, что даже с использованием этой дополнительной информации восстановление канонических проекций является совершенно нетривиальным занятием. Разумеется, после того, как пузл однажды собран, а на тыльной стороне каждого писика указаны номера соответствующей горизонтали и вертикали, следующая сборка пузла не требует уже никаких интеллектуальных усилий. Сравнение коробки с писиками и собранной картинки иллюстрирует различие между прямым произведением *как множеством* и как множеством *вместе с каноническими проекциями* и показывает, что разложение множества в прямое произведение задает на этом множестве нетривиальную и, в действительности, **чрезвычайно сильную** структуру.

4. Коммутативность прямого произведения. В элементарных учебниках обычно говорится, что прямое произведение множеств некоммутативно, в том смысле, что, вообще говоря, $A \times B \neq B \times A$.

Задача. Докажите, что если $A \times B = B \times A$, то $A = B$.

Решение. Действительно, предположим, что $A \not\subseteq B$ и пусть $a \in A \setminus B$, а $b \in B$. Тогда $(a, b) \in A \times B$, но $(a, b) \notin B \times A$. Совершенно аналогично доказывается и что $A \times B \neq B \times A$ и для случая $B \not\subseteq A$.

Однако в действительности *равенство* множеств является **абсолютно** бессмысленным понятием при рассмотрении прямых произведений, которые определены лишь с точностью до канонических изоморфизмов. А с этой точки зрения прямое произведение вполне коммутативно.

Задача. Докажите, что $(B \times A, \mathrm{pr}_2, \mathrm{pr}_1)$ является прямым произведением A и B.

Решение. Определим отображение $\mathrm{sw} : B \times A \longrightarrow A \times B$, полагая $\mathrm{sw}(b, a) = (a, b)$. Ясно, что $\mathrm{pr}_2 = \mathrm{pr}_1 \circ \mathrm{sw}$ и $\mathrm{pr}_1 = \mathrm{pr}_2 \circ \mathrm{sw}$.

Таким образом, $A \times B \approx B \times A$.

§ 10. Универсальное свойство прямого произведения

В настоящем параграфе мы дадим *правильное* определение прямого произведения. При этом мы предполагаем, что читатель владеет понятиями композиции отображений, биекции и обратного отображения. Читателю, не знакомому с этими понятиями, рекомендуется при первом чтении пропустить настоящий параграф.

Определение. Прямым произведением *двух множеств A и B называется множество $A \times B$ вместе с отображениями $\mathrm{pr}_1 : A \times B \longrightarrow A$ и $\mathrm{pr}_2 : A \times B \longrightarrow B$, называемыми* **каноническими проекциями** *$A \times B$ на первый и второй множитель, удовлетворяющее следующему* **универсальному свойству**. *Для любого множества C и любых отображений $f : C \longrightarrow A$ и*

заимствований из западных языков, так как при этом по чисто фонетическим причинам получаются если не наиболее правдоподобные, то, по крайней мере, наиболее узнаваемые результаты.

$g : C \longrightarrow B$

$$\begin{array}{ccc} A \times B & \xrightarrow{\mathrm{pr}_1} & A \\ {\scriptstyle \mathrm{pr}_2}\downarrow & & \uparrow{\scriptstyle f} \\ B & \xleftarrow[g]{} & C \end{array}$$

существует единственное отображение $(f, g) : C \longrightarrow A \times B$ *такое, что* $f = \mathrm{pr}_1 \circ (f, g)$ *и* $g = \mathrm{pr}_2 \circ (f, g)$.

Иногда, если нужно явно указать проекции, пишут $(A \times B, \mathrm{pr}_1, \mathrm{pr}_2)$. В частности, если в этом определении взять $f = \mathrm{pr}_1$ и $g = \mathrm{pr}_2$, то, очевидно, $\mathrm{id} = \mathrm{id}_{A\times B}$ удовлетворяет равенству $\mathrm{pr}_i = \mathrm{pr}_i \circ \mathrm{id}$, $i = 1, 2$, причем, согласно универсальному свойству id является **единственным** отображением из $A \times B$ в себя, обладающим этим свойством.

Задача. Убедитесь, что $(\mathrm{pr}_1, \mathrm{pr}_2) = \mathrm{id}_{A\times B}$.

2. Конструкция прямого произведения. Покажем, что наивное прямое произведение, о котором шла речь в § 2, вместе с проекциями pr_1 и pr_2, определенными посредством $(a, b) \mapsto a$ и $(a, b) \mapsto b$, действительно обладает универсальным свойством. Действительно, пусть $f : C \longrightarrow A$ и $g : C \longrightarrow B$ – два произвольных отображения. Определим $f \times g : C \longrightarrow A \times B$, полагая $(f \times g)(a, b) = (f(a), g(b))$. Для любого $c \in C$ выполняются равенства $\mathrm{pr}_1 \circ (f \times g)(\mathrm{c}) = \mathrm{pr}_1(f(c), g(c)) = \mathrm{a(c)}$ и $\mathrm{pr}_2 \circ (f \times g)(c) = \mathrm{pr}_2(f(c), g(c)) = g(c)$. Очевидно, что $f \times g$ является единственным отображением с таким свойством. В самом деле, пусть $h : C \longrightarrow A \times B$ другое отображение, дающее в композиции с первой и второй проекциями f и g, соответственно. Любое отображение $h : C \longrightarrow A \times B$ сопоставляет элементу $c \in C$ пару $(h_1(c), h_2(c))$, $h_1(c) \in A$, $h_2(c) \in B$. Условие на h означает теперь в точности, что $h_1(c) = f(c)$ и $h_2(c) = g(c)$. Таким образом, наивное определение из § 1 является в действительности не определением, а *конструкцией* прямого произведения. Можно придумать много других конструкций прямого произведения, в том числе и не обращающихся к понятию упорядоченных пар.

3. Канонический изоморфизм прямых произведений. Сейчас мы покажем, что универсальное свойство однозначно определяет прямое произведение множеств, с точностью до **единственной** биекции, коммутирующей с каноническими проекциями.

Теорема. *Пусть* C *и* D *– два прямых произведения множеств* A *и* B*, с каноническими проекциями* $\pi_1 : C \longrightarrow A$, $\pi_2 : C \longrightarrow B$ *и* $\rho_1 : D \longrightarrow A$, $\rho_2 : D \longrightarrow B$. *Тогда существует единственная биекция* $\phi : C \longrightarrow D$ *такая, что* $\pi_i = \rho_i \circ \phi$.

Доказательство. Итак, пусть теперь заданы **два** прямых произведения C и D множеств A и B. Тогда согласно универсальному свойству C существует **единственное** отображение $\phi : C \longrightarrow D$ и такое, что $\pi_i = \rho_i \circ \phi$. Совершенно аналогично, согласно универсальному свойству D существует **единственное** отображение $\psi : D \longrightarrow C$ и такое, что $\rho_i = \pi_i \circ \psi$. Таким образом, $\psi \circ \phi : C \longrightarrow C$ обладает тем свойством, что $\pi_i = \pi_i \circ (\psi \circ \phi)$ и, в силу универсального свойства C имеем $\psi \circ \phi = \mathrm{id}$. Точно так же из универсального свойства D вытекает, что $\phi \circ \psi = \mathrm{id}$. Это и означает, что ϕ и ψ являются взаимно обратными биекциями.

Построенные в теореме биекции коммутирующие с проекциями, называются **(каноническими) изоморфизмами** C и D. Поскольку построенное в § 1 наивное прямое произведение $A \times B$ обладает универсальным свойством, любое другое прямое произведение множеств A и B *канонически изоморфно* ему, но вопрос об их *равенстве* абсолютно бессмысленен.

4. Прямое произведение через неупорядоченные пары. Пусть A и B два непересекающихся множества. Тогда легко построить их прямое произведение в терминах *неупорядоченных* пар. В самом деле, положим

$$A \times B = \{\{a, b\} \mid a \in A,\ b \in B\}$$

и определим проекции $A \times B$ на A и B, полагая $\mathrm{pr}_1 : \{a, b\} \mapsto a$ и $\mathrm{pr}_2 : \{a, b\} \mapsto b$, если $a \in A$ и $b \in B$. Заметим, что из того, что A и B дизъюнктны, вытекает, что так описанные проекции pr_1 и pr_2 действительно являются отображениями. Легко видеть, что сопоставление $\{a, b\} \mapsto (a, b)$ устанавливает изоморфизм так определенного прямого произведения с прямым произведением, определенным ранее в терминах упорядоченных пар. Разумеется, тот факт, что сопоставление $\{a, b\} \mapsto (a, b)$ является отображением, снова следует из дизъюнктности A и B.

§ 11. Функторы на категории множеств, 1st installment: ковариантные функторы

Этот параграф явится нашим первым знакомством с одним из ведущих принципов современной математики – функториальностью, которая будет центральной темой Части III. Введем пока понятие функтора на категории множеств и отображений. Начнем с функторов одного аргумента.

1. Ковариантные функторы. Существуют два типа функторов: функторы, сохраняющие направление стрелок, они будут называться **ковариантными** и функторы, обращающие направление стрелок, они будут называться **контравариантными**. Определим вначале ковариантные функторы.

Определение. Ковариантный функтор F *на категории множеств состоит из следующих данных:*

1. *Сопоставления каждому множеству* X *некоторого однозначно определенного множества* $F(X)$*;*

2. *Сопоставление каждому отображению* $f : X \longrightarrow Y$ *некоторого однозначно определенного отображения* $F(f) : F(X) \longrightarrow F(Y)$*;*

подчиненных следующим условиям:

Fun1 *Сохранение тождественного отображения:* $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$*;*

Fun2 *Сохранение композиции:* $F(g \circ f) = F(g) \circ F(f)$ *для любых двух отображений* f *и* g*, для которых определена композиция* $g \circ f$*.*

В частности, аксиома Fun2 утверждает, что композиция $F(g) \circ F(f)$ *определена*, если определена композиция $g \circ f$.

• **Тождественный функтор.** Первый пример ковариантного функтора, который приходит на ум, это **тождественный функтор**, который сопоставляет каждому множеству само это множество, а каждому отображению – само это отображение.

• **Постоянные функторы.** Любое множество Z определяет **постоянный функтор** F на категории множеств. А именно, положим $F(X) = Z$ для любого множества X и $F(f) = \mathrm{id}_Z$ для любого отображения f. Снова выполнение аксиом функтора очевидно.

• **Главные ковариантные функторы.** Оказывается, любое множество Z определяет некоторый гораздо более интересный ковариантный функтор $F = \mathrm{Map}(Z, ?)$ на категории

множеств. А именно, функтор F сопоставляет множеству X множество $\mathrm{Map}(Z,X)$ всех отображений из Z в X, а отображению $f : X \longrightarrow Y$ – отображение $F(f) : F(X) \longrightarrow F(Y)$, такое, что $g \mapsto f \circ g$ для любого $g \in F(X) = \mathrm{Map}(Z,X)$.

Задача. Проверьте, что описанная выше конструкция действительно определяет ковариантный функтор на категории множеств.

§ 12. Функторы на категории множеств, 2nd installment: контравариантные функторы

1. Контравариантные функторы. В отличие от ковариантных функторов контравариантные функторы заменяют направление всех отображений на противоположное.

Определение. Контравариантный функтор *F на категории множеств состоит из следующих данных:*

1. *Сопоставления каждому множеству X некоторого однозначно определенного множества $F(X)$;*

2. *Сопоставление каждому отображению $f : X \longrightarrow Y$ некоторого однозначно определенного отображения $F(f) : F(Y) \longrightarrow F(X)$;*

подчиненных следующим условиям:

Cof1 *Сохранение тождественного отображения: $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$;*

Cof2 *Сохранение композиции: $F(g \circ f) = F(f) \circ F(g)$ для любых двух отображений f и g, для которых определена композиция $g \circ f$.*

В частности, аксиома Fun2 утверждает, что композиция $F(f) \circ F(g)$ *определена*, если определена композиция $g \circ f$. Обратите внимание, что здесь отображению $f : X \longrightarrow Y$ сопоставляется отображение $F(f)$ из $F(Y)$ в $F(X)$, а не из $F(X)$ в $F(Y)$, как в случае ковариантного функтора. Эту мысль выражают, говоря, что F обращает стрелки.

• **Главные контравариантные функторы.** С другой стороны, главные ковариантные функторы имеют столь же важный и интересный контравариантный аналог. А именно, любое множество Z определяет контравариантный функтор $F = \mathrm{Map}(?,Z)$ на категории множеств. Этот функтор F сопоставляет множеству X множество $\mathrm{Map}(X,Z)$ всех отображений из Z в X, а отображению $f : X \longrightarrow Y$ – отображение $F(f) : F(Y) \longrightarrow F(X)$, такое, что $g \mapsto g \circ f$ для любого $g \in F(Y) = \mathrm{Map}(Y,Z)$.

Задача. Проверьте, что описанная выше конструкция действительно определяет контравариантный функтор на категории множеств.

2. Несуществование контравариантного аналога тождественного функтора. Для любого множества Z постоянный функтор является не только ковариантным, но и контравариантным. В то же время для категории множеств нет никакого естественного контравариантного аналога тождественного функтора. Первым кандидатом на эту роль был бы функтор, который сопоставляет каждому множеству X само это множество, а каждому отображению $f : X \longrightarrow Y$ **обратное** отображение $f^{-1} : Y \longrightarrow X$, при этом, очевидно, $\mathrm{id}_X^{-1} = \mathrm{id}_X$ и $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. Однако определить так контравариантный функтор на категории множеств и отображений так вряд ли удастстя, поскольку далеко не всякое отображение имеет обратное *отображение*. На языке теории категорий это выражают говоря, что категория множеств и отображений не изоморфна своей двойственной категории. Как мы увидим в следующей части, этим она решительно отличается от категории множеств и бинарных отношений, которая, как раз, самодвойственна (для каждого отношения есть симметричное отношение.)

§ 13. Функторы на категории множеств, 3rd installment: функтор степени

Сйечас мы обсудим два важнейших функтора, каждый из которых сопоставляет множеству X его булеан 2^X.

• **Контравариантный функтор степени.** Полагая в предшествующем определении $Z = \{0, 1\}$, мы получаем чрезвычайно важный частный случай, заслуживающий специального изучения. А именно, рассмотрим функтор P_-, который сопоставляет каждому множеству X множество 2^X его подмножеств, а каждому отображению $f : X \longrightarrow Y$ отображение $P_-(f) : 2^Y \longrightarrow 2^X$, которое сопоставляет подмножеству $A \subseteq Y$ его прообраз в X относительно f, иными словами, $P_-(f)(A) = f^{-1}(A)$. Так построенный функтор P_- называется **функтором степени** или, если нужна особая точность, **контравариантным функтором степени** на категории множеств. Этот функтор, по существу, является специальным случаем главного контравариантного функтора. В самом деле, характеристическая функция подмножества $P_-(A)$ является композицией f и характеристической функции подмножества A.

• **Ковариантный функтор степени.** Функтор степени допускает естественный ковариантный аналог. А именно, рассмотрим функтор P_+, который сопоставляет каждому множеству X множество 2^X его подмножеств, а каждому отображению $f : X \longrightarrow Y$ отображение $P_+(f) : 2^X \longrightarrow 2^Y$, которое сопоставляет подмножеству $A \subseteq X$ его образ в Y относительно f, иными словами, $P_+(f)(A) = f(A)$. Так построенный функтор P_+ называется **ковариантным функтором степени** на категории множеств.

Предостережение. Стоит отметить, что этот функтор **не является** частным случаем главного ковариантного функтора и обязан своим существованием дополнительной структуре на множестве $\{0, 1\}$, а именно тому, что $\{0, 1\}$ рассматривается как *множество с отмеченной точкой* 0. В самом деле, характеристическая функция $\tilde{\chi}$ подмножества $P_+(A)$ выражается через характеристическую функцию χ подмножества A следующим образом:

$$\tilde{\chi}(y) = \begin{cases} 1 & \exists x \in X,\ f(x) = y \quad \& \quad \chi(x) = 1, \\ 0 & \forall x \in X,\ f(x) = y \implies \chi(x) = 0. \end{cases}$$

Поэтому, говоря просто о *функторе степени* мы будем всегда иметь в виду **контравариантный** функтор степени.

Задача. Каждый из функторов P_-P_-, P_-P_+, P_+P_-, P_+P_+ переводит X в 2^{2^X}. Во что эти функторы переводят $f : X \longrightarrow Y$?

Задача. Можно ли определить контравариантный функтор $\bigwedge_-$ и ковариантный функтор $\bigwedge_+$, сопоставляющие каждому множеству X множество $\bigwedge(X)$ его *конечных* подмножеств?

§ 14. Функторы на категории множеств, 4th installment: функторы двух аргументов

1. Функторы двух аргументов. В действительности нам часто придется рассматривать функторы двух и более аргументов. Такой функтор может быть ковариантным по одним аргументам и контравариантным по другим. Например, функтор двух аргументов может быть ковариантен по обоим аргументам, либо ковариантен по первому аргументу и контравариантен по второму, либо контравариантен по первому аргументу и ковариантен по второму, либо, наконец, контравариантен по обоим аргументам. Мы дадим определение функтора, контравариантного по первому и ковариантного по второму аргументу, для которого у нас есть интересный пример, функтор Map.

Определение. Функтор *F двух аргументов на категории множеств* **контравариантный по первому аргументу и контравариантный по второму** *состоит из следующих данных:*

1. *Сопоставления каждым двум множествам X и Y некоторого однозначно определенного множества $F(X, Y)$;*

2. *Сопоставление каждым двум отображениям $f : X \longrightarrow Y$ и $g : U \longrightarrow V$ некоторого однозначно определенного отображения $F(f, g) : F(Y, U) \longrightarrow F(X, V)$;*

подчиненных следующим условиям:

Bif1 *Сохранение тождественного отображения: $F(\mathrm{id}_X, \mathrm{id}_Y) = \mathrm{id}_{F(X,Y)}$;*

Bif2 *Сохранение композиции: $F(g \circ f, i \circ h) = F(f, i) \circ F(g, h)$ для любых четырех отображений $X \longrightarrow^f Y \longrightarrow^g Z$, $U \longrightarrow^h V \longrightarrow^i W$.*

Некоторые авторы называют функторы, контравариантные по первому и ковариантные по второму аргументу, просто **контра-ко-функторами**). Функторы двух аргументов иногда называются также **бифункторами**. Это название особенно часто употребляется для функторов, *ковариантных по обоим аргументам*. Такие функторы называются еще **дважды ковариантными**, а функторы, контравариантные по обоим аргументам, – **дважды контравариантными**.

Задача. 1. Определить функторы двух аргументов для всех остальных возможных комбинаций ковариантности и контравариантности.

2. Определить функтор трех аргументов, ковариантный по первому аргументу и контравариантный по второму и третьему.

• **Главный бифунктор.** Главный ковариантный функтор и главный контравариантный функтор можно объединить в один функтор двух аргументов, называемый **главным бифунктором**. А именно, Map сопоставляет каждым двум множествам X и Y множество $\mathrm{Map}(X,Y)$ всех отображений из X в Y, а любым двум отображениям $f : X \longrightarrow Y$ и $g : U \longrightarrow V$ – отображение $\mathrm{Map}(f,g) : \mathrm{Map}(Y,U) \longrightarrow \mathrm{Map}(X,V)$, сопоставляющее каждому отображению $h \in \mathrm{Map}(Y,U)$ композицию $g \circ h \circ f \in \mathrm{Map}(X,V)$.

§ 15. Функториальность прямого произведения

На категории множеств и отображений зависимость объединения и пересечения от своих аргументов не является функториальной. В то же время, прямое произведение (как и свободное объединение) является функтором своих аргументов.

1. Объединение и пересечение не являются функторами. Сопоставления $(X,Y) \mapsto X \cup Y$ и $(X,Y) \mapsto X \cap Y$ невозможно естественно доопределить до функторов двух аргументов на категории множеств и *отображений*. Впрочем, как легко видеть, они задают функторы на категории множеств и *отношений*, см. Гл. ?. В самом деле, будем пользоваться обозначениями предыдущего параграфа и записывать $\cup$ и $\cap$ как префиксы, т.е. $\cup(X,Y) = X \cup Y$ и $\cap(X,Y) = X \cap Y$. Пусть теперь $f : X \longrightarrow Y$ и $g : U \longrightarrow V$. Что естественно называть $\cup(f,g)$ и $\cap(f,g)$? Это должны быть некоторые естественно определенные отображения из $X \cup U$ в $Y \cup V$ и из $X \cup U$ в $Y \cup V$, соответственно. Однако такие *отображения* можно определить лишь если ограничения f и g на $X \cap U$ совпадают, т.е. если $f(x) = g(x)$ для любого $x \in X \cap U$, а отнюдь не в общем случае. А именно, отображение $\cap(f,g)$ будет совпадать с ограничением $f|_{X\cap U} = g|_{X\cap U}$, а отображение $\cup(f,g)$ – со склейкой $f \cup g$, определенной посредством

$$f \cup g(x) = \begin{cases} f(x) & x \in X, \\ g(x) & x \in U. \end{cases}$$

Это определение корректно лишь потому, что ограничения f и g на $X \cap U$ совпадают.

2. Функториальность прямого произведения. В отличие от объединения и пересечения, прямое произведение $\prod$ является дважды контравариантным функтором. Это значит, что если положить $\prod(X,Y) = X \times Y$, то любым двум отображениям $f : X \longrightarrow U$ и $g : Y \longrightarrow V$ можно осмысленным образом сопоставить некоторое отображение $f \times g : X \times Y \longrightarrow U \times V$ так, чтобы при этом выполнялись аксиомы функтора. Достаточно задать значение отображения $f \times g$ на всей парах (x,y), $x \in X$, $y \in Y$. Полагая $(f \times g)(x,y) = (f(x), g(y))$ мы действительно получим отображение из $\mathrm{Map}(X \times Y, U \times V)$.

Задача. Проверьте, что изложенная выше конструкция задает дважды ковариантный функтор на категории множеств.

Предостережение. Построенное в предыдущем пункте отображение $f \times g$ не следует путать с отображением (f,g), фигурировавшим в определении прямого произведения. На самом деле (f,g) – отображение, зависящее от *одного* аргумента, $(f,g)(z) = (f(z), g(z))$, в то время как $f \times g$ – отображение, зависящее от *двух* аргументов, $(f \times g)(x,y) = (f(x), g(y))$. Впрочем, они тесно связаны между собой, а именно, отображение (f,g) естественно истолковывается как композиция **диагонального отображения** $Z \longrightarrow Z \times Z$, $z \mapsto (z,z)$ с отображением $f \times g$.

3. Функторы одного аргумента. Замораживая один из аргументов в прямом произведении мы получаем ковариантные функторы одного аргумента $? \times X$ и $X \times ?$. Так как в силу коммутативности прямого произведения они будут канонически изоморфны (как функторы,

см. Главу 9), достаточно рассмотреть первый из них. Включим отображение $f : Y \longrightarrow Z$ в коммутативный квадрат:

$$\begin{array}{ccc} Y \times Z & \xrightarrow{f\times \mathrm{id}} & Z \times X \\ {\scriptstyle \mathrm{pr}_1}\downarrow & & \downarrow{\scriptstyle \mathrm{pr}_1} \\ Y & \xrightarrow[f]{} & Z \end{array}$$

Что можно сказать о связи инъективности и сюръективности f и $f \times \mathrm{id}$.

§ 16. Метрические пространства

Основной принцип теории возмущений состоит в том, что введение небольшого дополнительного возмущения, нарушающего симметрию исходной задачи, позволяет различать вещи, которые в исходной постановке казались идентичными. Категория множеств *слишком* проста, чтобы в ней можно было ясно видеть **все** аспекты категорных конструкций. В настоящем параграфе мы введем небольшое дополнительное возмущение: перейдем от категории множеств к категории метрических пространств.

1. Метрические пространства. Напомним, что **метрическим пространством** называется множество X вместе с отображением $d : X \times X \longrightarrow \mathbb{R}$, называемым обычно **расстоянием** или **метрикой**, удовлетворяющим следующим свойствам:

MS1 **положительность** $d(x, y) \geq 0$, причем $d(x, y) = 0$ в том и только том случае, когда $x = y$;

MS2 **симметричность** $d(x, y) = d(y, x)$;

MS3 **неравенство треугольника** $d(x, z) \leq d(x, y) + \delta(y, z)$.

Большинство рассматриваемых в алгебре метрических пространств, в действительности являются **ультраметрическими**, т.е. вместо неравенства треугольника они удовлетворяют более сильному **ультраметрическому неравенству**:

$$d(x, z) \leq \max(d(x, y), d(y, z)).$$

2. Морфизмы метрических пространств. В *элементарных* учебниках анализа, даже достаточно продвинутых[182], в качестве морфизмов метрических пространств обычно рассматриваются **сжимающие отображения**. Напомним, что отображение $f : X \longrightarrow Y$, где (X, d_X), (Y, d_Y) два метрических пространства, называется **сжимающим**, если

$$d_Y(f(x), f(y)) \leq d_X(x, y)$$

для любых $x, y \in X$. В этом случае изоморфизмами будут **изометрии**, т.е. такие биективные отображения, что $d_Y(f(x), f(y)) = d_X(x, y)$ для любых $x, y \in X$. С другой стороны, в топологии, говоря об эквивалентных метриках на X, обычно имеют в виду, что они задают на X одну и ту же топологию (в этом случае морфизмы – это просто непрерывные отображения).

Однако в алгебре принято рассматривать категорию метрических пространств с запасом морфизмов *гораздо* большим, чем сжимающие отображения, и *гораздо* меньшим, чем непрерывные отображения. А именно, в качестве морфизмов метрических пространств обычно принимаются **липшицевы отображения**. Напомним, что $f : X \longrightarrow Y$, называется **липшицевым**, с константой $c \in \mathbb{R}_+$, если

$$d_Y(f(x), f(y)) \leq c d_X(x, y)$$

для любых $x, y \in X$. Таким образом, сжимающее отображение – это в точности Липшицево отображение с константой $c = 1$. В этом случае изоморфизмами будут **билипшицевы отображения**, т.е. такие биективные отображения, для которых существуют константы $c_1, c_2 \in \mathbb{R}_+$ такие, что

$$c_1 d_X(x, y) \leq d_Y(f(x), f(y)) \leq c_2 d_X(x, y)$$

[182] А.Н.Колмогоров, С.В.Фомин, Элементы теории функций и функционального анализа. – М., Наука, 1976.

для любых $x, y \in X$.

Замечание. *Профессиональные* аналисты обычно рассматривают категорию метрических пространств с еще более широким запасом морфизмов. А именно, говорят, что отображение $f : X \longrightarrow Y$ удовлетворяет **условию Гельдера порядка** α, $0 < \alpha \leq 1$, если существует такая константа $c \in \mathbb{R}_+$, что

$$d_Y(f(x), f(y)) \leq c d_X(x, y)^\alpha$$

для любых $x, y \in X$. Условие Гельдера порядка $\alpha > 1$ не представляет интереса, так как определяет слишком сильно сжимающие отображения. Например, не существует никаких гельдеровых функций $f : \mathbb{R} \longrightarrow \mathbb{R}$ порядка $\alpha > 1$, кроме постоянных[183].

3. Прямое произведение метрических пространств. В соответствии с общим определением прямое произведение метрических пространств (X, d_X) и (Y, d_Y) – это такое метрическое пространство (Z, d_Z), вместе с липшицевыми отображениями $\pi_1 : Z \longrightarrow X$, $\pi_2 : Z \longrightarrow Y$, что для любого метрического пространства (W, d_W) и любых липшицевых отображений $f : W \longrightarrow X$, $g : W \longrightarrow Y$, существует единственное липшицево отображение $h : W \longrightarrow Z$, такое, что $f = \pi_X \circ h$, $g = \pi_2 \circ h$.

Ясно, что $Z = X \times Y$ как множество, но как ввести метрику на $X \times Y$ так, чтобы отображение $(f, g)(w) = (f(w), g(w))$ стало липшицевым? Можно, например, определить на $X \times Y$ **метрику Чебышева**:

$$d^\infty_{X\times Y}((x_1, y_1), (x_2, y_2)) = \max(d_X(x_1, x_2), d_Y(y_1, y_2)),$$

тогда (f, g) липшицево с константой $\max(c(f), c(g))$.

Для разнообразия можно положить

$$d^1_{X\times Y}((x_1, y_1), (x_2, y_2)) = d_X(x_1, x_2) + d_Y(y_1, y_2),$$

тогда (f, g) липшицево с константой $c(f) + c(g)$ Это так называемая **городская метрика** (taxicab metric).

Можно, наконец, определить расстояние эвклидовым образом

$$d^2_{X\times Y}((x_1, y_1), (x_2, y_2)) = \sqrt{d_X(x_1, x_2)^2 + d_Y(y_1, y_2)^2},$$

тогда (f, g) липшицево с константой $\sqrt{c(f)^2 + c(g)^2}$.

Однако в действительности, **любая** из этих метрик (и множество других) определяют на $X \times Y$ структуру прямого произведения в категории метрических пространств. Таким образом, ни о какой 'единственности' прямого произведения 'на самом деле' здесь не может идти речи. Ясно, что в категории метрических пространств и гельдеровых отображений существует еще больше возможностей выбора метрики на $X \times Y$.

§ 17. Прямое произведение произвольных семейств

В настоящем параграфе мы обобщим понятие прямого произведения на случай произвольного семейства множеств. Эта конструкция предполагает знакомство с понятием отображения. Кроме того, непустота бесконечных произведений непустых множеств уже совершенно не является очевидной и гарантируется *только* аксиомой выбора.

1. Наивное определение. Пусть теперь $\{X_i, i \in I\}$ – любое семейство множеств, где I некоторое множество индексов.

[183] Лоран Шварц, Анализ, т.1, М., Мир, 1972. – с.87.

Определение. Прямое произведение $\prod X_i$, $i \in I$, *семейства* $\{X_i\}_{i\in I}$ *определяется как множество всех отображений* $f : I \longrightarrow \cup X_i$, *таких, что* $f_i = f(i) \in X_i$.

В частности, если все множества X_i равны между собой – мы обозначим их общее значение через X, то произведение такого семейства есть в точности множество $X^I = \mathrm{Map}(I, X)$ всех отображений из I в X.

Произведение пустого семейства. Отметим предельный случай пустого семейства, который реально возникнет при исследовании алгебраических операций в Разделе 4. В этом случае как множество индексов I, так и обьединение семейства пусты. Ясно, что существует ровно одно отображение из пустого множества в любое множество, а именно **пустое отображение** (график которого пуст). Тем самым произведение пустого семейства есть одноэлементное множество $\varnothing$. В частности, для любого непустого множества X имеем $X^0 = \varnothing$ (единственный элемент этого множества можно еще интерпретировать как 0-ку ('**нульку**') элементов '$\Lambda = ()$').

2. Мультипликативная аксиома. Ясно, что если хотя бы одно из множеств X_i пусто, то произведение $\prod X_i$ также пусто. Обратное утверждение не столь очевидно. Оно называется называется **аксиомой выбора в мультипликативной форме**, **аксиомой выбора в форме Рассела** или просто **мультипликативной аксиомой**. В действительности отсюда сразу вытекает, что тогда в множестве $\prod X_i$ довольно много элементов.

ZF8 (Мультипликативная форма аксиомы выбора). *Декартово произведение любого семейства непустых множеств непусто.*

Очевидно, что это утверждение является переформулировкой аксиомы выбора. Если $\prod X_i \neq \varnothing$ и $(x_i) \in \prod X_i$ какой-то элемент этого множества, то $f : I \longrightarrow \cup X_i$, $i \mapsto a_i$ является функцией выбора и обратно, если $f : I \longrightarrow \cup X_i$ – какая-то функция выбора, то $(f(i))$ – элемент прямого произведения $\prod X_i$.

§ 18. Прямое произведение множеств с отмеченной точкой

Большинство рассматриваемых в алгебре объектов имеет выделенный элемент, обычно это нейтральный элемент некоторой алгебраической операции, скажем, 0 или 1. Для таких объектов понятие прямого произведения обладает замечательными особенностями, которые мы рассмотрим в этом и следующем параграфах.

1. Множества с отмеченной точкой. Сейчас мы определим объекты, который с точки зрения общей алгебры является множествами с одной **нульарной** операцией. Удивительно, какая богатая комбинаторная структура скрывается за этим непритязательным понятием.

Определение. *Пара* $(A, *_A)$, *состоящая из множества* A *и элемента* $* = *_A \in A$, *называется* **множеством с отмеченной точкой**.

Часто, допуская вольность речи, множество с отмеченной точкой обозначают одной буквой A, однако это не должно вводить в заблуждение: поведение множеств с отмеченной точкой радикально отличается от поведения множеств. В действительности, оно естественно описывается в теоретико-категорных, а вовсе не в теоретико-множественных терминах.

Множество с отмеченной точкой всегда не пусто, так как оно содержит по крайней мере один элемент – саму отмеченную точку. Совершенно особую во всей теории играют одноэлементные множества, состоящие лишь из отмеченной точки, такое множество обычно обозначается через $\{*\}$. Для множеств с отмеченной точкой невозможно разумно определить булевы операции объединения и пересечения, так как непонятно, что следует считать отмеченной точкой в объединении или пересечении двух множеств с отмеченной точкой. Эти операции имеют смысл лишь для множеств с *общей* отмеченной точкой).

2. Морфизмы множеств с отмеченной точкой. Для множеств с отмеченной точкой имеет смысл рассматривать не любые отображения, а лишь такие, которые переводят отмеченную точку в отмеченную точку.

Определение. *Пусть* $(A, *_A)$ *и* $(B, *_B)$ *– два множества с отмеченной точкой. Отображение* $f : A \longrightarrow B$ *называется* **морфизмом** *множеств с отмеченной точкой, если* $f(*_B) = *_B$.

Задача. Убедитесь, что тождественное отображение, композиция двух морфизмов и отображение, обратное к биективному морфизму множеств с отмеченной точкой, сами являются морфизмами множеств с отмеченной точкой.

Особая роль множества $\{*\}$ связана с тем, что для любого множества с отмеченной точкой A существует единственный морфизм $A \longrightarrow \{*\}$ и единственный морфизм $\{*\} \longrightarrow A$. На языке теории категорий это означает, что $\{*\}$ является **нулевым объектом** категории множеств с отмеченной точкой

3. Прямое произведение множеств с отмеченной точкой. В § 1 и § 3 мы дали два определения прямого произведения множеств. Каждое из них легко обобщить на множества с отмеченной точкой.

Наивное определение. Прямым произведением *двух множеств с отмеченной точкой* $(A, *_A)$ *и* $(B, *_B)$ *называется множество с отмеченной точкой* $(A \times B, (*_A, *_B))$.

В дальнейшем пара $(*_A, *_B)$ будет обозначаться через $*_{A\times B}$. Очевидно, что канонические проекции pr_1 и pr_2 являются морфизмами множеств с отмеченной точкой, т.е. $\mathrm{pr}_1(*_{A\times B}) = *_A$ и $\mathrm{pr}_2(*_{A\times B}) = *_B$.

Категорное определение. *Пусть* A *и* B *– два множества с отмеченной точкой. Их* **прямым произведением** *называется множество с отмеченной точкой* $A \times B$ *вместе с морфизмами* $\mathrm{pr}_1 : A \times B \longrightarrow A$, $\mathrm{pr}_2 : A \times B \longrightarrow B$, *называемыми* **каноническими проекциями** $A \times B$ *на первый и второй множитель, удовлетворяющее следующему* **универсальному свойству***:*

Для любого множества с отмеченной точкой C *и любых морфизмов* $f : C \longrightarrow A$ *и* $g : C \longrightarrow B$ *существует единственный морфизм* $f \times g : C \longrightarrow A \times B$ *такой, что* $f = \mathrm{pr}_1 \circ (f \times g)$ *и* $g = \mathrm{pr}_2 \circ (f \times g)$.

Задача. Докажите, что наивное прямое произведение множеств с отмеченной точкой удовлетворяет универсальному свойству и, тем самым, является их категорным прямым произведением.

Задача. Докажите, что любые два прямых произведения канонически изоморфны, т.е. если C и D – два прямых произведения множеств с отмеченной точкой A и B, то существует единственный обратимый морфизм множеств с отмеченной точкой $C \longrightarrow D$, коммутирующий с каноническими проекциями.

4. Канонические вложения. Для прямого произведения множеств имеются канонические проекции $\mathrm{pr}_1 : A \times B \longrightarrow A$ и $\mathrm{pr}_2 : A \times B \longrightarrow B$, но нет, вообще говоря, никакого естественного способа определить *вложения* $\iota_1 : A \longrightarrow A \times B$ и $\iota_2 : B \longrightarrow A \times B$. Для множеств с отмеченной точкой такой способ есть.

Определение. *Пусть* A *и* B *– два множества с отмеченной точкой. Морфизмы* $\iota_1 : A \longrightarrow A \times B$, $a \mapsto (a, *_B)$ *и* $\iota_2 : B \longrightarrow A \times B$, $b \mapsto (*_A, b)$ *называются* **каноническими вложениями** *сомножителей* A *и* B *в прямое произведение.*

Задача. Убедитесь, что $\mathrm{pr}_1 \circ \iota_1 = \mathrm{id}_A$ и $\mathrm{pr}_2 \circ \iota_2 = \mathrm{id}_B$.

5. Прямые суммы. Забегая вперед, отметим, что для многих важнейших категорий (абелевы группы, векторные пространства, R-модули, кольца) произведение $A \times B$ вместе с только что построенными каноническими вложениями ι_1 и ι_2 удовлетворяет универсальному свойству, двойственному к универсальному свойству прямого произведения (во всех перечисленных выше примерах отмеченной точкой в A является 0_A). Иначе говоря, в этих случаях $A \times B$ является **одновременно** и произведением и копроизведением A и B. В этих случаях $A \times B$ обычно называется **прямой суммой** A и B и обозначается $A \oplus B$. Однако произведение $A \times B$ **не является** копроизведением в категории множеств с отмеченной точкой, поэтому

мы не будем говорить о нем как о прямой сумме, тем не менее, возможность естественно вкладывать A и B в $A \times B$ играет важную роль. Копроизведением множеств с отмеченной точкой является букетное произведение, которое мы рассмотрим в § 21.

Задача. Обобщите все содержание этого параграфа на случай i) произведений конечного числа множеств с отмеченной точкой, ii) произведений произвольного семейства множеств с отмеченной точкой.

§ 19. Ограниченное прямое произведение

Здесь мы рассмотрим очень важный вариант прямого произведения относящийся к случаю *бесконечных* семейств **пар множеств**. В случае множеств с отмеченной точкой эта конструкция является одной из центральных конструкций алгебры – конструкцией слабого прямого произведения/прямой суммы. Конструкция ограниченного прямого произведения является одной из основных в теории чисел, где при помощи нее строятся адели и идели.

1. Ограниченное прямое произведение пар множеств. Мы будем называть **парами множеств** такие пары (A, B), для которых $B \subseteq A$ ('множество с выделенным подмножеством'). Если (A_1, B_1) и (A_2, B_2) – две пары множеств, то **морфизмом** (A_1, B_1) в (A_2, B_2) называется такое отображение $f : A_1 \longrightarrow A_2$, что $f(B_1) \subseteq B_2$.

Напомним, что когда мы говорим, что какое-то свойство выполняется для **почти всех** элементов $i \in I$ некоторого множества, это означает, что свойство выполняется для всех $i \in I$, **кроме конечного их числа**. Например, утверждения "почти все планеты во Вселенной необитаемы" и "почти все планеты во Вселенной населены мыслящими существами" не противоречат друг другу. Рассмотрим произвольное семейство пар (A_i, B_i), $i \in I$.

Определение. *Положим*

$$\prod\nolimits_{B_i} A_i = \left\{(a_i) \in \prod A_i \mid a_i \in B_i \text{ для почти всех } i \in I\right\},$$

где все произведения берутся по $i \in I$. Пара $\left(\prod_{B_i} A_i, \prod B_i\right)$ называется **ограниченным прямым произведением** *семейства (A_i, B_i), $i \in I$.*

Существование ограниченного прямого произведения сразу следует из существования прямого произведения и аксиомы подмножеств. Ограничения канонических проекций pr_i с $\prod A_i$ на $\prod_{B_i} A_i$ по прежнему обозначаются через pr_i. Ясно, что если множество индексов I конечно, то $\prod_{B_i} A_i = \prod A_i$, поэтому эта конструкция отличается от конструкции прямого произведения лишь для бесконечного числа сомножителей.

2. Ограниченное прямое произведение множеств с отмеченной точкой. Множества с отмеченной точкой можно рассматривать как частный случай пар множеств, если сопоставить такому множеству $(A, *_A)$ пару $(A, \{*_A\})$. Получающийся при этом случай ограниченных прямых произведений особенно важен. Итак, пусть A_i, $i \in I$, – произвольное семейство множеств с отмеченной точкой. Множество

$$\prod\nolimits^* A_i = \left\{(a_i) \in \prod A_i \mid a_i = *_{A_i} \text{ для почти всех } i \in I\right\},$$

с отмеченной точкой $(*_{A_i})_{i \in I}$ называется ограниченным прямым произведением семейства A_i. Для большинства конкретных ситуаций, в которых мы будем использовать эту конструкцию, ограниченное прямое произведение будет называться **прямой суммой** A_i и обозначаться $\bigoplus A_i$, но по причинам, которые мы объяснили в предыдущем параграфе, мы воздерживаемся от того, чтобы использовать это название в общем случае.

Сейчас мы убедимся, что ограниченное прямое произведение **намного** меньше прямого произведения. В следующей задаче предполагается, что читатель уже владеет содержанием § ? и ? Главы 6.

Задача. Пусть $I = \mathbb{N}$, а все $A_i = \mathbb{Z}$, причем $\mathbb{Z}$ рассматривается как множество с выделенной точкой 0. Проверьте, что $\prod^* A_i$ счетно, в то время как $\prod A_i$ имеет мощность континуума.

§ 20. Свободное объединение

В этом параграфе мы рассмотрим операцию свободного объединения множеств, двойственную к операции прямого произведения.

1. Наивное определение свободного объединения. Следующее утверждение позволяет провести явную конструкцию свободного объединения двух множеств.

Лемма. *Для двух произвольных множеств A и B существуют такие множества A' и B', что $A \cong A'$, $B \cong B'$ и $A' \cap B' = \varnothing$.*

Доказательство. Возьмем две различные вещи a и b, например, $a = \varnothing$ и $b = \{\varnothing\}$ и положим $A' = \{a\} \times A$ и $B' = \{b\} \times B$. Тогда отображения $A \longrightarrow A'$, $x \mapsto (a, x)$ и $B \longrightarrow B'$, $y \mapsto (b, y)$ устанавливают биекцию между A и A' и между B и B', соответственно. С другой стороны, $A' \cap B' = \varnothing$ так как из $(a, x) = (b, y)$ для некоторых $x \in A$ и $y \in B$ следовало бы, что $a = b$ и $x = y$.

Пусть A и B – любые множества. Согласно доказательству Леммы множества упорядоченных пар $A' = \{(x, 1) \mid x \in A\}$ и $B' = \{(y, 2) \mid y \in B\}$ дизъюнктны.

Определение. *Объединение $A' \cup B'$ по-прежнему называется* **свободным объединением** *множеств A и B и обозначается $A \coprod B$.*

Свободное объединение множеств называется также их **копроизведением**, **свободной суммой** или (обычно в топологии) **несвязной суммой** или просто **суммой**. Знак $\coprod$, называется знаком копроизведения, а его TEXническое название `\coprod`. Эта операция легко обобщается на любое конечное число слагаемых. Например, вместо $X_1 \times \ldots \times X_n$ обычно пишут $\coprod\limits_{i=1}^{n} X_i$.

Задача. Докажите, что i) $A \coprod B \cong B \coprod A$, ii) $(A \coprod B) \coprod C \cong A \coprod (B \coprod C)$.

2. Универсальное свойство свободного объединения. Отображения $\iota_1 : A \longrightarrow A \coprod B$, $a \mapsto (a, 1)$ и $\iota_2 : B \longrightarrow A \coprod B$, $b \mapsto (b, 2)$ называются **каноническими вложениями** множеств A и B в $A \coprod B$. Они действительно являются вложениями, причем их образы в $A \coprod B$ дизъюнктны. Как и в случае прямых произведений, в действительности свободное объединение является не просто множеством $A \coprod B$, а множеством $A \coprod B$ **вместе с** каноническими вложениями ι_1, ι_2. В действительности свободное объединения полностью характеризуется универсальным свойством, двойственным универсальному свойству прямого произведения.

Определение. Свободным объединением *двух множеств A и B называется множество $A \coprod B$ вместе с отображениями $\iota_1 : A \longrightarrow A \coprod B$ и $\iota_2 : B \longrightarrow A \coprod B$, называемыми* **каноническими вложениями** *первого и второго слагаемого в $A \coprod B$, удовлетворяющее следующему* **универсальному свойству**. *Для любого множества C и любых отображений $f : A \longrightarrow C$ и $g : B \longrightarrow C$*

$$\begin{array}{ccc} A \coprod B & \xleftarrow{\iota_1} & A \\ {\scriptstyle \iota_2}\uparrow & & \downarrow{\scriptstyle f} \\ B & \xrightarrow[g]{} & C \end{array}$$

существует единственное отображение $f \uplus g : A \coprod B \longrightarrow C$ *такое, что* $f = (f \uplus g) \circ \iota_1$ *и* $g = (f \uplus g) \circ \iota_2$.

3. Свободные объединения произвольных семейств. Эта конструкция легко обобщается на случай любого семейства $\Omega = \{A_i, i \in I\}$, в этом случае свободное объединение обозначается обычно $\coprod A_i$, $i \in I$. Один из часто используемых способов определить копроизведение состоит в том, чтобы положить

$$\coprod_{i\in I} A_i = \bigcup_{i\in I} A_i \times \{i\}.$$

Предостережение. В большинстве наиболее употребительных *конкретных* категорий прямое произведение объектов *как множество* совпадает с теоретико-множественным прямым произведением. В то же время копроизведение, даже если оно существует, принимает самые различные обличия и *крайне редко* совпадает с несвязной суммой. Так, в категории множеств с отмеченной точкой копроизведение это **букетное произведение**, в категориях абелевых групп и модулей это **прямая сумма**, в категории всех групп это **свободное произведение**, в категории алгебр это **тензорное произведение** и т.д. Вот *для разнообразия* пример категории, где копроизведение все же совпадает с несвязным объединением: категория частично упорядоченных множеств, где копроизведением является **кардинальная сумма**.

4. Правило суммы. Если множества A и B конечны, причем A содержит m элементов, а B содержит n элементов, то множество $A \coprod B$ тоже конечно и содержит $m+n$ элементов. Вообще, для любых двух множеств A и B мощность их свободного объединения $A \times B$ равна **сумме** мощностей множеств A и B, $|A \coprod B| = |A| + |B|$.

§ 21 Букетное произведение множеств с отмеченной точкой

Сейчас, чтобы показать, что копроизведение гораздо более деликатная операция, чем произведение, мы построим копроизведение в категории множеств с отмеченной точкой. Эта конструкция очень часто используется в топологии.

1. Букетное произведение. Пусть теперь A и B – два множества с отмеченной точкой.

Определение. *Букетным произведением* $A \vee B$ *множеств* A *и* B *с отмеченной точкой называется их амальгамированная сумма* $A \coprod_C B$ *под одноэлементным множеством* $C = \{*\}$.

Чтобы $A \coprod_C B$ было множеством с отмеченной точкой, отображения f и g здесь должны быть морфизмами множеств с отмеченной точкой и, поэтому определены однозначно: $f(*) = *_A \in A$, $g(*) = *_B \in B$. Тогда $A \coprod_C B$ представляет собой фактор $A \coprod B$ по отношению эквивалентности, все классы которого одноэлементны, за исключением ровно одного двухэлементного класса $\{(*_A, 1), (*_B, 2)\}$, который и является отмеченной точкой фактор-множества $A \coprod B/\sim_C$. Таким образом, $A \coprod_C B$ можно представлять себе как свободное объединение множеств A и B, в котором отмеченная точка $*_A \in A$ отождествлена с отмеченной точкой $*_B \in B$. Примеры букетных произведений.

Задача. Нарисуйте букетное произведение i) двух окружностей, ii) двух отрезков, выделенные точки которых являются их серединами.

2. Вложение букетного произведения в прямое произведение. Заметим, что букетное произведение множеств с отмеченной точкой может быть естественным образом реализовано не только как *фактор-множество* свободного объединения соответствующих множеств, но и как *подмножество* их прямого произведения. А именно, букетное произведение A и B проще всего представлять себе как

$$A \vee B = \{(a, *_B) \in A \times B \mid a \in A\} \cup \{(*_A, b) \in A \times B \mid b \in B\}.$$

Совершенно ясно, что два множества, объединение которых рассматривается в правой части, пересекаются ровно по одному элементу, а именно, по $(*_A, *_B)$.

3. Смятое произведение множеств с отмеченной точкой. Смятым произведением (smash product) множеств с отмеченной точкой A и B называется фактор-множество $A\sharp B = A\times B/\sim$ их прямого произведения $A\times B$ по наименьшему отношению эквивалентности $\sim$, для которого все элементы $A \vee B$ попадают в один класс. Это отношение эквивалентности определяется следующим образом: $(a_1, b_1) \sim (a_2, b_2)$, в том и только том случае, когда $(a_1, b_1) = (a_2, b_2)$ или $(a_1, b_1), (a_2, b_2) \in A \vee B$. Смятое произведение довольно интересная операция.

Задача. Убедитесь, что $S^1\sharp S^1 \cong S^2$.

§ 22. Расслоенное произведение

В настоящем параграфе мы построим очень широкое обобщение понятия прямого произведения двух множеств. А именно, мы введем понятие расслоенного произведения, которое является *совместным* обобщением таких понятий, как пересечение, прямое произведение, график функции, полный прообраз, уравнитель и т.д.

1. Наивное определение расслоенного произведения. Предположим, что нам заданы два отображения $f : A \longrightarrow C$ и $g : B \longrightarrow C$.

Определение. Расслоенное произведение A *и* B **над** C *может быть определено как множество*

$$A \times_C B = \{(a, b) \in A \times B \mid f(a) = g(b)\}.$$

Расслоенное произведение часто называется также **коамальгамой** или **пуллбэком** (pull-back) множеств A и B над C. Сразу отметим три важных обстоятельства:

• Конечно, на самом деле расслоенное произведение зависит не только от множеств A, B, C, но и от отображений f и g. Однако во всех случаях, когда мы будем его использовать, эти отображения будут явно определяться контекстом.

• Как и в случае прямого произведения, расслоенное произведение – это не просто множество $A \times_C B$, а множество $A \times_C B$ **вместе с** парой канонических проекций $\pi_1 : A \times_C B \longrightarrow A$ и $\pi_2 : A \times_C B \longrightarrow B$, являющихся ограничениями канонических проекций pr_1 и pr_2.

• Так как прямые произведения существуют, существование расслоенных произведений гарантируется аксиомой подмножеств.

2. Частные случаи расслоенного произведения. Сейчас мы покажем, что обычные прямые произведения, пересечения, графики отображений и полные прообразы точек все могут быть истолкованы как частные случаи операции расслоенного произведения.

• **Прямое произведение.** Рассмотрим случай, когда $C = \{*\}$ состоит из одной точки. В этом случае существует единственная возможность как для f, так и для g, причем $f(a) = g(b) = \{*\}$ для любых $a \in A$ и $b \in B$. Таким образом, в этом случае $A \times_C B = A \times B$.

• **Пересечение.** Пусть $C = A \cup B$, а f и g – естественные вложения A и B в $A \cup B$, соответственно. Тогда $A\times_C B$ состоит из тех пар (a, b), для которых $a = b$, т.е. **канонически изоморфно** пересечению $A \cap B$ (изоморфизм задается посредством $(a, a) \mapsto a$).

• **График отображения.** Пусть $C = B$, f – произвольное отображение, а $g = \mathrm{id}_B$ – тождественное отображение. Тогда $A \times_B B$ – это в точности множество тех пар (a, b), для которых $f(a) = b$, т.е. график отображения f.

• **Полный прообраз точки относительно отображения.** В этом подпункте мы слегка изменим обозначения и будем обозначать через B то, что мы раньше обозначали через C, а через f – произвольное отображение $A \longrightarrow B$. Пусть, кроме того, $g : \{*\} \longrightarrow B$ – отображение, переводящее $*$ в b_0. Тогда $A \times B\{*\}$ состоит из всех пар $(a, *)$, для которых $f(a) = g(*) = b_0$. Таким образом $A \times B\{*\}$ **канонически изоморфно** полному прообразу $f^{-1}(b_0)$ точки b_0 (изоморфизм задается посредством $(a, *) \mapsto a$).

Задача. Пусть $A = B$. Верно ли, что $A \times_C A$ находится в биективном соответствии с $\mathrm{Eq}(f, g)$?

Решение. Нет, в действительности эквалайзер соответствует $A \times_{A\times C} A$, где отображения A в $A \times C$ задаются, *например*, следующим образом: $(\mathrm{id}, f), (\mathrm{id}, g) : A \longrightarrow A \times C$. Какие еще пары отображений A в $A \times C$ можно здесь рассматривать?

3. Декартовы квадраты. Дадим теперь правильное определение расслоенного произведения в терминах универсального свойства. Квадрат

$$\begin{array}{ccc} D & \xrightarrow{\pi_1} & A \\ {\scriptstyle \pi_2}\downarrow & & \downarrow{\scriptstyle f} \\ B & \xrightarrow[g]{} & C \end{array}$$

называется **декартовым квадратом** (часто говорят также **универсальным квадратом**), если он коммутативен и для любого коммутативного квадрата

$$\begin{array}{ccc} X & \xrightarrow{\theta_1} & A \\ {\scriptstyle \theta_2}\downarrow & & \downarrow{\scriptstyle f} \\ B & \xrightarrow[g]{} & C \end{array}$$

существует единственное отображение $\eta : X \longrightarrow D$ такое, что $\theta_1 = \pi_1 \circ \eta$ и $\theta_2 = \pi_2 \circ \eta$. Так вот, **расслоенное произведение** A и B над C это *в точности* множество $A \times_C B$ *вместе с отображениями* $\pi_1 : A \times_C B \longrightarrow A$, $\pi_2 : A \times_C B \longrightarrow B$, для которого квадрат

$$\begin{array}{ccc} A \times_C B & \xrightarrow{\pi_1} & A \\ {\scriptstyle \pi_2}\downarrow & & \downarrow{\scriptstyle f} \\ B & \xrightarrow[g]{} & C \end{array}$$

является декартовым. Автор оставляет читателю самостоятельно сформулировать (и доказать!) все относящиеся сюда утверждения, которые полностью параллельны тому, что мы доказывали для декартовых произведений.

Задача. Докажите, что если в декартовом квадрате отображение π_2 тоже является инъекцией/сюръекцией то отображение π_2 тоже является инъекцией/сюръекцией. Ясно, что f и π_2 здесь можно заменить на g и π_1, а вот верна ли обратная импликация: если π_2 является инъекцией/сюръекцией, то f тоже является инъекцией/сюръекцией.

Предостережение. Здесь самым существенным образом использована специфика теории множеств. В общем случае инъекции здесь можно заменить на мономорфизмы, но не на эпиморфизмы. То, что это так для множеств, связано исключительно с тем обстоятельством, что в категории множеств эпиморфизм является ретракцией (аксиома выбора!)

Обобзим теперь пример с полным прообразом точки.

Задача. Пусть $B \subseteq C$, $D \subseteq A$. Покажите, что

$$\begin{array}{ccc} D & \xrightarrow{\hookrightarrow} & A \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle f} \\ B & \xrightarrow[\hookrightarrow]{} & C \end{array}$$

в том и только том случае является декартовым квадратом (т.е. $D = A \times_C B$), когда $D = f^{-1}(B)$ и $h = f|D$.

§ 23. Амальгамированная сумма

В настоящем параграфе мы рассмотрим конструкцию амальгамированной суммы, двойственную к конструкции расслоенного произведения. Амальгамированые суммы являются

очень широким совместным обобщением свободных объединений, объединений, коуравнителей и т.д.

1. Наивное определение амальгамированной суммы. Амальгамированная сумма представляет собой понятие двойственное к понятию расслоенного произведения. Таким образом, достаточно заменить во всех определениях и примерах направление всех отображений на противоположеное и поменять местами прямые произведения и свободные объединения, объединения и пересечения, подмножества и фактор-множества и т.д. Итак, начнем с того, что зададим отображения $f : C \longrightarrow A$ и $g : C \longrightarrow B$. Расслоенное произведение было *подмножеством* прямого произведения $A \times B$. Это значит, что амальгамированная сумма должна быть *фактор-множеством* свободного объединения $A \coprod B$.

Определение. Амальгамированная сумма A *и* B **под** C *может быть определена как фактор-множество их свободного объединения* $A \coprod B$ *по наименьшему отношению эквивалентности* $\sim_C$ *такому, что для каждого* $c \in C$ *выполняется* $f(c) \sim_C g(c)$.

Амальгамированная сумма иногда называется также **амальгамой**, **расслоенным произведением**, **расслоенной суммой** или **пушаутом** (push-out) множеств A и B под C. К амальгамированным произведениям применимо все, что мы сказали о расслоенных произведениях:

• Как и в случае расслоенных произведений, амальгамированная сумма зависит не только от множеств A, B, C, но и от отображений f и g.

• Снова амальгамированная сумма – это не просто множество $A \times_C B$, а множество $A \times_C B$ **вместе с** парой канонических отображений $\iota_1 : A \longrightarrow A \times_C B$ и $\iota_2 : B \longrightarrow A \times_C B$, являющихся факторизациями канонических вложений ι_1 и ι_2.

• Так как мы уже знаем, что свободные объединения существуют, существование амальгамированных сумм гарантируется аксиомой подстановки.

2. Частные случаи амальгамированной суммы. Сейчас мы покажем, что свободные объединения и объединения могут быть истолкованы как частные случаи операции амальгамированной суммы, а в следующем параграфе введем еще один важный пример амальгамированных сумм – букетные произведения множеств с отмеченной точкой.

• **Свободное объединение.** Рассмотрим случай, когда $C = \varnothing$ пусто. В этом случае существует единственная возможность как для f, так и для g, причем условие наложенное на $\sim_C$ в определении пусто, так что $\sim_C$ является просто отношением равенства на $A \coprod B$. Таким образом, в этом случае $A \coprod_C B = A \coprod B$.

• **Объединение.** Пусть $C = A \cap B$, а f и g – естественные вложения $A \cup B$ в A и B, соответственно. Тогда $A \coprod_C B$ является фактором $A \coprod B$ по наименьшему отношению эквивалентности содержащему отношение R такое, что $(c, 1)R(c, 2)$ для всех $c \in C = A \cap B$. Ясно, что в данном случае $\sim_C = \Delta_{A \coprod B} \cup R$, где, как обычно, Δ обозначает диагональ декартова квадрата $(A \coprod B)^2$, т.е., иными словами, отношение равенства на $A \coprod B$. Таким образом, $A \coprod_C B$ **канонически изоморфно** объединению $A \cup B$ (изоморфизм задается посредством $(a, 1) \mapsto a$ для $a \in A \setminus B$, $(b, 2) \mapsto b$ для $b \in B \setminus A$ и, наконец, $\{(c, 1), (c, 2)\} \mapsto c$ для $c \in C = A \cap B$).

3. Кодекартовы квадраты. Дадим теперь правильное определение амальгамированной суммы в терминах универсального свойства. Квадрат

$$\begin{array}{ccc} C & \xrightarrow{f} & A \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle \iota_1} \\ B & \xrightarrow[\iota_2]{} & D \end{array}$$

называется **кодекартовым квадратом** (часто говорят также **коуниверсальным квадратом**), если он коммутативен и для любого коммутативного квадрата

$$\begin{array}{ccc} X & \xrightarrow{f} & A \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle \theta_1} \\ B & \xrightarrow[\theta_2]{} & X \end{array}$$

существует единственное отображение $\eta : D \longrightarrow X$ такое, что $\theta_1 = \eta \circ \iota_1$ и $\theta_2 = \eta \circ \iota_2$. Так вот, **амальгамированная сумма** A и B под C это *в точности* множество $A \coprod_C B$ *вместе с отображениями* $\iota_1 : A \longrightarrow A \times_C B$, $\iota_2 : B \longrightarrow A \times_C B$, для которого квадрат

$$\begin{array}{ccc} C & \xrightarrow{f} & A \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle \iota_1} \\ B & \xrightarrow[\iota_2]{} & A \coprod_C B \end{array}$$

является кодекартовым.

Задача. Сформулируйте и докажите аналоги всех утверждений, высказанных в предыдущем параграфе для расслоенных произведений.

Гл. 4. Отображения

Мы, которых называют теперь *реформаторами*, стремимся положить в основу преподавания *понятие функции*, ибо это есть то понятие, которое в течение последних 200 лет заняло центральное место всюду, где только мы встречаем математическую мысль.

Феликс Клейн[184]

В этой главе систематически вводятся основные понятия, связанные с отображениями множеств. Со многими из них читатель уже, несомненно, встречался в школьном курсе, а некоторые, кроме того, вкратце напоминались в Главе 3. Однако наша терминология и обозначения могут несколько отличаться от школьных. Кроме того, с видом на теорию категорий, мы гораздо тщательнее, чем это принято в элементарных учебниках, прорабатываем алгебраические аспекты теории отображений: композиция, итерации, связь односторонней обратимости и регулярности с инъективностью и сюръективностью, функториальность, взаимоотношения с прямыми произведениями, морфизмы между отображениями, ядра и уравнители и т.д. В §§ 6 – 15 мы обсуждаем способы задания отображений и трактуем основные примеры.

§ 1. Отображения: первые слова

Халатное, поверхностное знакомство с митьковской лексикой приводит к быстрому искажению и, в конечном итоге, вырождению смысла цитат и выражений.

Владимир Шинкарев, 'Митьки', часть 8

Все, что мы делали до сих пор, являлось просто подготовкой к тому, чтобы поставить на твердую основу понятие отображения. Мы сделаем это в § 4, но до этого

1. Наивное определение отображения. Отображения (alias **морфизмы**) множеств – одно из центральных понятий математики. В различных контекстах отображения называются также преобразованиями, функциями, движениями, действиями, сдвигами, перестановками, симметриями, функционалами, операторами, формами, семействами, последовательностями, словами, трансформациями, векторами, матрицами и т.д.

Наивное определение. Отображение $f : X \longrightarrow Y$ *сопоставляет каждому элементу* x *множества* X *единственный элемент* y *множества* Y*, обозначаемый* $f(x)$ *и называемый* **образом** *элемента* x *под действием* f*.*

Часто, в зависимости от контекста, образ элемента x под действием f обозначается иначе, например, $f[x]$, fx, f_x, ${}^f x$, x^f, xf, (f, x), (x, f) и даже $(x)f$ – что, в общем-то, абсолютно оправданно, если ось абсцисс направлена вертикально вверх, см. по этому поводу замечания Литтлвуда в "Математической смеси").

Равенство $y = f(x)$ записывается также в виде $f : x \mapsto y$ и читается, например, как:

• x **отображает** x **в** y,

[184]Ф.Клейн, Элементарная математика с точки зрения высшей, т.I. – М. Наука, 1987, стр.18.

- f **переводит** x **в** y,
- f **сопоставляет** элементу x элемент y,
- f **преобразует** x **в** y,
- f **трансформирует** x **в** y,
- x **переводится в** y отображением f,
- x **переходит в** y под действием f,
- y является **образом** x под действием f,
- y **получается из** x применением отображения f,
- y **соответствует** x при отображении f,

и миллионом других способов. Обратите внимание, что при этом используется **другая** стрелка, '$\mapsto$', называемая \mapsto на TEXническом жаргоне, в отличие от обычной стрелки '$\longrightarrow$', называемой \longrightarrow. Полностью отображение f записывается как **тройка** (X, Y, Γ) и в § ? мы дадим формальное определение отображений, объясняющее, что такое на самом деле f с теоретико-множественной (т.е. *чисто экстенсиональной*) точки зрения.

2. Замечания о терминологии. Как уже было сказано, имеется много различных названий отображений в специальных случаях. Единственным термином, *полностью* синонимичным слову 'отображение' является выражение **морфизмы множеств** или, если нужна совсем исключительная точность, **морфизмы в категории множеств**. В школьной программе отображения f обычно называются **функциями**, при этом образ $y = f(x)$ под действием f обычно называется **значением** f **в точке** x или отвечающим **аргументу** x, а x традиционно называется также **переменной** (variable). Если $f(x) = y$, то традиционно говорят еще, что f **обращается в** y **в точке** x. В старинных источниках 'переменная' называется '*переменной величиной*', но, поскольку я не знаю, что такое '*величина*' (Grösse), и чем она отличается от '*количества*' (quantity), и не смог найти ни одного определения этих понятий в доступной мне литературе, я не буду пользоваться словом 'величина' как математическим термином. Иногда X рассматривается как множество **индексов**, и в этом случае f называется **семейством** элементов Y, образ $x \in X$ под действием f обозначается f_x, а само отображение f изображается в этом случае посредством $(f_x)_{x\in X}$. В § 3 мы подробно обсудим понятия, связанные с семействами, **последовательностями**, etc. Отображения из множества X в себя обычно называются **преобразованиями** этого множества или **операторами** на этом множестве, алгебраисты часто называют их **эндоморфизмами** этого множества (особенно, если оно снабжено какой-либо дополнительной структурой). Впрочем, советская школа функционального анализа называла операторами произвольные отображения из одного векторного пространства в другое, и при этом говорила даже о *не всюду определенных* и *многозначных* операторах.

3. Функция, значение функции и имя функции. Следует тщательнейшим образом различать функцию и ее значение. Традиционные учебники изобилуют нелепостями[185] типа 'функция x^2', 'функция $\sin(x)$' и т.д. В

[185] В.П.Хавин считает, что x является именем тождественной функции $\mathrm{id}_{\mathbb{R}}$ и тогда выражение 'функция x^2' становится вполне осмысленным! Однако использование подобного экстравагантного соглашения нужно, конечно, специально оговаривать. Кроме того, даже при этом соглашении x в выражении 'функция $\sin(x)$' абсолютно излишне!

действительности, sin уже является *именем* функции и поэтому правильно говорить 'sin' либо 'функция $x \mapsto \sin(x)$', а $\sin(x)$ представляет *значение* этой функции в точке x. Заметим, что в школе пишут $\sin x$ вместо $\sin(x)$, что было бы логично, если бы значение функции f обозначалось через fx. Однако мы трактуем sin, cos, ln точно так же, как все другие имена функций и, соответственно, пишем $\cos(x)$, $\ln(x)$ и т.д. Проблема состоит в том, что большинство функций вообще не имеют общепринятых имен, не содержащих переменных. Как, например, *называется* функция $x \mapsto (x-1)(x+1)^{-1}$?

4. Отображения и функции. Так как наша терминология основана на традициях профессиональной алгебры, она заметно отличается как от школьной терминологии, так и от словоупотребления, принятого в большинстве учебников 'высшей математики'. Как уже было сказано, в элементарных учебниках слова 'отображение' и 'функция' используются как синонимы. Однако алгебраисты обычно называют функциями **только** отображения, принимающие значения в коммутативном кольце R (а в математическом анализе 'функциями' обычно называются гораздо более сложные образования, чаще всего классы отображений относительно различных отношений эквивалентности). Кроме того, во многих разделах анализа, в особенности в комплексном анализе, принято говорить о 'многозначных функциях' и 'частичных функциях'. Такое обычное в математическом анализе словоупотребление, как 'векторнозначная функция векторного аргумента' было бы крайне удивительно в алгебраической литературе, где в этом контексте предпочитают говорить о 'преобразованиях', 'операторах' и т.д. Поэтому для нас слова 'отображение' и 'функция' **не являются синонимами**. Первое из них есть **термин**, выражающий точный и устойчивый смысл, второе используется в десятках разных смыслов, в частности,

• Как точный алгебраический термин, означающий отображения со значениями в **коммутативном** кольце R;

• Как указание на то, что отображения рассматриваются с **поточечными** операциями ('сумма функций', 'произведение функций');

• Как общепринятое сокращение выражения **росток функции** (например, 'рациональная функция', 'мероморфная функция');

• Как часть устойчивых словосочетаний ('характеристическая функция');

• В аналитических примерах в тех смыслах, как это принято в анализе (т.е. как классы эквивалентности функций или функционалов: 'функции из L^2', 'обобщенные функции');

• В **поэтическом смысле** как выражение некой интенции (впрочем, эту функцию слова 'функция' бывает трудно отличить от его использования в анализе).

§ 2. "О функциях вообще"

Сейчас мы коротко обсудим классическое понятие функции, начиная с того момента, как фон Лейбниц ввел этот термин. С XVII века до конца XIX века отчетливо прослеживаются три основных метафоры функции, которые вынуждены были сосуществовать, пока одна из них полностью не вытесняла другую:

• **переменная величина** alias **кривая** (XVII – XVIII век);

• **аналитическое выражение** (XVIII – XIX век);

• **закон** alias **соответствие** (XIX – XX век).

В следующем параграфе и в Главе IX мы обсуждаем еще две возникшие в XX веке метафоры функции, алгоритмическую и категорную:

• **черный ящик** alias **оракул**, перерабатывающий вход в выход.

• **морфизм** alias **стрелка** (arrow). При этом вообще не важно, как функция действует на индивидуальных элементах, а лишь как она взаимодействует с другими функциями.

Мы не знаем, как будут мыслить функцию математики XXI века и что придет на смену нашим метафорам.

1. Функции до Эйлера. Ньютон стоял на чисто геометрической (механической?) точке зрения и называл переменные 'флюэнтами', а функции – 'ординатами' или 'кривыми'. Само

слово ‘функция’, как и десятки других общепринятых сегодня терминов и обозначений, было введено фон Лейбницем. Впрочем, по-видимому, даже алгебраически настроенный Лейбниц считал **все** функции аналитическими. Вот одно из классических определений того периода, принадлежащее Иоганну Бернулли. “Функцией переменной величины называется величина, составленная **каким угодно способом** из этой переменной величины и постоянных”. Это уже почти современное определение, если понять буквально выделенные слова ‘каким угодно способом’. Впрочем, сомнительно, чтобы математики XVII – XVIII веков понимали его совсем буквально. Так, еще в 1813 году (!!!) в книге “Теория аналитических функций” Лагранж прямо утверждал, что **любая** функция может быть представлена степенным рядом. Впрочем в этом смысле он лишь продолжал полуторавековую традицию. Например, Даниил Бернулли учил, что **любая** кривая представляется в виде ряда, правда не степенного, а тригонометрического.

2. Функция по Эйлеру. Чтение книги Эйлера “Введение в анализ бесконечно малых” и сегодня производит совершенно ошеломляющее впечатление[186]. Имеет место по крайней мере одно из следующих двух утверждений: эта книга удивительно современна или все остальные учебники анализа удивительно старомодны. Мне, во всяком случае, было трудно избавиться от впечатления, что все школьные учебники, как и учебники высшей математики, математического анализа, калькулюса и т.д. списаны с этой книги, вплоть до обозначений и конкретных примеров. На стр.30 этой книги дается следующее определение функции: ‘Functio quantitatis variabilis est **expressio analytica** quomodocunque composita ex illa quantitate variabili et numeris seu quantitatibus constantibus. Omnis ergo expressio analytica, in qua praeter quantitatem variabilem z omnes quantitates illam expressionem componentes sunt constantes, erit functio ipsius z’ (‘Функция переменной величины есть **аналитическое выражение**, произвольным образом составленное из этой переменной величины и чисел или постоянных величин. Следовательно, всякое аналитическое выражение, в котором за исключением переменной величины z все остальные величины суть постоянные, является функцией этого z.’). Заметим, что далее Эйлер специально говорит о ‘functiones multiformes’ в отличие о ‘functiones uniformes’. То, что выражение ‘многозначные функции’ у Эйлера не было оговоркой, подтверждается всем содержанием главы “О функциях вообще”. Так, он тщательнейшим образом определяет двузначные, трехзначные и четырехзначные функции и сопровождает свои определения многочисленными примерами. В частности, “Двузначная функция z есть такая, которая при любом определенном значении z имеет два значения. Такого рода функции представляют квадратные корни, как $\sqrt{2z+z^2}$” (l.c. 11^0). Насколько это разумнее того, что говорится по поводу квадратных корней в школьной программе сегодня! Еще одно недвусмысленное свидетельство дает пункт 16^0 той же главы: ‘Si fuerit y functio quaecunque ipsius z, tum vicissim z erit functio ipsius y’ (‘Если y будет функцией z, то и, обратно, z будет функцией y’). Таким образом, очевидно, что Эйлер вкладывал в слово ‘функция’ скорее тот смысл, который мы сегодня придаем слову ‘отношение’, а не слову ‘отображение’! Более того, там же Эйлер говорит о ‘functiones implicites’: “Так, Z будет неявной иррациональной функцией z, если оно определяется уравнением $Z^7 = azz^2 - bz^5$, так как даже при помощи знаков радикала нельзя получить явного значения Z, *потому что обычная алгебра еще не достигла такой степени совершенства*” (!!!). В то же время, в отличие от современного чисто экстенсионального подхода, Эйлер всюду подчеркивает существование *аналитического выражения*, формулы, связывающей аргумент и значение функции.

3. Функция по Фурье. Совершенно замечательно определение, которое дает Фурье в своей книге “Аналитическая теория теплоты” (1822 год): “Общая функция $f(x)$ представляет собой последовательность значений или ординат, каждая из которых произвольна. Совсем не предполагается, что эти ординаты подчиняются определенному закону; они могут следовать совершенно произвольно и каждая из них задается как если бы она была единственной величиной.” Очевидно, что здесь функция не предполагается ни аналитической, ни дифференциируемой, ни даже непрерывной. Это определение тем более замечательно, если учесть, что с господствующей точки зрения на историю математики Фурье идейно целиком принадлежал XVIII веку и если сравнить его с пониманием современников Фурье, которых мы обычно считаем гораздо более продвинутыми, таких, как Дирихле.

4. Функция по Дирихле. Очень часто приоритет в определении функции вообще отдается Дирихле, при этом обычно ссылаются на его статью 1837 года “Über die Darstellung

[186]Л.Эйлер, Введение в анализ бесконечно малых, т.I. – ОНТИ, М.–Л., 1936, с.1–352.

ganz willkürlicher Funktionen ...". Однако, насколько я могу судить, это мнение основано исключительно на названии этой статьи. В тексте же весьма тщательно определяются **непрерывные** функции на интервале $]a, b[$: "если теперь каждому x соответствует одно единственное конечное y и **притом так, что** когда x ..." Знал ли Дирихле, что не все функции непрерывны? Как показывает пример функции Дирихле, знал.

5. Отображение по Дедекинду. Современное определение отображения было впервые дано Дедекиндом. Вот отрывок из его книги "Что такое числа и зачем они нужны": "Под **отображением** ϕ какой-либо системы S мы будем понимать **закон**, согласно которому каждому определенному элементу s этой системы сопоставляется вполне определенная вещь, которая называется образом s и обозначается символом $\phi(s)$; можно то же обстоятельсто выразить, другими словами: $\phi(s)$ соответствует элементу s, или $\phi(s)$ получается из s путем отображения ϕ или s переходит в $\phi(s)$ путем отображения ϕ". Определение Дедекинда и близкие к нему определения Кантора содержали неопределенное слово 'закон' (Gesetz). Чтобы избавиться от него, Пеано предложил понимать отображения $X \longrightarrow Y$ чисто экстенсионально, как подмножества прямого произведения $X \times Y$.

Ясно, что определение Дедекинда возникло в контексте его занятий теорией чисел, алгеброй и теорией множеств, а вовсе не как обобщение аналитического понятия функции. Именно поэтому Дедекинд и Кантор ощущали необходимость введения нового термина 'отображение' (Abbildung) для этого нового более общего понятия. Поэтому мне совершенно непонятно стремление школьных методистов снова сделать – вопреки традиции, удобству и здравому смыслу – термин 'функция' синонимом термина 'отображение'.

§ 3. Метафора функции: stimulus and response

> Под психологической функцией я понимаю известную форму психической деятельности, которая принципиально остается равной себе при различных обстоятельствах.
>
> Карл Густав Юнг, "Психологические типы", § 831.

> Секретная система определяется абстрактно как некоторое множество отображений одного пространства (множества возможных сообщений) в другое пространство (множество возможных криптограмм). Каждое конкретное отображение из этого множества соответствует способу шифрования при помощи конкретного ключа.
>
> Клод Шеннон[187]

> **Function** (*n.*) The way in which an object, or an artifact or part of an artifact, or part of an organism acts to carry out its purpose, *e.g.* **a** the function of a clutch in a motor car is to connect and disconnect, as needed, the engine from the gearbox; **b** the function of a galvanometer is to detect the flow of an electric current; **c** a function of the liver is to convert glucose to glycogen for the storage of carbohydrate.
>
> Longman Dictionary of Scientific Usage, AJ043.

Сейчас мы опишем функцию как **черный ящик** (`black box`), перерабатывающий **вход** (`input`, стимул, аргумент) в **выход** (`output`, отклик, значение):

$$\text{вход } x \longrightarrow \boxed{\begin{array}{c}\text{функция}\\ f\end{array}} \longrightarrow \text{выход } f(x)$$

[187]Теория связи в секретных системах. – секретный доклад, датированный 1 сентября 1945 года, рассекреченный и опубликованный в 1949 году. Русский перевод можно найти в книге К.Шеннон, Работы по теории информации и кибернетике. – ИЛ, М., 1963, с.1–829. стр.333–402. Большой фрагмент этой работы воспроизводится также в книге 'Введение в криптографию', под ред. В.В.Ященко. МЦНМО, М., 1998, с.1–271, на стр.234–271.

Именно эта метафора стала основным интуитивным образом функции в XX веке. Полезно осознать, что эта метафора отличается от метафоры XIX века так же, как квантовая механика отличается от классической!

Отличие этой точки зрения от точки зрения XIX века состоит в том, что мы не знаем, что *в действительности* находится внутри черного ящика. В XIX веке функция мыслилась как закон, который мы полностью контролируем или, хотя бы, можем полностью понять! Существенно, что это описание является чисто феноменологическим. *Может быть* генеральный конструктор и знает, **что** находится внутри черного ящика, **как** он работает и **почему** реагирует определенным образом на определенные запросы. Однако с точки зрения большинства юзеров, даже *самых* продвинутых, все это не имеет *никакого* значения.

Возникновение такого представления о функции поддерживается тем, что как только мы начали всерьез что-то вычислять, мы вдруг осознали, что черный ящик имеет внутреннюю структуру. Допустим, мы рассматриваем функцию $f : x \mapsto x^{1000}$ или, *для круглого счета*, $f : x \mapsto x^{1024}$ и хотим *реально* вычислить какое-то из ее значений, ну хотя бы

$$\begin{aligned} 2^{1024} =& 179769313486231590772930519078902473361797697894230657273430081 \\ & 157732675805500963132708477322407536021120113879871393357658789 \\ & 768814416622492847430639474124377767893424865485276302219601246 \\ & 094119453082952085005768838150682342462881473913110540827237163 \\ & 350510684586298239947245938479716304835356329624224137216 \end{aligned}$$

В этом случае совершенно не безразлично, как именно представляется функция f и как именно вычисляется это значение, а именно $x^{1024} = x * x * \ldots * x$, где сомножитель x повторен 1024 раза, или

$$x^{1024} = ((((((((((x \uparrow 2) \uparrow 2) \uparrow 2) \uparrow 2) \uparrow 2) \uparrow 2) \uparrow 2) \uparrow 2) \uparrow 2) \uparrow 2).$$

Но ведь с чисто экстенсиональной точки зрения это одна и та же функция! В наше время все больше математиков начинают учитывать точку зрения вычислителей и программистов, состоящую в том, что совершенно не безразлично, что именно находится в черном ящике. Непосвященным кажется, что с ростом вычислительных возможностей скорость алгоритмов не имеет больше значения, однако в действительности дело обстоит прямо противоположным образом.

Более того, во многих случаях этот черный ящик может действовать как **оракул**, т.е. выдавать по нашему запросу значение функции таким образом, что мы не только не знаем, но не можем и не должны знать, как именно вычисляется эта функция. Типичным примером оракула является шифровальная машина. В настоящее время оракулы широко применяются в системах связи, компьютерных и банковских сетях, и т.д. Нет сомнения, что в генераторах паролей, ключей, PIN'ов и тому подобного используется какой-то алгоритм – но тому, кто сообщает номер своей кредитной карточки интернет магазину, совершенно обязательно знать, какой именно.

• **Автомат по продаже газированной воды.** В годы моего детства на улицах Санкт-Петербурга стояли автоматы по продаже газированной воды[188],

[188]В.П.Хавин, Основы математического анализа. – Лань, СПб, 1998, с.1–446, стр.32.

допускавшие два[189] возможных инпута:

A – опускание в специальный слот монеты номиналом `1 копейка`,

B – опускание туда же монеты номиналом `3 копейки`.

Теоретически исправный автомат f реагировал на эти инпуты следующим предсказуемым образом: $f(A)$ – стакан воды без сиропа, $f(B)$ – стакан воды с сиропом.

• **Управление бытовыми приборами.** В первом приближении кассетный магнитофончик можно представлять себе как черный ящик, который в ответ на нажатие одной из пяти кнопок `Rewind`, `Play`, `FastForward`, `Stop`, `Eject` производит одну из пяти названных здесь операций.

§ 4. Область, кообласть и график отображения

> Геометрические преобразования (вращения, отражения, растяжения и т.д.) являются функциями, которые практически буквально описывают движение, а в прикладной математике силы фактически моделируются функциями. Описанные здесь динамические свойства представляют собой существенную часть значения слова "функция", как оно употребляется в математике. Определение фунции через упорядоченные пары не отражает этого. Оно является формальной теоретико-множественной *моделью* интуитивной идеи функции – моделью, которая охватывает лищь один аспект этой идеи, а не все ее значение в целом.
>
> Роберт Голдблатт, [Go], стр.32.

Здесь мы дадим экстенсиональное определение отображения по Пеано и Дедекинду: отображение считается полностью определенным, *только* если задано **что**, **куда** и **как** отображается. Все обсуждаемые в этом параграфе понятия будут проиллюстрированы в следующих 10 параграфах.

1. Область и кообласть отображения. В теоретико-множественной трактовке отображений мы обязаны эксплицировать[190] **все** элементы отображения, в частности, область определения и область значений. Стоит отметить, что при этом никакой симметрии между областью определения и областью значений нет. **Что** отображается еще можно восстановить по графику – но, конечно, не по формуле, поэтому бессмысленно и *опасно* говорить о 'функции $f(x)$'. С другой стороны, **куда** это отображается, вообще никогда не восстанавливается по графику и должно **во всех случаях** явно задаваться!

Определение. *Множество X называется* **областью определения** *отображения $f : X \longrightarrow Y$ и обозначается $D(f)$, а множество Y называется* **областью значений** *отображения f и обозначается $R(f)$.*

В последнее время получает все большее распространение альтернативная терминология, пришедшая из теории категорий, когда $D(f)$ называется просто

---

[189] Мы не обсуждаем более продвинутые автоматы с несколькими слотами, где можно было получить газированную воду с разными видами сиропа. Мы не обсуждаем также ненормативные инпуты такие как засовывание в слот других предметов, сильный удар кулаком или ногой и т.д.

[190] `Эксплицировать` – проговаривать, выводить из подсознания в сознание, объяснять, прояснять, излагать, интерпретировать, проговаривание очевидных деталей `эксплицирование`, `экспликация`,

областью отображения f, а $R(f)$ **кообластью** – и в этом случае обозначается $C(f)$. Говорят также, что f действует из X в Y. Естественно, обозначения $D(f)$, $R(f)$ и $C(f)$ происходят просто от первых букв английских слов `domain`, `range` и `codomain`.

2. График отображения. Однако основным в определении отображения является сам способ, которым элементам X сопоставляются элементы Y. С чисто экстенсиональной точки зрения этот способ тоже должен задаваться некоторым множеством (поскольку в ортодоксальной теории вообще не существует ничего, кроме множеств!)

Определение. *Множество* $\Gamma(f) \subseteq X \times Y$, *состоящее из всех пар* $(x, f(x))$, $x \in X$, *называется* **графиком** *отображения* $f : X \longrightarrow Y$.

Вспомнив график какой-нибудь функции, из тех, что Вы рисовали в школе, Вы немедленно поймете, что он как раз и является графиком этой функции с точки зрения этого определения, если, конечно, отождествить точку плоскости с упорядоченной парой ее координат.

3. Определение отображения. Теперь мы в состоянии дать *формальное* определение отображения как тройки, состоящей из области определения, области значений и графика. Следующее определение было дано Пеано.

Определение. Отображением *из множества* X *в множество* Y *называется тройка* (X, Y, Γ), *где* $\Gamma \subseteq X \times Y$ *подмножество произведения* $X \times Y$ *обладающее следующим свойством: если* $(x, y_1), (x, y_2) \in \Gamma$, *то* $y_1 = y_2$.

В этом определении исчезло всякое упоминание о ‘законе’, ‘правиле’, etc.

4. Равенство отображений. Напомним, что $D(f)$ и $R(f)$ входят в определение отображения f. Таким образом, наше общее определение равенства упорядоченных троек дает нам следующее понятие равенства отображений.

Определение. *Два отображения* f *и* g **равны**, *если и только если*

1) *их области совпадают,* $D(f) = D(g) = X$,
2) *их кообласти совпадают,* $R(f) = R(g) = Y$,
3) *для любого* $x \in X$ *выполнено равенство* $f(x) = g(x)$.

Поясним введенные в этом параграфе понятия на следующем примере.

Контрольный пример. Рассмотрим следующие четыре отображения:

i) $\mathbb{R} \longrightarrow \mathbb{R}$, $x \mapsto x^2$;
ii) $\mathbb{R}_+ \longrightarrow \mathbb{R}$, $x \mapsto x^2$;
iii) $\mathbb{R} \longrightarrow \mathbb{R}_+$, $x \mapsto x^2$;
iv) $\mathbb{R}_+ \longrightarrow \mathbb{R}_+$, $x \mapsto x^2$.

Это четыре *разных* отображения с **абсолютно** различными свойствами:

- Отображение i) не является ни инъективным, ни сюръективным.
- Отображение ii) инъективно, но не сюръективно.
- Отображение iii) сюръективно, но не инъективно.
- Наконец, отображение iv) биективно.

Таким образом, из этих четырех отображений только последнее допускает обратное отображение $\mathbb{R}_+ \longrightarrow \mathbb{R}_+$, $x \mapsto \sqrt{x}$. Мы видим, насколько бессмысленно и преступно принятое в элементарных учебниках выражение “функция $f(x) = x^2$”, не содержащее явного указания области и кообласти отображения.

§ 5. Семейства, последовательности, слова

Поясним теперь использование терминов ‘семейство’, ‘последовательность’ и ‘слово’.

1. Семейства. Обычное различие в понимании слов ‘отображение’ и ‘семейство’ чисто социологическое. Индивидуально семейство это просто отображение. Но понятие *равенства* двух семейств отличается от понятия равенства отображений[191]. А именно, кообласть *не входит* в определение равенства семейств.

Определение. *Два семейства f и g считаются* **равными**, *если*

1) *их области совпадают, $D(f) = D(g) = X$;*

2) *для любого $x \in X$ выполнено равенство $f(x) = g(x)$.*

Область определения семейства называется обычно **множеством индексов**, а вместо $f(x)$ используют **индексную запись** f_x. Многие авторы придерживаются следующего соглашения: индексы семейств обозначаются малыми латинскими буквами ‘i, j, h’ и так далее, если множество индексов X конечно или счетно, и малыми греческими буквами ‘α, β, γ’ и так далее, если про мощность множества индексов ничего не предполагается. Мы не будем, как правило, подчеркивать это различие, так как в алгебре оно редко играет роль. Семейство f обычно записывается как $\{f_x, x \in X\}$ или $\{f_x\}_{x \in X}$.

2. Последовательности. Для многих математиков слово ‘последовательность’ является просто синонимом ‘семейства’, это принято, например, в топологии. Однако, мы будем следовать терминологии, принятой в математическом анализе, и называть **последовательностями** лишь такие семейства, область определения (‘множество индексов’) которых конечна или счетна, в то время как область определения семейства может быть произвольной. Последовательность обычно задается просто перечислением своих значений, например, конечная последовательность f длины n, записывается как $f_1, f_2, \dots, f_n$, а бесконечная последовательность как $f_1, f_2, \dots, f_n, \dots$. При этом последовательность f, для которой $D(f) = \underline{n}$, называется **конечной**, точнее, последовательностью **длины** n, а последовательность f, для которой $D(f) = \mathbb{N}$, – **бесконечной**. Таким образом, говоря о конечности последовательности обычно имеют в виду конечность множества *индексов*, а не значений, последовательность $0, 1, 0, 1, 0, 1, \dots$ бесконечна. Последовательности, для которых $D(f) = \mathbb{Z}$, называются **бесконечными в обе стороны** последовательностями.

3. Слова. В алгебре конечные последовательности со значениями в множестве Y часто называются **словами в алфавите** Y. При этом слово $x_1, \dots, x_n$ обычно записывается просто как $x_1 \dots x_n$. Например, $w = blablabla$ является словом длины 9 в алфавите $\{a, b, l\}$ (или каком-то большем алфавите, например, латинском – напомним, что понятие равенства слов не зависит от алфавита!) таким, что $w_1 = b$, $w_2 = l$, $w_3 = a$ и так далее. Таким образом, множество слов длины n в алфавите Y – это, по-существу, то же самое, что n-я декартова степень Y^n множества Y, но при этом элемент $(x_1, \dots, x_n)$ записывается

[191] В качестве курьеза отметим, что в “Математической энциклопедии” (т.IV, с.153) равенство отображений определяется как равенство семейств, при этом произносится следующая загадочная фраза: “В этом случае совпадают и области значений этих О.”.

как $x_1 \dots x_n$. Особенно часто эта запись используется когда одновременно рассматриваются *все* слова конечной длины в алфавите Y. В любом алфавите Y имеется единственное слово длины 0 (единственное отображение $\underline{0} = \varnothing$ в Y), называемое обычно **пустым** словом и обозначаемое $\Lambda = ()$. Заметим, что здесь Λ представляет собой не греческую букву 'Lambda', а перевернутую букву 'V', первую букву слова `void` – на самом деле, конечно, `vuoto`. Множество всех слов конечной длины в алфавите Y обозначается $W(Y)$, ясно, что обозначение 'W' указывает на первую букву слова `Wort` – или `word`. Таким образом, по определению

$$W(Y) = Y^0 \cup Y^1 \cup Y^2 \cup \dots$$

Иногда рассматривают и бесконечные слова в алфавите Y, т.е. последовательности $\mathbb{N} \longrightarrow Y$, также записываемые в этом случае $x_1 x_2 \dots x_n \dots$

§ 6. Первые примеры отображений

Начнем с тех примеров, которые естественно возникают в самой теории множеств.

1. Универсальные объекты категории множеств. В категории множеств есть три объекта, играющие совершенно особую роль с точки зрения отображений.

• Пустое множество $\varnothing$, являющееся **инициальным** alias **универсальным отталкивающим** объектом, т.е. для каждого множества X существует единственное отображение $\varnothing \longrightarrow X$;

• Одноэлементное множество $\{\varnothing\}$, являющееся **финальным** alias **универсальным притягивающим** объектом, т.е. для каждого множества X существует единственное отображение $X \longrightarrow \{\varnothing\}$;

• Двухэлементное множество $\{\varnothing, \{\varnothing\}\}$, которое является **классификатором подобъектов**, т.е. обладает тем свойством, что подмножества множества X отвечают отображениям $X \longrightarrow \{\varnothing, \{\varnothing\}\}$, см. об этом § 10.

2. Первые примеры отображений. Вот несколько очевидных, но от этого не менее важных примеров отображений.

• **Постоянное отображение.** Пусть X и Y – любые множества, а $c \in Y$ – произвольный, но фиксированный элемент множества Y. Отображение $f : X \longrightarrow Y$, перевожящее все элементы множества X в элемент c называется **постоянным отображением**, которое будет в дальнейшем обозначаться через co_c. Например, если $Y = R$ – коммутативное кольцо, то постоянное отображение co_0 называется обычно **нулевым отображением** или **нулевой функцией**. Если нет опасности двусмысленности, вместо co_0 обычно пишут просто 0.

• **Тождественное отображение.** Пусть X – любое множество. Тогда определено отображение $\mathrm{id} = \mathrm{id}_X : X \longrightarrow X$ такое, что $x \mapsto x$ для всех $x \in X$, называемое **тождественным** отображением X на себя. Обозначение id_X является сокращением от английского identical. Некоторые авторы обозначают id_X через 1_X и называют его **единичным** отображением X на себя. В следующем параграфе мы покажем, как построить громадные классы отображений из этих двух базисных типов.

• **Вложение.** Пусть теперь $X \subseteq Y$ – любая пара множеств. Тогда определено отображение $\hookrightarrow\colon X \longrightarrow Y$ такое, что $x \mapsto x$ для всех $x \in X$, называемое **вложением** X в Y. Обозначение $\hookrightarrow$ является сокращением от английского inclusion. Вложение обычно обозначается специальной стрелкой $f : X \hookrightarrow Y$, которая TEXнически называется `\hookrightarrow`. Заметим, что хотя график отображения $\hookrightarrow\colon X \longrightarrow Y$ совпадает с графиком отображения id_X, эти отображения *различны* (например, первое из них не сюръективно, если $X \neq Y$, в то время как второе сюръективно).

• **Диагональное отображение.** Тождественное отображение является частным случаем следующего очень важного отображения. Именно, пусть $Y = X^n$ есть n-я декартова степень множества X. Определим отображение $\Delta : X \mapsto X^n$ посредством $\Delta(x) = (x, \dots, x)$. Это отображение называется **диагональным отображением**.

• **Наименьший элемент.** Пусть X некоторое упорядоченное множество, а $Y \subseteq X$ – какое-то его подмножество. Обозначим через $\inf(Y)$ наименьший элемент множества Y, *если он существует*. Согласно определению наименьшего элемента, если такой элемент в множестве Y существует, то он *единственен*, так что сопоставление $Y \mapsto \inf(Y)$ задает отображение из множества тех $Y \in 2^X$, для которых наименьший элемент существует, в множество X. Однако, пример $Y = \varnothing$ показывает, что наименьший элемент не обязан существовать. Одна из формулировок **аксиомы индукции** состоит в том, что для любого непустого подмножества $Y \subseteq \mathbb{N}$ наименьший элемент существует. Таким образом, математическая индукция основана на том, что сопоставление $Y \mapsto \inf(Y)$ задает *отображение* $\inf : 2^{\mathbb{N}} \setminus \{\varnothing\} \longrightarrow \mathbb{N}$.

§ 7. Некоторые классические функции

В этом параграфе мы упоминаем несколько классических примеров функций, которые рассматриваются (или *могли бы* рассматриваться) в школьном курсе математики, но не являются 'элементарными'.

• **Абсолютная величина.** Рассмотрим функцию $|\ | : \mathbb{R} \longrightarrow \mathbb{R}_+$, $x \mapsto |x|$, сопоставляющую вещественному числу x его абсолютную величину:

$$|x| = \begin{cases} x, & \text{если } \ x \geq 0, \\ -x, & \text{если } \ x \leq 0. \end{cases}$$

• **Знак.** Определим функцию $\mathrm{sign} : \mathbb{R} \longrightarrow \{0, +1, -1\}$, полагая

$$\mathrm{sign}(x) = \begin{cases} +1, & \text{если } \ x > 0, \\ 0, & \text{если } \ x = 0, \\ -1, & \text{если } \ x < 0. \end{cases}$$

Знак и абсолютная величина являются примерами функций, полученных склейкой, см. § 31.

• **Пол и потолок.** Функция **целая часть** $\mathrm{Ent} : \mathbb{R} \longrightarrow \mathbb{Z}$, $x \mapsto \mathrm{Ent}(x)$, сопоставляет каждому вещественному числу x наибольшее целое, не превосходящее x. Традиционно эта функция называется **антье** (от французского entier) и обозначается еще $x \mapsto [x]$, а в последнее время она все чаще называется **пол**

(от английского floor) и обозначается $x \mapsto \lfloor x \rfloor$. Однако нам будет удобно различать пол и целую часть. А именно, мы рассматриваем пол как функцию $\lfloor\ \rfloor : \mathbb{R} \longrightarrow \mathbb{R}$. По аналогии с ней определяется функция **потолок** $\lceil\ \rceil : \mathbb{R} \longrightarrow \mathbb{R}$, $x \mapsto \lceil x \rceil$, сопоставляющая каждому вещественному числу x наименьшее целое, не меньшее x. Ясно, что $\lceil x \rceil = -\lfloor -x \rfloor$.

• **Дробная часть.** Функция $\mathrm{Frac} : \mathbb{R} \longrightarrow [0,1[$, $x \mapsto \mathrm{Frac}(x)$, сопоставляет вещественному числу x разность $x - \lfloor x \rfloor$. Традиционно $\mathrm{Frac}(x)$ обозначается через $\{x\}$, но это приводит к таким чудовищным конфликтам обозначений, что мы предпочитаем полностью отказаться от этого обозначения. Ну в самом деле, не писать же $\{0\} = 0$.

• **Функция Дирихле.** Функция $\mathrm{Dir} : \mathbb{R} \longrightarrow \{0,1\}$, $x \mapsto \mathrm{Dir}(x)$, определяется формулой

$$\mathrm{Dir}(x) = \begin{cases} 1, & \text{если } x \text{ рационально,} \\ 0, & \text{если } x \text{ иррационально.} \end{cases}$$

Иными словами, функция Дирихле – это характеристическая функция подмножества рациональных чисел в множестве вещественных чисел.

• **Функция Римана.** Функция $R : \mathbb{R} \longrightarrow \mathbb{R}$, $x \mapsto R(x)$, определяется формулой $R(x) = 1/n$, если $x = m/n$ представление рационального числа x в виде несократимой дроби, и $R(x) = 0$, если x иррационально.

Задача по анализу. Доказать, что R непрерывна во всех иррациональных точках и разрывна во всех рациональных точках.

Решение. В каждом интервале (a,b), $a < b$, содержится бесконечное число иррациональных точек, но лишь конечное число рациональных точек вида m/n, где n не превосходит наперед заданное число N.

• **Функция Хевисайда.** Функция $H : \mathbb{R} \longrightarrow \{0,1\}$, $x \mapsto H(x)$, определяется формулой

$$H(x) = \begin{cases} 0, & \text{если } \ x < 0, \\ 1, & \text{если } \ x \geq 0. \end{cases}$$

§ 8. Некоторые арифметические функции

Арифметическими функциями называются функции, определенные на $\mathbb{N}$ или $\mathbb{N}_0$, обычно с комплексными значениями. Впрочем, ниже мы рассматриваем только арифметические функции, принимающие целые или натуральные значения. Используемые нами обозначения арифметических функций традиционны, например, обозначение $\phi(n)$ для функции Эйлера восходит еще к Гауссу.

1. Основная теорема арифметики. Проверка корректности многих приводимых ниже определений зависит от следующего утверждения, традиционно называемого **основной теоремой арифметики**, которое будет доказано в Книге III. Каждое натуральное число $n \in \mathbb{N}$ может быть единственным *с точностью до порядка* образом разложено в произведение простых множителей: $n = p_1 \dots p_r$, где $p_i \in \mathrm{Prim}$. Иными словами, если $n = q_1 \dots q_s$, где $q_i \in \mathrm{Prim}$, то $r = s$ и, быть может *после перестановки сомножителей*, $q_i = p_i$. Обычно разложение на простое записывается как **каноническое разложение** $n = p_1^{m_1} \dots p_s^{m_t}$, где простые $p_1, \dots, p_t$ попарно различны и расположены в порядке возрастания, $p_1 < \dots < p_t$. Многие из приводимых ниже функций определяются в терминах входящих в каноническое разложение простых и их

степеней. Корректность определения этих функций вытекает из *единственности* канонического разложения.

2. Арифметические функции. Вот несколько классических примеров.

• **Факториал.** Рассмотрим отображение $! : \mathbb{N}_0 \longrightarrow \mathbb{N}$, $n \mapsto n!$, которое определяется рекурсивно посредством $0! = 1$, $n! = (n-1)!n$.

• **Функция Эйлера.** Функция $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$, $n \mapsto \phi(n)$, обозначает количество элементов из $\underline{n}$, взаимно простых с n. В Главе 5 мы получим формулу для $\varphi(n)$ в терминах канонического разложения. В старинных учебниках функция $\phi(n)$ именовалась **тотиентой**.

• **Функция Мебиуса.** Функция $\mu : \mathbb{N} \longrightarrow \mathbb{Z}$, $n \mapsto \mu(n)$, определяется следующим образом. $\mu(n) = 0$, если n делится на квадрат протсого числа p и $\mu(n) = (-1)^t$, где t – число различных простых делителей числа n (в частности, так как число различных простых делителей 1 равно 0, то $\mu(1) = 0$).

• **Число делителей.** Функция $d : \mathbb{N} \longrightarrow \mathbb{N}$, $n \mapsto d(n)$, сопоставляет натуральному n число различных натуральных делителей числа n.

• **Число простых делителей.** Функция $\omega : \mathbb{N} \longrightarrow \mathbb{N}$, $n \mapsto \omega(n)$, сопоставляет натуральному n число *различных* простых делителей числа n, а функция $\Omega : \mathbb{N} \longrightarrow \mathbb{N}$, $n \mapsto \Omega(n)$, – число *всех* простых делителей числа n (т.е. количество множителей в разложении n в произведение простых). В обозначениях пункта 2 имеем $\omega(n) = t$, а $\Omega(n) = s = m_1 + \ldots + m_t$.

• **Сумма делителей.** Функция $\sigma : \mathbb{N} \longrightarrow \mathbb{N}$, $n \mapsto \sigma(n)$, сопоставляет натуральному n сумму всех его различных натуральных делителей числа n.

• **Функция Лиувилля.** Функция $\lambda : \mathbb{N} \longrightarrow \mathbb{N}$, $n \mapsto \lambda(n)$, задается посредством

$$\lambda(n) = (-1)^{\Omega(n)} = (-1)^{m_1+\ldots+m_t}.$$

• **Функция Хармса.** Определим функцию $h : \mathbb{N} \longrightarrow \mathbb{N}$, полагая

$$1 \mapsto 1, \quad 2 \mapsto 2^2, \quad 3 \mapsto 3^{3^3}, \quad 4 \mapsto 4^{4^{4^4}}, \quad 5 \mapsto 5^{5^{5^{5^5}}}, \ldots$$

Эта функция хорошо известна специалистам по теории алгоритмов как **пример Аккермана**[192,193]. Она замечательна тем, что является общерекурсивной, но при этом растет быстрее, чем любая примитивно рекурсивная функций.

• **Подряд идущие цифры числа π.** Определим функцию $f : \mathbb{N} \longrightarrow \{0, 1\}$ следующим образом. Положим $f(n) = 1$ если в десятичном разложении числа π есть ровно n идущих подряд цифр 7 и $f(n) = 0$ в противном случае. Подавляющее большинство математиков согласится с тем, что приведенная выше фраза полностью описывает *правило* определяющее некоторую функцию на $\mathbb{N}$. Тем не менее, в настоящее время не известно никакого *алгоритма* для вычисления значения функции f в данной точке n.

---

[192] W.Ackermann, Zum Hilbertschen Aufbau der reelen Zahlen. – Math. Ann., 1928, Bd.99, S.118–133.

[193] А.И.Мальцев, Алгоритмы и рекурсивные функции. – Наука, М., 1965, с.1–391, стр.112–114.

§ 9. Геометрические преобразования

В действительности, кроме числовых функций в школьном курсе рассматривается совсем другой тип отображений, в котором динамический аспект выражен гораздо отчетливее, чем в числовых функциях – **геометрические преобразования**. Рассмотрим, например, возникающие в школьном курсе геометрии преобразования эвклидовой плоскости $\mathbb{R}^2$. Мы отождествляем точку плоскости с парой (a, b) ее координат, при этом **эвклидово расстояние** между точками $x = (a, b)$ и $y = (c, d)$ определяется как $d(x, y) = \sqrt{(a-c)^2 + (b-d)^2}$.

1. Эвклидовы движения. В элементарной геометрии чаще всего используются изометрии, т.е. преобразования, сохраняющие расстояния. Изометрии эвклидовых пространств называются **эвклидовыми движениями**. Иными словами, эвклидово движение $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ характеризуется тем свойством, что для любых двух точек $d(f(x), f(y)) = d(x, y)$. При таком преобразовании каждая фигура движется как твердое тело и переходит в конгруэнтную (или, как говорит Лев Семенович Понтрягин, 'равную') ей фигуру. Вот несколько типов эвклидовых движений.

• **Трансляции.** Самым простым типом геометрических преобразований являются трансляции, сдвигающие каждую точку пространства на одно и то же расстояние в одном и том же направлении. В школе трансляции часто называются также **свободными векторами** или **параллельными переносами**.

• **Повороты.** Движение f плоскости имеющее ровно одну неподвижную точку x, называется **поворотом** вокруг этой точки. При этом x называется центром поворота f.

• **Отражения.** Отражение на плоскости задается выбором неподвижной прямой (зеркала отражения, в случае плоскости зеркало часто называется осью). При отражении каждая точка переходит в точку, симметричную ей относительно зеркала.

2. Эвклидовы подобия. Довольно часто используются также эвклидовы подобия. При подобии все расстояния меняются на один и тот же множитель $c \in \mathbb{R}_+$, называемый **коэффициентом подобия**. Тем самым, эвклидово подобие $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ характеризуется тем свойством, что для любых двух точек $d(f(x), f(y)) = cd(x, y)$. Преобразование подобия является **конформным**, иными словами, при этом преобразовании сохраняются углы.

• **Гомотетии.** Эвклидово подобие f называется **гомотетией**, если у него есть неподвижная точка x, называемая центром и для каждой точки $y \in \mathbb{R}^2$ точка $f(y)$ лежит на луче xy.

В разделах геометрии, изучаемых в математических кружках рассматриваются и такие геометрические преобразования, которые определены только на части точек. Вот еще один ключевой пример конформного преобразования, к которому мы вернемся в книгах II и IV.

• **Инверсии.** Пусть S – окружность радиуса r на плоскости $\mathbb{R}^2$, x – центр этой окружности/ Инверсия $f : \mathbb{R}^2 \setminus \{0\} \longrightarrow \mathbb{R}^2 \setminus \{0\}$, относительно окружности S переводит каждую точку $y \neq x$ в такую точку z, лежащую на луче xy, что $d(x, y)d(x, z) = r^2$.

Мы вернемся к этим примерам при изучении групп. В дальнейшем нам встретятся и другие типы геометрических преобразований в пространствах с неэвклидовой метрикой.

§ 10. Табличное задание отображений

В случае, когда область отображения f конечна, для него часто используется **табличная запись**.

1. Таблица значений функции. В элементарной математике под 'табличным заданием' функции обычно имеют в виду **таблицу значений** этой функции, т.е. картинку вида

x	x_1	x_2	$\dots$	x_n
$f(x)$	$f(x_1)$	$f(x_2)$	$\dots$	$f(x_n)$

При этом **не подразумевается**, что x_i в верхней строчке пробегают все элементы области пределения $D(f)$. Ясно, что на самом деле подобная таблица задает не саму функцию f, а лишь ее ограничение на $\{x_1, \dots, x_n\}$.

2. Табличное задание функции. В случае же, когда X конечно, функция действительно может быть полностью задана перечислением всех ее значений. При этом отображение записывается в виде двустрочной матрицы, в верхней строчке которой перечисляются все элементы области отображения f, в каком-то порядке, а под ними в нижней строчке – соответствующие значения отображения f, при этом запятые между элементами обычно не ставятся. Например, если область отображения f равна $X = \{x_1, \dots, x_n\}$, то оно запишется так:

$$f = \begin{pmatrix} x_1 & \dots & x_n \\ f(x_1) & \dots & f(x_n) \end{pmatrix}$$

Ясно, что отображение не зависит от порядка элементов верхней строки, а только от того, какие элементы стоят в нижней строке под соответствующими элементами верхней строки.

3. Примеры табличного задания. Табличное задание функций окружает нас повсюду. Практически любой список, с которым нам приходится встречаться, представляет собой именно табличное задание некоторой функции.

• **Оглавление** книги представляет собой табличное задание функции, сопоставляющей каждой главе номер ее первой странице.

• **Указатель** задает функцию, сопоставляющую каждому термину страницу, на которой он появляется в первый раз.

• **Ведомость** экзамена представляет собой табличное задание функции, сопоставляющей каждому студенту группы его оценку на экзамене.

• **Меню** в ресторане есть задание функции, сопоставляющей каждому блюду его цену (впрочем, оно может содержать и дополнительную информацию).

• **Список** вида

♡	`\heartsuit`
♢	`\diamondsuit`
♣	`\clubsuit`
♠	`\spadesuit`

задает функцию, сопоставляющую масти ее TEXовское имя.

4. Перестановки. Табличное задание очень часто используется для задания функций из $\underline{m}$ в $\underline{n}$. Напомним, что согласно нашему общему соглашению

функция, задаваемая таблицей, не зависит от порядка элементов первой строки, а только от того, каким элементы стоят под соответствующими элементами первой строки. Например,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 1 & 2 & 5 \end{pmatrix} = \begin{pmatrix} 4 & 1 & 3 & 2 \\ 5 & 1 & 2 & 1 \end{pmatrix}$$

изображают одно и то же отображение $\underline{4} \longrightarrow \underline{5}$, а именно, отображение, переводящее 1 и 2 в 1, 3 в 3 и 4 в 5.

Перечислим, например, все отображения из $\underline{2}$ в $\underline{2}$:

$$\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}.$$

Табличная запись особенно часто используется для изображения **перестановок** степени n, т.е. биективных отображений $\underline{n}$ на себя (см. § ?). Элементы второй строки перестановки с точностью до порядка совпадают с элементами первой строки и встречаются по одному разу. Изобразим, для примера, все перестановки множества $\underline{3}$:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Табличная запись часто называется еще **полной записью** перестановки, в отличие от **сокращенной записи**, в которой перестановка изображается второй строкой своей таблицы. При этом подразумевается, что в первой строке элементы множества $\underline{n}$ располагаются в **естественном** порядке, т.е. как $1, 2, \ldots, n$.

§ 11. Полиномиальные функции

В следующих примерах через R обозначается произвольное **коммутативное кольцо**. Это означает, что элементы R можно складывать и умножать, причем операции сложения и умножения в R подчиняются обычным правилам действий над числами. Тот, кто пока не знаком с этим понятием, может представлять себе, что $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ или $\mathbb{C}$. В действительности последние три из этих числовых образований являются **полями**, т.е. в них, кроме того, можно делить на любое ненулевое число.

1. Сумма и произведение функций. Пусть, вначале, X – произвольное множество, а R – поле. Тогда для любых двух функций $f, g : X \longrightarrow R$ можно определить две новые функции $f + g, fg : X \longrightarrow R$, называемые **суммой** и **произведением** f и g, соответственно. Чтобы задать эти функции, достаточно определить их значение в каждой точке $x \in X$. Эти значения определяются как сумма и произведение значений f и g в точке x, соответственно:

$$(f + g)(x) = f(x) + g(x) \qquad (fg)(x) = f(x)g(x).$$

Уже эти простейшие операции позволяют строить громадный запас новых функций, отправляясь от нескольких простейших базисных функций, таких,

как тождественное отображение id и константы co_c. Например, умножая функцию f на постоянную функцию co_c мы получаем **скалярное кратное** cf функции f, т.е. функцию, значения которой определяются посредством $(cf)(x) = cf(x)$, иными словами, значение cf в точке x равно произведению значения f в x на c. В частности, так получается функция $-f = (-1)f$, называемая **противоположной** к f. А имея противоположную функцию мы можем определить **разность** функций $f-g$ как $f+(-g)$. Таким образом, по определению, значение функции $f-g$ в точке x равно $(f-g)(x) = f(x)-g(x)$.

2. Полиномиальные функции. Пусть, далее, $f \in K[t]$ – произвольный многочлен от одной переменной t над полем K. Напомним, что наивно под многочленом подразумевается *выражение* вида $f = a_n t^n + \ldots + a_1 t + a_0$, где $a_i \in K$. Многочлену f можно сопоставить отображение $\overline{f} : K \longrightarrow K$ по следующему правилу: элемент $a \in K$ заменяется на постоянное отображение co_a, переменная t заменяется на тождественное отображение id_K, а сложение и умножение многочленов на сложение и умножение функций. Иными словами, отображение $\overline{f}$ переводит любой элемент $x \in K$ в **значение** $f(x)$ многочлена f в точке x, т.е. в элемент $f(x) = a_n x^n + \ldots a_1 x + a_0$ поля K, получающийся подставновкой x в многочлен f вместо переменной t и фактическим проведением операций в поле K.

Получающиеся так отображения $\overline{f}$, $f \in K[t]$, называются **полиномиальными функциями**, или, в алгебраической геометрии, **регулярными функциями**. Примерами полиномиальных функций являются отображения $x \mapsto 1$, $x \mapsto x^2$, $x \mapsto (x-1)^3$ и вообще любые функции, получающиеся из тождественного отображения и постоянных отображений применением сложения и умножения. Можно называть полиномиальные функции **полиномиальными отображениями**, но в алгебре этот последний термин обычно указывает на то, что рассматривается **многомерная** ситуация (несколько многочленов от нескольких переменных).

В школьном курсе f обычно отождествляется с $\overline{f}$. При этом $\overline{f}$ обозначается просто через f и в часто именно эта функция и **называется** многочленом. С точки зрения профессионального алгебраиста это **преступная** практика. Действительно, многочлен f *определяет* функцию $\overline{f}$. Более того, в обычно рассматриваемых в школьной программе случаях он, в свою очередь, *однозначно определяется* функцией $\overline{f}$. Тем не менее совершенно неправильно говорить, что он *является* этой функцией. Дело в том, что в других не менее важных случаях два различных многочлена могут определять одну и ту же полиномиальную функцию. Чем бы ни был многочлен, он заведомо не является функцией $f : K \longrightarrow K$. Как мы объясняем в книге III, если многочлен и можно *естественным образом* отождествить с какой-то функцией, то тогда уж с функцией $f : \mathbb{N}_0 \longrightarrow K$.

§ 12. Рациональные функции

В этом параграфе мы продолжим обсуждение примеров функций, встречавшихся в школьной программе. Здесь мы предполагаем, что K является некоторым полем, например, $K = \mathbb{Q}, \mathbb{R}$ или $\mathbb{C}$.

1. Множество нулей функции. Элемент $x \in X$ называется **нулем** функции $g : X \longrightarrow K$, если g обращается в 0 в точке x, т.е. $g(x) = 0$. Обозначим через

$X(g)$ **множество нулей** функции g, т.е.

$$X(g) = \{x \in X \mid g(x) = 0\}.$$

В случае, когда $g = \overline{f} : K \longrightarrow K$ – полиномиальная функция, определенная многочленом $f \in K[t]$, принято называть нули функции g **корнями** многочлена f в поле K. В элементарной математике часто говорят даже о 'корнях функции' g. Такое словоупотребление совершенно чуждо практике, принятой, скажем, в комплексном анализе, где испольуется исключительно термин 'нуль функции' (как в выражении 'нули и полюсы'). Более того, профессиональные алгебраические геометры обычно говорят даже о 'нулях многочленов'.

Обозначим через X_g дополнение к множеству нулей функции g, т.е. множество тех точек $x \in X$, в которых функция f **не обращается** в 0.

$$X_g = X \setminus X(g) = \{x \in X \mid g(x) \neq 0\}.$$

Точки, в которых g не обращается в 0, называются еще **ненулями** функции g.

Комментарий. В случае, когда множество X конечно или дискретно, естественно называть X_g **носителем** функции g, и обозначать его через $\mathrm{Supp}(g)$. Однако основной случай, который нас будет интересовать в настоящем параграфе – это случай полиномиального отображения $g : K \longrightarrow K$. Для бесконечного поля K называть X_g носителем не совсем уместно. Дело в том, что любое поле K естественно снабжается коконечной топологией (совпадающей в этом случае с топологией Зариского), а в случае топологических пространств носителем функции обычно называется **замыкание** множества ее ненулей. Тем самым в случае бесконечного поля носителем любой ненулевой полиномиальной функции является все поле K, а вовсе не множество ненулей этой функции.

2. Частное функций. Пусть $f, g : X \longrightarrow K$ – две функции с значениями в поле K. Тогда их **частным** называется функция $f/g : x \mapsto f(x)/g(x)$. Частное двух функций не определено в нулях функции g, т.е тех $x \in X$, для которых $g(x) = 0$. Таким образом, с теоретико-множественной точки зрения $f/g : X_g \longrightarrow K$. Это значит, что по отношению к исходной области определения X функций f и g их частное f/g является, вообще говоря, лишь **частичной функцией**, т.е. отображает в Y не само множество X, а лишь его подмножество X_g. Тем не менее, с категорной точки зрения (принятой, скажем, в алгебраической геометрии) f/g является морфизмом X в K. Чтобы отметить этот факт и сохранить X в обозначениях, обычно пишут $f/g : X \dashrightarrow K$, где стрелка $\dashrightarrow$, TEXнически называемая `\dashrightarrow`, указывает на то, что f/g не является **всюду определенным**. Ясно, что функция f/g в том и только том случае всюду определена, когда g нигде не обращается в 0, т.е. $g(x) \neq 0$ для всех $x \in X$.

3. Рациональные функции. Неформально, рациональными функциями называются функции, получающиеся из постоянных отображений и тождественного отображения применением **рациональных** алгебраических операций сложения, умножения и деления на ненулевую функцию. Дадим теперь точное определение. По причинам, которые станут ясны через мгновение, мы предпочтем отступить от школьной терминологии и называть отношение двух полиномиальных функций **рациональным отображением**.

Определение. Рациональным отображением *называется отображение вида* $f/g : K_g \longrightarrow K$, *где* f *и* g *суть две полиномиальные функции* $K \longrightarrow K$, *причем* $g \neq 0$.

Напомним, что $g \neq 0$ означает, что найдется хотя бы одно $x \in X$, для которого $g(x) \neq 0$. Примерами рациональных отображений являются полиномиальные функции, которые в этом контексте называются еще **целыми** рациональными функциями. А вот несколько примеров рациональных отображений, не являющихся целыми (и, следовательно, вообще говоря, не всюду определенных!):

$$x \mapsto \frac{1}{x}, \qquad x \mapsto \frac{x}{x+1}, \qquad x \mapsto \frac{x-3}{x^2+1}, \qquad x \mapsto \frac{x^2+x+1}{x^2-1}.$$

Задача. Где определены указанные выше отображения?

Ответ. Ну, по крайней мере для третьего и четвертого из них это зависит от того, над каким полем мы их рассматриваем.

4. Равенство рациональных функций. Нюанс здесь состоит в том, что обычно используемое понятие равенства рациональных функций **отличается** от общего понятия равенства отображений. А именно, по определению $f : x \mapsto x^2/x$ является рациональным отображением. Совпадает ли оно с тождественным отображением $\mathrm{id}_K : x \mapsto x$. Если использовать общее определение равенства отображений, то **нет**, так как области определения этих отображений различны. В самом деле, id_K всюду определена на K, в то время как f определена лишь в тех точках, где знаменатель дроби x^2/x не обращается в 0, т.е. лишь для $x \neq 0$. Таким образом, $D(f) = K \setminus \{0\} \neq K = D(\mathrm{id}_K)$.

В то же время, любой школьный учебник алгебры скажет Вам, что $x^2/x = x$. Для этого в школьной программе вводится понятие 'естественной области определения' рациональной функции. Следующее неформальное рассуждение служит лишь мотивировкой последующего формального определения, поэтому мы сохраняем в нем всю нечистоплотность элементарного подхода. А именно, пусть f/g – любое рациональное отображение. Молчаливо отождествив полиномиальные функции с соответствующими многочленами и вспомнив арифметические свойства многочленов, можно найти *наибольший общий делитель* числителя и знаменателя, скажем h. Тогда, $f = f_0 h$, $g = g_0 h$, где f_0 и g_0 *взаимно просты*. После этого множество K_{g_0} провозглашается **естественной областью определения** функции f/g, причем значение f/g в точке $x \in K_{g_0}$ определяется как $(f/g)(x) = f_0(x)/g_0(x)$. Таким образом, 'естественная область определения' рациональной функции f/g может быть строго шире, чем область определения f/g как рационального отображения, что и наблюдается, например, для функции $x \mapsto x^2/x$. А теперь формализуем описанное выше рассуждение.

5. Ростки отображений. Это значит, что в действительности под рациональной функцией' в школьной программе подразумевается вовсе не рациональное отображение, а нечто совсем другое, и сейчас мы покажем, как можно придать смысл пересказанной выше чепухе. Для этого напомним, что подмножество A множества X называется **коконечным** (co-finite), если $X \setminus A$ конечно. Множество всех коконечных подмножеств в X обозначается через Cof_X.

Задача. Докажите, что Cof_X образует **фильтр** в 2^X, а именно,

1) Если A и B коконечны, то и $A \cap B$ коконечно;

2) Если A коконечно и $A \subseteq B$, то и B коконечно.

Определение. Ростком *отображений из X в Y называется класс эквивалентности отображений $f : X_f \longrightarrow Y$, где X_f – некоторое коконечное подмножество в X, относительно следующего отношения эквивалентности: $f \sim g$ в том и только том случае, когда $f|_{X_f \cap X_g} = g|_{X_f \cap X_g}$.*

Задача. Покажите, что описанное в этом определении отношение действительно является отношением эквивалентности на множестве частичных отображений $f : X \dashrightarrow Y$ с коконечной областью определения.

Указание. Воспользуйтесь предыдущей задачей.

Описанные выше ростки представляют собой так называемые **общие** или **родовые** ростки функций (generic germs). Они определяются посредством открытых множеств коконечной топологии, совпадающей в случае поля с топологией Зариского. Только они обычно и будут

нас интересовать в алгебре, в связи с рациональными функциями. Разумеется, в геометрии и анализе обычно рассматривают ростки относительно **других** фильтров, например, фильтра окрестностей данной точки ('росток в точке'), фильтра множеств, дополнение к которым имеет меру 0, и т.д.

6. Ростки рациональных отображений. Теперь ясно, что, например, отображения $f : x \mapsto x/x$ и $g : x \mapsto x - 1/x - 1$ будучи **разными** отображениями, принадлежат одному и тому же **ростку**. В самом деле, первое из них определено на $K \setminus \{0\}$, а второе на $K \setminus \{1\}$, но на пересечении их областей определения $K \setminus \{0, 1\}$ они совпадают. Теперь мы готовы дать правильное определение рациональной функции.

Определение. Рациональной функцией $h : K \dashrightarrow K$ *называется росток рациональных отображений из* K *в* K.

Любое рациональное отображение $f/g : K_g \longrightarrow K$, принадлежащее данному ростку, **представляет** данную рациональную функцию. При этом существует единственное рациональное отображение $f_0/g_0 : K_{g_0} \longrightarrow K$, область определения которого содержит области определения всех других рациональных отображений, представляющих данную рациональную функцию. Тогда K_{g_0} и называется **естественной областью определения** этой рациональной функции. Множество $K(g_0)$ нулей функции g_0 называется множеством **полюсов** рациональной функции f/g.

§ 13. Алгебраические функции

Что такое алгебраическая функция переменных $x_1, \ldots, x_n$? Обычно говорят, что это функция, удовлетворяющая алгебраическому уравнению

$$f(x_1, \ldots, x_n, y) = 0.$$

В случае функций одной независимой переменной это просто функции удовлетворяющие алгебраическому уравнению $f(x, y) = 0$, т.е., иными словами,

$$f_n(x)x^n + \ldots + f_1(x)y + f_0(x) = 0.$$

По этому определению выходит, что $y = |x|$ алгебраическая функция, так как она удовлетворяет алгебраическому уравнению $y^2 - x^2 = 0$. Конечно, это глупость, но причина здесь принципиальная. Дело в том, что алгебраическая функция по самой сути своей многозначна и в $|x|$ в точке 0 происходит скачок с ветки на ветку.

Многозначные функции. Обобщим понятие отображения. Скажем, что задана многозначная функция $f : X \multimap Y$, если каждому $x \in X$ сопоставлено непустое подмножество в Y. Существует два основных способа свести понятие многозначной функции к понятию отображения.

- Рассматривать многозначную функцию как отображение $X \mapsto 2^Y$.
- Рассматривать многозначную функцию как отображение $\widetilde{X} \mapsto Y$.

Мы не будем пытаться дать общее определение алгебраической функции, а ограничимся несколькими примерами и пояснениями, достаточными, чтобы охватить те алгебраические функции, которые встречались в школьной программе.

Любая рациональная функция является алгебраической. А вот несколько примеров **иррациональных** алгебраических функций:

$$x \mapsto \sqrt{x-1}, \qquad x \mapsto \sqrt{x} - 1, \qquad x \mapsto \sqrt[3]{\sqrt{x} - 1}, \qquad x \mapsto \frac{1 - \sqrt{x}}{1 + \sqrt{1}}.$$

Пусть теперь K – поле, скажем, $K = \mathbb{R}, \mathbb{C}$. Вообще, алгебраическая функция переменной x – это функция f, удовлетворяющая уравнению $F(x, f) = 0$, где $F \in K[x, y]$ многочлен от двух переменных. Вообще говоря, алгебраическая функция не является отображением. Дело в том, что одному значению аргумента как правило соответствует несколько различных значений функции.

Функция $x \mapsto \sqrt{x}$. Если ограничиться вещественными числами, то вообще невозможно определить $\sqrt{x}$ в случае, когда $x < 0$. Поэтому в элементарной математике обычно говорят, что $\sqrt{x}$ определен только если $x \geq 0$. С другой стороны, в этом случае все равно существует два значения корня $\sqrt{x}$ и в элементарной математике совершенно произвольно выбирается один из них, а именно, неотрицательный. Таким образом, $x \mapsto \sqrt{x}$ рассматривается как функция $\mathbb{R}_+ \longrightarrow \mathbb{R}_+$.

Настоящее решение проблемы многозначности состоит не в том, чтобы считать, что одному аргументу сопоставляется множество значений, а в том, чтобы создать несколько копий аргумента. Именно в этом состоит идея введения римановых поверхностей.

§ 14. 'Элементарные' функции

> Я стал немного забывать теорию функций. Ну, это восстановится. Врач обещал ... врет, наверно.
>
> Владимир Высоцкий. 'Дельфины и психи (записки сумасшедшего)'

Мы не будем пытаться дать математическое определение выражению 'элементарная функция'. В обычном словоупотреблении это выражение не является математическим термином, а означает, примерно, 'функция встречающаяся или употребляемая в элементарной математике[194]. Вот какое (де)лирическое определение дается, например, в Математической Энциклопедии: '**Элементарные функции** – класс функций, состоящий из *многочленов, показательных функций, логарифмических функций, тригонометрических функций* и *обратных тригонометрических функций*, а также функций, получающихся из перечисленных выше с помощью арифметических операций и суперпозиции, примененных конечное число раз.' Например, из этого определения совершенно неясно, где определены элементарные функции. Интересно, что авторы справочника[195] не пытаются дать определение 'элементарной функции', а просто рассматривают основные примеры. Аналитические функции, не являющиеся элементарными, принято называть **специальными**.

Комментарий 1. Ясно, почему на элементарном уровне никто не пытался дать определение элементарной функции. Ведь нет ни одной теоремы, которая начиналась бы так: 'Пусть f – элементарная функция. Тогда ...' А там, где нет доказательств, не нужны и точные определения. Именно такой характер носит большая часть прикладной математики – разумеется, не *настоящих* **приложений** математики, которыми занимались **математики** первого ряда, а *фиктивной* прикладной математики, которой занимаются **прикладные** математики[196,197], которые скрывают бессодержательность своей деятельности и свое непонимание

---

[194]'Аналитическая функция – функция встречающаяся или употребляемая в анализе'.

[195]Л.А.Люстерник, О.А.Червоненкис, А.Р.Янпольский, Математический анализ, Вычисление элементарных функций. – Физматгиз, М., 1963, с.1–247.

[196]'Кто прикладывает математика?' – 'Who applies the mathematician?'.

[197]'Applied Mathematics is **bad** mathematics' – Paul Halmos.

духа математики мнимым прикладным характером своих исследований. Типичными иллюстрациями являются теория нечетких множеств, классический хаос, в особенности, 'теория' фракталей[198] и пр.

Комментарий 2. Для меня лично, классе так в 7-м, главной трудностью при изучении школьной математики было понять, что часть даваемых в школьных учебниках 'определений' является настоящими математическими определениями, часть можно превратить в настоящие математические определения, а часть носит чисто лингвистический характер. **Основная** цель изучения математики в школе – воспитание интеллектуальной честности. С этой точки зрения **худшее**, что может быть, это смешивать настоящие определения и псевдо-определения, наподобие приведенного выше 'определения' элементарных функций.

Комментарий 3. Это не значит, что выражение элементарная функция *не имеет* математического смысла. Напротив, абсолютно точный смысл выражению 'элементарная функция' был придан Лиувиллем и именно этот смысл инструментален в дифференциальной алгебре. А именно, элементарной функцией называется функция, принадлежащая некоторому полю, получающемуся из конечного расширения поля рациональных функций присоединением конечного числа интегралов и экспонент от интегралов.

Поэтому мы не будем пытаться определить элементарные функции, а просто перечислим основные элементарные функции, рассматривавшиеся в школьной программе. Инвариантный смысл этих функций состоит в том, что они являются единственными непрерывными гомоморфизмами между аддитивной и мультипликативной структурами вещественных чисел (см. Книгу II). В книге IV мы даем правильные определения всех этих функций в комплексной области, а в Книге V – линейные заивсимости между ними.

- **Показательная функция**: $\mathbb{R} \longrightarrow \mathbb{R}^+$, $x \mapsto c^x$, где $c \in \mathbb{R}_+$.
- **Степенная функция**: $\mathbb{R}_+ \longrightarrow \mathbb{R}_+$, $x \mapsto x^c$, где $c \in \mathbb{R}$.
- **Логарифм** $\mathbb{R}_+ \mapsto \mathbb{R}$, $x \mapsto \log_c(x)$, где $c \in \mathbb{R}_+$, $c \neq 0$.

Следующие два примера функций определяются как линейные комбинации показательных функций. Они тоже естественно возникают в книгах II и IV как компоненты гомоморфизмов $\mathbb{R} \mapsto \mathrm{GL}(2, \mathbb{R})$.

- **Круговые функции**: $\mathbb{R} \mapsto \mathbb{R}$, $x \mapsto \cos(x)$ и $x \mapsto \sin(x)$.
- **Гиперболические функции**: $\mathbb{R} \mapsto \mathbb{R}$, $x \mapsto \mathrm{ch}(x)$ и $x \mapsto \mathrm{sh}(x)$.

§ 14. Трансцендентные функции

1. Алгебраически трансцендентные функции. Общим для всех элементарных функций является то, что они удовлетворяют очень простым функциональным уравнениям (теоремы сложения, Книга II) и очень простым дифференциальным уравнениям (Книга IV). Напомним, что функция f называется **алгебраически трансцендентной**, если она удовлетворяет алгебраическому дифференциальному уравнению, изучение таких функций составляет предмет **дифференциальной алгебры**. С чисто алгебраической точки зрения[199] алгебраически трансцендентная функция – это функция, производные которой порождают поле конечной степени трансцендентности над $\mathbb{Q}$. **Все** элементарные функции – и большинство наиболее употребительных специальных функций (такие как функции Бесселя и многие

[198] Я не утверждаю, что в теории фракталей нет математического субстрата – наоборот, **за ней** стоит очень содержательная математика. Я утверждаю лишь, что коммерческая деятельность Бенуа Мандельброта & Co^o не удовлетворяет принятым в математике стандартам.

[199] J.F.Ritt, E.Gourin, An assemblage-theoretic proof of the existence of transcendentally transcendental functions. – Bull. Amer. Math. Soc., 1927, vol.33, p.182–184.

другие) – являются алгебраически трансцендентными. Класс алгебраически трансцендентных функций является кольцом, замкнутым относительно композиции и перехода к обратным функциям[200]

Гамма-функция. Первый пример **трансцендентно трансцендентной** функции был построен Эйлером, это знаменитая **Гамма-функция**, определяемая интегральным представлением

$$\Gamma(x) = \int_0^\infty t^{x-1}e^{-t}dt,$$

Однако первое безукоризненное доказательство того, что эта функция не удовлетворяет никакому алгебраическому дифференциальному уравнению, было получено только в самом конце XIX века Отто Гельдером[201]. Позже Александр Островкий получил совсем простое доказательство[202] основанное на бесконечном спуске с использованием функционального уравнения $\Gamma(x+1) = x\Gamma(x)$.

Сразу после работы Гельдера Адольф Гурвиц рассматривая очень быстро сходящиеся ряды построил целые классы трансцендентно трансцендентных функций[203] наподобие

$$\sum_{n=0}^{\infty} \frac{x^n}{(n^n)!}.$$

Много дальнейших примеров можно найти в статье[204]

§ 15. Характеристическая функция подмножества

Упомянутое в предыдущем параграфе обозначение Y^X для множества всех отображений из X в Y согласовано с обозначением 2^X для множества всех подмножеств множества X, о котором шла речь в Главе 2.

1. Определение. *Сопоставим подмножеству $A \subseteq X$* **характеристическую функцию** $\chi_A : X \longrightarrow \{0,1\}$*, принимающей на $x \in X$ значение 1, если $x \in A$ и 0 в противном случае:*

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

Очевидно, что подмножество $A \subseteq X$ однозначно определяется своей характеристической функцией χ_A, т.е. для двух таких подмножеств

$$A = B \qquad \Longleftrightarrow \qquad \chi_A = \chi_B$$

Таким образом 2^X действительно эквивалентно $\{0,1\}^X$.

2. Поле $\mathbb{F}_2 = \{0,1\}$ из двух элементов. Напомним, что на множестве $\{0,1\}$ естественно вводятся операции сложения и умножения, называемые **булевыми** сложением и умножением или, иначе, сложением и умножением **по модулю**

---

[200] A.Ostrowski, Über Dirichletsche Reihen und algebraische Differentialgleichungen. – Math. Z., 1920, Bd.8, S.241–298.

[201] O.Hölder, Über die Eigenschaft der Gamma Funktion keiner algebraische Differentialgleichung zu genügen. – Math. Ann., 1887, Bd.28, S.1–13.

[202] A.Ostrowski, Zum Hölderschen Satz über $\Gamma(x)$. – Math. Ann., 1925, Bd.94, S.248–251.

[203] A.Hurwitz, Sur le développement des fonctions satisfaisant à une équation différentielle algébrique. – Ann. Ecole Norm. Sup., 1889, t.6, p.327–332

[204] L.A.Rubel, A survey of transcendentally transcendental functions. – Amer. Math. Monthly, 1989, vol.96, N.9, p.777–788.

2. Эти операции известны в логике и computer science как разделительная дизъюнкция `xor` и конъюнкция `and`, соответственно. Напомним их таблицы Кэли:

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Множество $\{0,1\}$ с этими операциями называется **полем из 2-х элементов** и обозначается $\mathbb{F}_2$. Начинающему проще всего мыслить себе это поле следующим образом. Будем считать, что 0 – это множество $2\mathbb{Z}$ четных чисел, а 1 – это множество $2\mathbb{Z}+1$ нечетных чисел. Тогда приведенные выше таблицы Кэли в точности описывают четность/нечетность результата сложения/умножения четных или нечетных чисел. Например, сумма двух нечетных чисел четна, что и объясняет правило $1+1=0$.

3. Характеристические функции и булевы операции. Смысл введения операций на множестве $\{0,1\}$ состоит в том, что теперь мы можем выразить булевы операции на подмножествах множества X в терминах операций над их характеристическими функциями.

Задача. Докажите, что для любых двух подмножеств $A, B \subseteq X$ имеют место равенства

i) $\chi_{A\cap B} = \chi_A\chi_B$,

ii) $\chi_{A\triangle B} = \chi_A + \chi_B$,

iii) $\chi_{A\cup B} = \chi_A + \chi_B + \chi_A\chi_B$,

iv) $\chi_{A\setminus B} = \chi_A + \chi_A\chi_B$.

Результаты этой задачи служат еще одним аргументом в пользу того, чтобы рассматривать $\cap$ как **произведение** множеств, и $\triangle$ – а вовсе не $\cup$ – как **сумму** множеств.

4. Характеристические функции со значениями в $\mathbb{Z}$. Иногда удобно считать, что значения 0 и 1 характеристической функции являются целыми числами и действия над ними производятся по обычным правилам действия над целыми числами. Например, в этом случае число элементов конечного подмножества $A \subseteq X$ будет выражаться как сумма $\sum \chi_A(x)$, $x \in X$, в то время как образовав подобную сумму по модулю 2, мы можем узнать лишь, четное или нечетное число элементов содержит множество A. Однако в этом случае выражение булевых операций в терминах операций над характеристическими функциями чуть сложнее.

Задача. Докажите, что если интерпретировать 0 и 1 в определении характеристической функции не как элементы поля $\mathbb{F}_2$, а как целые числа, то правило i) из предыдущей задачи не меняется, а правила ii) – iv) приобретают следующую форму:

ii)$'$ $\chi_{A\triangle B} = \chi_A + \chi_B - 2\chi_A\chi_B$,

iii)$'$ $\chi_{A\cup B} = \chi_A + \chi_B - \chi_A\chi_B$,

iv)$'$ $\chi_{A\setminus B} = \chi_A - \chi_A\chi_B$.

§ 16. Множество всех отображений

1. Множество отображений $\mathrm{Map}(X,Y)$**. Множество** всех **отображений** из X в Y обозначается обычно одним из следующих трех образов: $\mathrm{Map}(X,Y)$ (от английского map или mapping – отображение), $\mathrm{Mor}(X,Y)$ (от английского morphism – особенно употребительно в последнее время под влиянием теории категорий), либо, наконец, Y^X (обратите внимание, что именно Y^X, а не X^Y!).

Первые два обозначения ясны сами по себе, а последнее связано с тем обстоятельством, что действительно имеет место равенство мощностей $|Y^X| = |Y|^{|X|}$. Это обозначение согласовано с обозначением 2^X для множества всех подмножеств множества X, о котором шла речь в § 1. В самом деле, любое подмножество $A \subseteq X$ может быть однозначно описано с помощью своей **характеристической функции** $\chi_A : X \longrightarrow \{0,1\}$, принимающей на $x \in X$ значение 1, если $x \in A$ и 0 в противном случае. Таким образом 2^X действительно эквивалентно $\{0,1\}^X$.

Задача. Докажите, что все отображения из X в Y действительно образуют множество.

Решение. Если X и Y заданы, то отображение $f : X \times Y$ полностью опрелеляется своим графиком Z, который является подмножеством в $X \times Y$. Таким образом, $\mathrm{Map}(X,Y)$ может быть отождествлено с подмножеством в $2^{X\times Y}$, состоящим из всех $Z \in 2^{X\times Y}$, удовлетворяющих условию $\forall x \in X\ \exists! y \in Y$, $(x,y) \in Z$. Таким образом, существование $\mathrm{Map}(X,Y)$ вытекает из аксиомы степени, аксиомы подмножеств и существования прямого произведения.

Задача (Правило степени). Доказать, что $\mathrm{Map}(X,Y) = |Y|^{|X|}$.

Решение. Вытекает из рассмотренного нами в предыдущей главе правила произведения. В самом деле, каждое отображение из X в Y можно отождествить с элементом произведения $Y \times \ldots \times Y$, где число множителей равно $|X|$.

§ 17. Ограничение и продолжение отображения

1. Ограничение отображения. Отображение задается как тройка, состоящая из области, кообласти и графика. Это оправдывает следующее определение.

Определение. *Говорят, что отображение f является* **подотображением** *отображения g и пишут $f \subseteq g$, если выполняются три следующих условия:*

1) $D(f) \subseteq D(g)$;

2) $R(f) \subseteq R(g)$;

3) $f(x) = g(x)$ *для любого* $x \in D(f)$.

Пусть теперь $f \in \mathrm{Map}(X,Y)$ и $A \subseteq X$. Тогда f однозначно определяет отображение $g \in \mathrm{Map}(A,Y)$, по правилу $g(x) = f(x)$ для любого $x \in A$. Это отображение называется **ограничением** (Beschränkung) отображения f на A и обозначается $f|_A$, а в некоторых контекстах, где фигурирует много различных подмножеств и нужна особая точность в указании того, что, откуда и куда ограничивается, также $\mathrm{res}^X_A(f)$ (от английского restriction). Таким образом, ограничение можно рассматривать как отображение $\mathrm{res}^X_A : \mathrm{Map}(X,Y) \longrightarrow \mathrm{Map}(A,Y)$.

2. Продолжение отображения. Наоборот, если задано отображение $g \in \mathrm{Map}(A,Y)$, то его можно продолжить до отображения $f \in \mathrm{Map}(X,Y)$, вообще говоря, многими различными способами. Любое отображение $f \in \mathrm{Map}(X,Y)$ такое, что $f|_A = g$, называется **продолжением** отображения g. Иногда, особенно если при этом происходит игра не только с областью определения, но и с областью значений, говорят также о **сужении** (Einschränkung) и **расширении** отображений.

Комментарий. Особенный интерес будут представлять для нас случаи, когда в *каком-то классе отображений* существует **единственное** продолжение: 'продолжение по линейности', 'продолжение до гомоморфизма' и т.д. Такие ситуации определяют так называемые 'универсальные' или 'свободные' объекты, примерами которых являются, среди прочего, свободные модули (в частности, векторные пространства и свободные абелевы группы); свободные группы; групповые и полугрупповые алгебры (в частности, кольца многочленов, многочленов Лорана и т.д.), тензорные, симметрические и внешние алгебры и т.д. Также и в анализе такие ситуации чрезвычайно важны ('продолжение по непрерывности', 'аналитическое продолжение'), а некоторые большие разделы математики, такие как теория обыкновенных дифференциальных уравнений и дифференциальных уравнений с частными производными, занимаются почти исключительно изучением возможности продолжения отображений, заданных 'начальными' или 'краевыми' условиями ('задача Коши', 'задача Дирихле' и т.д.).

§ 18. Образы и прообразы

Важнейшими понятиями, которыми начинающий должен полностью овладеть, для того, чтобы сознательно использовать отображения и понимать их свойства, являются понятия образа и прообраза.

1. Образ подмножества. Пусть $f : X \longrightarrow Y$ и $A \subseteq X$. Тогда $f(A) = \{f(x) \mid x \in A\}$ называется **образом** множества A относительно (или под действием) отображения f. Отметим три частных случая этого определения:

a) $f(\varnothing) = \varnothing$;

b) Для любого $x \in X$ выполняется $f(\{x\}) = \{f(x)\}$;

c) Образ $f(X)$ области $X = D(f)$ под действием f обозначается обычно $\mathrm{Im}(f)$ (от английского `image`) и называется **образом отображения** f. Иными словами, $\mathrm{Im}(f)$ – это множество таких $y \in Y$, для которых существует такое $x \in X$, что $f(x) = y$.

2. Прообраз и полный прообраз элемента. Вообще говоря, для $y \in \mathrm{Im}(f)$ может существовать много x со свойством $f(x) = y$. Любой $x \in X$ такой, что $f(x) = y$ называется **прообразом** y (alias **обратным образом** y, сравни определение обратной функции ниже и обратного отношения в § 3).

Множество *всех* прообразов некоторого $y \in Y$ обозначается $f^{-1}(y)$ и называется **полным прообразом** элемента Y (а в геометрическом контексте **слоем** f над y или **множеством уровня** f, отвечающим значению y). Разумеется, если $y \notin \mathrm{Im}(f)$, то $f^{-1}(y) = \varnothing$.

Вообще, для любого подмножества $B \subseteq Y$ его **полный прообраз** $f^{-1}(B)$ определяется как $f^{-1}(B) = \{x \in X \mid f(x) \in B\}$. Ясно, что $f^{-1}(B) = \cup f^{-1}(y)$, $y \in B$.

Задача. Пусть $Y \subseteq X$, $\iota : Y \hookrightarrow X$ – каноническое вложение. Тогда для любого подмножества $Z \subseteq X$ имеем $\iota^{-1}(Z) = Z \cap Y$.

3. Коллизия обозначений. Предположим, что подмножество $A \subseteq X$ само является элементом X. Как различить значение функции f на элементе A и ее образ на подмножестве A, если и то и другое обозначается через $f(A)$? Куратовский и Мостовский [KM] вводят обозначение $f^1(A)$ для образа на подмножестве A, т.е. $\mathrm{Im}(f|_A)$. При этом они смело пишут $f^{-1}(A)$, а ведь использование этого обозначения ведет точно к такой же двусмысленности! Nobody is perfect.

Как показывает следующая задача, это несовершенство обозначений может приводить к серьезным ошибкам ([Bu], задача II–3–11).

Задача. Найти ошибку в следующем рассуждении: Пусть $\mathbb{N}$ – множество натуральных чисел, A – множество целых чисел $n > 2$, для которых существуют

три таких строго положительных целых числа x, y, z, что $x^n + y^n = z^n$. Множество A непусто (иначе говоря, "великая теорема Ферма" неверна). В самом деле, пусть $B = \{A\}$ и $C = \{\mathbb{N}\}$; так как B и C – множества, состоящие из единственного элемента, то существует биекция f множества B на множество C. Таким образом, $f(A) = \mathbb{N}$; если бы A было бы пусто, то мы получили бы $\mathbb{N} = f(\varnothing) = \varnothing$, что абсурдно.

4. Прообраз образа и образ прообраза. Пусть, как обычно, $f : X \longrightarrow Y$ – отображение X в Y, $A \subseteq X$, $B \subseteq Y$.

Задача. Докажите, что для любого подмножества $A \subseteq X$ и любого подмножества $B \subseteq Y$ имеют место включения

1) $A \subseteq f^{-1}(f(A))$,

2) $B \supseteq f(f^{-1}(B))$.

Приведите примеры того, что эти включения могут быть строгими. В действительности, как мы увидим в §§ 21 и 24, требование, чтобы первое из этих включений превращалось в равенство, выделяет класс инъективных отображений, а превращение в равенство второго из этих включений – класс сюръективных отображений.

Задача. Покажите, что $f^{-1}(B) = f^{-1}(B \cap f(X))$. Таким образом, равенство $B = f(f^{-1}(B))$ имеет место в том и только том случае, когда $B \subseteq f(X)$.

5. Согласованность полного прообраза с булевыми операциями. Оказывается, что полный прообраз ведет себя замечательно по отношению к теоретико-множественным операциям.

Задача. Пусть $f : X \longrightarrow Y$. Доказать, что для любых двух подмножеств $A, B \subseteq Y$ имеют место равенства

1) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$,

2) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$,

3) $f^{-1}(A \setminus B) = f^{-1}(A) \setminus f^{-1}(B)$.

6. Поведение образа относительно булевых операций. Поведение же образа несколько сложнее, некоторые из перечисленных выше равенств сохраняются, но другие становятся включениями, вообще говоря, строгими.

Задача. Пусть $f : X \longrightarrow Y$. Доказать, что для любых двух подмножеств $A, B \subseteq X$ имеет место

1) $f(A \cup B) = f(A) \cup f(B)$,

2) $f(A \cap B) \subseteq f(A) \cap f(B)$,

3) $f(A \setminus B) \supseteq f(A) \setminus f(B)$,

привести примеры, показывающие, что включения в пунктах 2) и 3) могут быть строгими.

7. We all make mistakes. С неравенством в пункте 2 этой задачи связана еще одна забавная история на тему "nobody is perfect" или "we all make mistakes". Доказательство основного результата в одной статье Лебега 1905 года использует следующее утверждение: проекция на прямую пересечения *убывающей* последовательности множеств на плоскости равна пересечению их проекций.

Незадача[205]**.** За 20 секунд найти очевидный контрпример к утверждению Лебега.

[205]David Gale, We all make mistakes II – Math. Int., 1992, V.14, N.1, P.54.

Решение. Зафиксируем $x \in \mathbb{R}$ и рассмотрим множества $X_n = \{(x,y) \mid 0 < y < 1/n\}$, $n \in \mathbb{N}$. Тогда $\bigcap X_n = \varnothing$. В то же время $\mathrm{pr}_1(X_n) = \{x\}$ для любого $n \in \mathbb{N}$, так что $\bigcap \mathrm{pr}_1(X_n) = \{x\}$.

Лемма в работе Лебега была сформулирована без доказательства, видимо он считал ее очевидной. Контрпример к этому очевидному утверждению был обнаружен Михаилом Суслиным в 1916 году и привел Суслина и Лузина к созданию теории аналитических множеств. 'Очевидные' (но неверные!) утверждения – один из основных источников математических ошибок, наряду с неправильным цитированием чужих результатов.

Само определение слова 'очевидно' совершенно не является очевидным: "Ce que l'un voit, l'autre ne le voit pas". Стивен Кранц[206] пересказывает следующий фрагмент Принстонского фольклора: "In the fifties, it was said in Princeton that there were four definitions of the word "obvious". If something was obvious in the sense of Beckenbach, then it is true and you can see it immediately. If something is obvious in the sense of Chevalley, then it is true and it will take you several weeks to see it. If something is obvious in the sense of Bochner, then it is false and it will take you several weeks to see it. If something is obvious in the sense of Lefschetz, then it is false and you can see it immediately." Там же он вспоминает определение теоремы, "верной в смысле Картана": "A theorem was true in the sense of Cartan, if Grauert could not find a counterexample in the space of one hour."

§ 19. Уравнитель отображений

Сейчас мы введем еще одну из важнейших конструкций, связанных с отображениями, которая объясняет, что такое *на самом деле* 'решение уравнений', о котором столько говорится в школьном курсе математики.

1. Уравнитель. Вот еще один важнейший случай расслоенных произведений.

Определение. *Пусть $f, g : X \longrightarrow Y$ – два отображения с одной и той же областью и кообластью. Их* **уравнителем** *называется подмножество*

$$E = \mathrm{Eq}(f,g) = \{x \in X \mid f(x) = g(x)\} \subseteq X.$$

Обозначение $\mathrm{Eq}(f,g)$ подсказано английским названием `equaliser`[207], которое в некоторых более новых книгах передается по-русски *без затей* как **эквализатор** или вовсе **эквалайзер**! С другой стороны, во многих старых книгах уравнитель называется **разностным ядром** или даже беззастенчиво просто **ядром** (от английского difference kernel). Эта последняя терминология *крайне* неудачна, как для множеств, где мы придали слову 'ядро' совершенно другой смысл, так и в общем случае. Например, в теории групп уравнителями являются *произвольные* подгруппы, в то время как ядрами лишь *нормальные* подгруппы! Кроме того, уравнители действительно отвечают за решение **уравнений**.

Задача: уравнивающие отображения. Пусть E – уравнитель пары f, g. Докажите, что тогда вложение $i : E \longrightarrow X$ действительно является **уравнивающим отображением** для отображений f и g. Это значит, что

i) $f \circ i = g \circ i$, и, во-вторых, что i является **универсальным** отображением с таким свойством, т.е. выполняется следующее условие.

ii) Для любого множества Z и любого отображения $h : Z \longrightarrow X$ такого, что $f \circ h = g \circ h$, существет единственное отображение $k : Z \longrightarrow E$ такое, что $h = i \circ k$.

---

[206] S.G.Krantz, Mathematical anecdotes. – Math. Int., 1990, vol.12, N.4, p.32–38.

[207] Следует иметь в виду, что здесь, как и **всюду** в настоящем курсе, мы используем исключительно британскую орфографию, американское написание этого слова `equalizer`. В дальнейшем подобные разночтения, как правило, не комментируются.

2. Решение уравнений. Мы остановились на термине ‘уравнитель’ не из почвенных соображений (“Mein Reich ist in der Luft”), а исключительно для того, чтобы подчеркнуть, что речь здесь идет, по существу, об основной теме школьной алгебры – решении уравнений. **Решить уравнение** $f(x) = g(x)$ на языке теории множеств означает найти уравнитель $E(f, g)$. При этом элементы этого уравнителя, т.е. те элементы $x \in X$, для которых фактически выполняется равенство $f(x) = g(x)$, называются **решениями** или, в некоторых ситуациях, **корнями** этого уравнения.

Например, в случае, когда $X = Y = K$ есть некоторое поле, $E(f, g) = E(f-g, 0)$, так что вычисление любых уравнителей сводится к сравнению функции с постоянной функцией $0 = \mathrm{co}_0$. Элементы $x \in K$, для которых $f(x) = 0$ называются в этом случае **корнями** функции f. Не будет большим преувеличением сказать, что около трех четвертей школьного курса алгебры посвящено решению алгебраических уравнений. Напомним, что **алгебраическим** уравнением (или, если быть совсем точным, **целый алгебраическим** уравнением) называется уравнение вида $f(x) = 0$, где f – полиномиальная функция.

Тут, правда, есть один существенный нюанс. Во многих важных ситуациях, например, в случае алгебраических уравнений, говоря о решении уравнения $f(x) = g(x)$, обычно имеют в виду нахождение уравнителя функций f и g не в категории множеств, а в категории **мультимножеств**, т.е. корни уравнения ищутся вместе с их **с кратностями**. Это значит, например, что вещественные решения уравнений $x = 0$ и $x^2 = 0$ **различны**, потому что кратность корня 0 равна 1 в первом случае и 2 во втором, хотя соответствующие теоретико-множественные уравнители совпадают.

§ 20. Предметы и ящики

Математик (*вынимая из головы шар*)
Я вынул из головы шар.
Я вынул из головы шар.
Я вынул из головы шар.
Я вынул из головы шар.
Андрей Семенович
Положь его обратно.
Положь его обратно.
Положь его обратно.
Положь его обратно.

Даниил Хармс, Математик и Андрей Семенович

Сейчас мы обсудим еще одну традиционную метафору функции, которую любят использовать специалисты по комбинаторике и теории вероятностей.

1. Предметы и ящики. Вместо того, чтобы бесхитростно говорить об отображениях, традиционная комбинаторика повествует о **задачах размещения**, в которых требуется *разместить* n ‘предметов’ по m ‘ящикам’ (например, рассадить n кроликов по m клеткам, засунуть m шаров в n урн, раскрасить n стран в m цветов и т.д.). С нашей точки зрения речь идет об **отображениях** n-элементного множества X в m-элементное множество Y, удовлетворяющих определенным ограничениям. При этом элементы множества X соответствуют предметам, элементы множества Y – ящикам, а отображение f сопоставляет каждому предмету его ящик. При этом на отображение f могут накладываться те или иные условия.

2. Инъективные, сюръективные и биективные отображения. Отображение называется **инъективным**, если в каждый ящик попадает не более одного объекта. Про такое отображение можно сказать, что оно удовлетворяет **принципу запрета Паули**: два фермиона не могут иметь один и тот же набор квантовых чисел. Отображение называется **сюръективным**, если в каждый ящик попадает хотя бы один объект. Наконец, отображение называется **биективным**, если в каждый ящик попадает **ровно** один объект, иначе говоря, если оно одновременно инъективно и сюръективно. Множества инъективных, сюръективных и биективных отображений из X в Y обозначаются через $\mathrm{Inj}(X,Y)$, $\mathrm{Sur}(X,Y)$ и $\mathrm{Bij}(X,Y)$, соответственно.

3. Различимые и неразличимые предметы и ящики. Как предметы, так и ящики могут быть **различимыми**, **неразличимыми** или **частично различимыми**. Это значит, что мы можем подсчитывать число отображений $X \longrightarrow Y$ с какими-то ограничениями, либо число **орбит** таких отображений под действием симметрических групп S_X и/или S_Y (см. ?.?) или каких-либо их подгрупп. При этом мы будем получать существенно различные ответы. Например, существует m способов положить один предмет в m различимых ящиков и единственный способ положить этот же предмет в m неразличимых ящиков. С точки зрения индивидуального студента совершенно не все равно, какую оценку он получил на экзамене, но с точки зрения статистики успеваемости важно лишь **сколько** студентов получило на экзамене оценку 'почти удовлетворительно' или 'весьма хорошо'. В некоторых разделах комбинаторики (например, в теории графов) в этом контексте обычно говорят о **помеченных** и **непомеченных** предметах и ящиках.

§ 21. Инъективные отображения

Следующий класс отображений на каждом шагу встречается в математике. В действительности, очень часто нам нужны такие функции, для которых значение аргумента x однозначно определяется значением функции $f(x)$.

Определение. *Если полный прообраз $f^{-1}(y)$ каждой точки $y \in Y$ содержит не более одного элемента, то отображение $f : X \longrightarrow Y$ называется* **инъективным**.

Иными словами, отображение f инъективно, если для любых $x_1, x_2 \in X$ равенство $f(x_1) = f(x_2)$ влечет равенство $x_1 = x_2$. Инъективные отображения часто называются просто **инъекциями**. Слово 'инъекция' латинского происхождения и означает 'вложение'. Однако в русском математическом узусе термин 'вложение' обычно применяется только к ситуации, когда $X \subseteq Y$, причем отображение a переводит каждый x в себя. Чтобы подчеркнуть, что f инъекция, используется специальная запись $f : X \rightarrowtail Y$, а для обозначения того, что f вложение – запись $f : X \hookrightarrow Y$. TEXнически стрелка '$\rightarrowtail$' называется `\rightarrowtail`, а стрелка '$\hookrightarrow$', соответственно, `\hookrightarrow`. Множество инъективных отображений из X в Y обозначается через $\mathrm{Inj}(X,Y)$.

Возвратимся теперь к вопросу об образе прообраза и прообразе образа, который мы рассматривали в § ?.

Задача. Покажите, что следующие условия эквивалентны:

1) $f : X \longrightarrow Y$ – инъективно,

2) Для любого подмножества $A \subseteq Y$ выполняется равенство $A = f^{-1}(f(A))$.

Задача. Покажите, что инъективность отображения $f : X \longrightarrow Y$ эквивалентна тому, что для любых $A, B \subseteq X$ имеет место равенство $f(A \cap B) = f(A) \cap f(B)$. Убедитесь, что достаточно даже накладывать это требование только на такие пары, что $A \cap B = \varnothing$.

Задача. Покажите, что инъективность отображения $f : A \longrightarrow B$ эквивалентна тому, что для любых $A, B \subseteq X$ имеет место равенство $f(A \setminus B) = f(A) \setminus f(B)$. Убедитесь, что достаточно даже накладывать это требование только на такие пары, что $A \subseteq B$.

Задача. Покажите, что если $g \circ f$ инъективно, то f инъективно.

Примеры инъективных отображений. Приведем первые примеры инъективных отображений. Много таких примеров встретится нам в дальнейшем.

• Если $Y \subseteq X$, то каноническое вложение $\hookrightarrow: Y \hookrightarrow X?\ y \mapsto y$, инъективно.

• Для любых двух множеств X, Y и *любого* отображения $f : X \mapsto Y$ отображение $(\mathrm{id}, f) : X \mapsto X \times Y$, $x \mapsto (x, f(x))$, инъективно.

• Для любого множества X отображение $X \mapsto 2^X$, $x \mapsto \{x\}$, инъективно (но никогда не является сюръективным!)

§ 22. Число инъективных отображений: перестановки и факториалы

Здесь мы вычислим количество инъективных отображений n-элементного множества в m-элементное.

1. Убывающий факториал. Пусть $m, n \in \mathbb{N}_0$. Выражение $[n]_m = n(n-1)\dots(n-m+1)$ называется **убывающим факториалом** длины m. Для $m = 0$ произведение пусто, поэтому $[n]_0 = 1$ для всех $n \in \mathbb{N}_0$.

2. Задача. Доказать, что $|\operatorname{Inj}(X, Y)| = [|Y|]_{|X|}$.

Сейчас мы введем еще одну версию факториала, которая становится интересной, если инъективность не имеет места.

3. Возрастающий факториал. Пусть $m, n \in \mathbb{N}_0$. Выражение $[n]^m = n(n+1)\dots(n+m-1)$ называется **возрастающим факториалом** длины m. Для $m = 0$ произведение пусто, поэтому $[n]^0 = 1$ для всех $n \in \mathbb{N}_0$.

4. Задача. Найти число **упорядоченных** размещений n предметов по m ящикам.

Указание. А как Вы думаете, зачем мы определили возрастающий факториал? Для доказательства нужно лишь заметить, сколькими способами можно разместить i-й объект, если $i-1$ объект уже размещены.

5. Задача (о трех поросятах). Перечислите все упорядоченные размещения трех поросят в трех домиках. С точки зрения волка отнюдь не все равно не только то, в каком именно домике (соломенном, деревянном или каменном) находятся поросята, но и то, в каком порядке съедать поросят, оказавшихся в одном домике. Он может начать с самого жирного или, наоборот, оставить самого жирного на десерт. Эта задача во всех вариантах (неразличимые/различимые поросята/домики, инъективность/неинъективность, сюръективность/несюръективность – если поросята построили пять домиков – и т.д.) обсуждается в книге Мацумаса Анно 'Три поросенка', адресованной 1-му классу японской школы (5-6 лет).

5. Факториал. Напомним, что **факториал** $n!$ числа $n \in \mathbb{N}_0$ определяется как $n! = 1 \cdot \ldots \cdot n$. Для $n = 0$ произведение пусто, поэтому $0! = 1$. Таким образом, $[n]_m = n!/(n-m)!$.

6. Задача. Доказать, что $|\operatorname{Bij}(X,Y)| = |X|!$ в случае $|X| = |Y|$ и 0 в противном случае.

7. Симметрическая группа. Множество $S_X = \operatorname{Bij}(X,X)$ является группой относительно композиции отображений, называемой **симметрической группой** множества X.

8. Симметрическая группа степени n. Введем обозначение $\underline{n}$ для начального отрезка длины n натурального ряда: $\underline{n} = \{1, \ldots, n\}$. Группа $S_{\underline{n}}$ обозначается просто S_n и называется **симметрической группой степени** n. Элементы этой группы называются **перестановками степени** n или **перестановками** n **символов**, а сами числа $1, \ldots, n$ называются в этом последнем случае **символами**.

9. Задача. Сколькими способами можно расставить на шахматной доске 8 ладей так, чтобы они не били друг друга.

Комментарий. Легко видеть (и это существенно при классическом определении определителя) что таких способов $8! = 40320$. Это число попало в "Guinness book of world records" в следующем контексте. Английский колокольный звон (change ringing – 'переборы с вариациями') принципиально отличается от русского. Дело в том, что в Англии раскачивают не язык колокола, а сам колокол, поэтому вызванивание мелодии на английских колоколах невозможно. Грубо говоря, 'переборы с вариациями' сводятся к вызваниванию на n колоколах всех $n!$ перестановок. Делается это по памяти. Мировой рекорд вызванивания всех 8! перестановок на 8 колоколах составляет около 18 часов, см. книгу "Этюды о симметрии".

10. Задача. Клетки шахматной доски занумерованы целыми числами от 1 до 64 следующим образом: первая горизонталь, слева направо, – числами от 1 до 8; вторая горизонталь – числами от 9 до 16 и т.д. Какие значения может принимать сумма номеров клеток, на которых стоят 8 ладей, не бьющих друг друга?

§ 23. Принцип Дирихле

Сейчас мы обсудим один из важнейших принципов конечной комбинаторики, который будет постоянно использоваться на протяжении всего нашего курса.

1. Принцип клеток и кроликов. В наиболее простой форме **принцип Дирихле** утверждает, что если $|X| > |Y|$, то **не существует** инъективных отображений $f : X \longrightarrow Y$. Иными словами, если нам даны n шаров, которые мы хотим распределить по m ящикам, причем $n > m$, то хотя бы в одном ящике окажется по крайней мере два шара.

В русской учебной литературе этот принцип часто называется также **принципом клеток и кроликов**: если нам дано n кроликов, которых мы хотим рассадить по m клеткам, причем $n > m$, то хотя бы в одной клетке окажется по крайней мере два кролика. В англоязычной литературе этот же принцип обычно называется 'pigeonhole principle' – 'принцип ящика для писем': если имеются n писем, которые нужно распихать по m отделениям ящика для пи-

сем, причем $n > m$, то хотя бы в одном отделении окажется по крайней мере два письма.

Представляется совершенно невероятным, чтобы столь тривиальное наблюдение приводило к нетривиальным результатам, – но, как замечает по этому поводу Олег Александрович Иванов[208] – "однако ..."

Задача. Легко видеть, что шахматную доску размера 8×8 можно покрыть костяшками домино 2×1 так, чтобы каждая костяшка покрывала две соседние клетки. Можно ли сделать то же самое с доской из которой вырезаны две клетки на противоположных концах диагонали?

Решение. Нет, потому что костяшка домино покрывает одну белую и одну черную клетку, а обе вырезанные клетки одного цвета (при этом неважно даже, что вырезаны клетки на одной из **главных** диагоналей).

Задача. Покажите, что для любого покрытия шахматной доски $\times 6$ костяшками домино 2×1 существует такое разрезание доски вертикальной или горизонтальной линией, которое не разрезает ни одной костяшки. Верно ли то же самое для доски 8×8?

Указание. Сколько костяшек может разрезать такая линия?

Задача. На белую плоскость брызнули черной краской. Докажите, что найдутся две точки одного цвета на расстоянии 1 метр друг от друга.

Указание 1. Таких пар точек очень много.

Указание 2. Воспользуйтесь **принципом Лагранжа** и считайте, что 2 – переменная величина, например, что $2 = 3$. Тогда на белое пространство брызнули красками двух цветов, скажем черной и красной. Вам будет много легче увидеть решение.

Сформулируем теперь принцип Дирихле в чуть большей общности, как утверждение о ядре любого отображения m-элементного множества в n-элементное.

Задача (принцип Дирихле). Пусть $m = m_1 + \ldots + m_n - n + 1$ кроликов рассажены по n клеткам. Тогда найдется такой номер i, что в i-й клетке окажется по крайней мере m_i кроликов.

Указание. $+1$.

Задача. В классе 30 учеников. Андрюша Крылов сделал в диктанте 13 ошибок, а остальные меньше. Докажите, что найдутся три ученика, сделавшие одинаковое количество ошибок (или не сделавшие ни одной).

Задача. Докажите, что у некоторой натуральной степени числа 17 семь последних цифр равны 0000001.

Задача. Группа из 21 студента **успешно** сдала сессию из трех экзаменов. Докажите, что по крайней мере 3 студента сдали сессию с одинаковыми оценками.

§ 24. Сюръективные отображения

Не реже, чем инъективные отображения, в математике встречаются и такие отображения, для которых каждый элемент области значений действительно является одним из значений функции.

[208] О.А.Иванов, Избранные главы элементарной математики. – Изд-во СПбГУ, Гл.7, откуда и взяты задачи 3, 5 и 6.

Определение. *Если* $\mathrm{Im}(f) = Y$*, то отображение* $f : X \longrightarrow Y$ *называется* **сюръективным**.

Иными словами, это условие означает, что для каждого $y \in Y$ найдется хотя бы одно $x \in X$ такое, что $f(x) = y$. В этом случае говорят также, что f отображение '**на**' (вместо обычного '**в**'). Слово **сюръекция** латинского происхождения и означает 'наложение'. Чтобы подчеркнуть, что f сюръекция, используется специальная стрелка $f : X \twoheadrightarrow Y$. TEXнически стрелка '$\twoheadrightarrow$' называется `\twoheadrightarrow`. Множество сюръективных отображений из X на Y обозначается через $\mathrm{Sur}(X, Y)$.

Задача. Покажите, что следующие условия эквивалентны:

1) $f : X \longrightarrow Y$ – сюръективно,

2) Для любого подмножества $B \subseteq Y$ выполняется равенство $B = f(f^{-1}(B))$.

Задача. Покажите, что если $g \circ f$ сюръективно, то g сюръективно.

Примеры сюръективных отображений. Упомянем несколько примеров, некоторые из которые будут детально анализироваться в дальнейшем.

• Если $\sim$ – отношение эквивалентности на множестве X, а $X/\sim$ – множество классов этой эквивалентности (фактор-множество по отношению $\sim$), то каноническая проекция $\pi : X \longrightarrow X/\sim$, $x \mapsto \overline{x}$, сопоставляющая каждому элементу его класс, сюръективна.

• Для любых двух множеств X, Y каноническая проекция $\mathrm{pr}_1 : X \times Y \longrightarrow X$, $(x, y) \mapsto x$, на сомножитель сюръективна.

• Для любого множества X отображение $X^2 \setminus \Delta_X \mapsto \bigwedge^2(X)$, $(x, y) \mapsto \{x, y\}$, сюръективно (бывает ли оно когда-нибудь инъективным?)

Следующий принципиальный результат описывает поведение сюръективных и инъективных отображений относительно функтора степени. Это, вероятно, самое важное и самое полезное утверждение о связи сюръективности и инъективности.

Теорема. *Отображение* $F : 2^Y \longrightarrow 2^X$, $B \mapsto f^{-1}(B)$ *в том и только том случае инъективно, когда исходное отображение* $f : X \longrightarrow Y$ *сюръективно. Отображение* F *в том и только том случае сюръективно, когда отображение* f *инъективно.*

Доказательство. !!!

Задача: функция Жуковского. Рассмотрим отображение $f : \mathbb{C}^* \longrightarrow \mathbb{C}$, заданное посредством $z \mapsto (z + 1/z)/2$. Является ли оно инъективным? Сюръективным? Чтобы ответить на первый из этих вопросов, не обязательно знать комплексные числа.

Ответ. Нет, так как $f(1/z) = f(z)$. Да, так как равенство $f(z) = w$ представляет собой квадратное уравнение относительно z с ненулевым свободным членом. Такое уравнение имеет ненулевой корень в $\mathbb{C}$.

§ 25. Биективные отображения

Не может быть более семи металлов, по числу планет: Солнцу соответствует золото, Луне – серебро, Меркурию – ртуть, Марсу – железо, Сатурну – свинец, Венере – медь, Юпитеру – олово.

Джероламо Кардано

Совершенно особую роль в теории множеств играют такие отображения, которые устанавливают **одно-однозначное соответствие** между областью определения и областью значений (`1-to-1-correspondence`).

Определение. *Отображение, $f : X \longrightarrow Y$, которое как инъективно, так и сюръективно, называется* **биективным** (*alias* **изоморфизмом**) *или* **взаимно однозначным**.

Это означает, что для любого $y \in Y$ существует единственный $x \in X$ такой, что $f(x) = y$. Когда нужно подчеркнуть, что f биекция, используется специальная стрелка $f : X \longleftrightarrow Y$. TEXнически стрелка '$\longleftrightarrow$' называется `\longleftrightarrow`. Множество биективных отображений из X на Y обозначается через $\mathrm{Bij}(X, Y)$. Если существует биекция из X в Y, то говорят, что между элементами X и Y можно установить **взаимно-однозначное соответствие** ('1-to-1 correspondence').

Биективное отображение X на себя называется обычно **перестановкой** множества X, этот термин особенно употребим в случае, когда X конечно. С точки же зрения теории категорий биективное отображение X на себя называется **автоморфизмом**. Множество всех биективных отображений X на себя часто обозначается $S(X)$ или S_X (эта группа изучается в Книге II).

Комбинируя результаты Задач обсуждавшихся в §§ 21 и 24, мы видим, что отображение $f : X \longrightarrow Y$ в том и только том случае биективно, когда для любого подмножества $B \subseteq Y$ выполняется равенство $B = f(f^{-1}(B))$ и для любого подмножества $A \subseteq Y$ выполняется равенство $A = f^{-1}(f(A))$. Мы вернемся к этой теме в § ?.

Примеры биективных отображений. Приведем несколько очевидных примеров, много дальнейших примеров обсуждается в Главе V.

- Отображение $\mathbb{R} \longrightarrow \mathbb{R}$, $x \mapsto x^3$, биективно.
- Отображение $\mathbb{R}_+ \longrightarrow \mathbb{R}_+$, $x \mapsto x^2$, биективно.
- Для любого множества X отображение $2^X \longrightarrow 2^X$, $Y \mapsto X \setminus Y$, биективно.
- Для любого множества X отображение $X \mapsto \bigwedge^1(X)$, $x \mapsto \{x\}$, биективно.

§ 26. Композиция отображений

1. Композиция отображений. Два отображения f и g такие, что $R(f) = D(g)$ можно **скомпонировать**. Точнее, пусть $f : X \longrightarrow Y$ и $g : Y \longrightarrow Z$ суть два отображения, область значений первого из которых совпадает с областью определения второго. Тогда их **композиция** $g \circ f : X \longrightarrow Z$ задается посредством равенства $(g \circ f)(x) = g(f(x))$, для любого $x \in X$. При этом $g \circ f$ читается как 'композиция f и g' или 'g кружочек f' (TEXнически кружочек '$\circ$' называется `\circ`). Обратите внимание на порядок факторов: отображение f, действующее первым, записывается вторым. Это связано с тем, что мы пишем функцию слева от аргумента, как $f(x)$. Разумеется, если бы мы использовали обозначение $(x)f$, то и композиция f и g записывалась бы как $f \circ g$, по формуле $(x)(f \circ g) = ((x)f)g$. Композиция двух отображений часто называется также их **суперпозицией** или **произведением**.

2. Ассоциативность композиции. Самым важным свойство композиции отображений является ее ассоциативность.

Лемма. *Если одно из выражений* $(h \circ g) \circ f$ *и* $h \circ (g \circ f)$ *определено, то определено и второе и при этом* $(h \circ g) \circ f = h \circ (g \circ f)$.

Доказательство. Пусть, например, определено первое из этих отображений. По определению это означает, что $D(h) = R(g)$ и $D(g) = D(h \circ g) = R(f)$. Но тогда, конечно, определено и $g \circ f$ и, кроме того $R(g \circ f) = R(g) = D(h)$, так что второе отображение действительно определено. Равенство же этих отображений доказывается следующей выкладкой:

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = (h(g(f(x))) = h((g \circ f)(x)) = (h \circ (g \circ f))(x).$$

См. § 7 по поводу некоторых следствий из ассоциативности.

3. Некоммутативность композиции. Композиция отображений весьма далека от коммутативности, т.е. для двух отображений f и g, вообще говоря, $f \circ g \neq g \circ f$. Это ясно хотя бы из того, что одна из частей равенства $f \circ g = g \circ f$ может быть определена без того, чтобы была определена другая, т.е. из равенства $R(f) = D(g)$ отнюдь не следует, что $R(g) = D(f)$. Но даже если как $f \circ g$, так и $g \circ f$ обе определены, они могут быть совершенно различны. Например, если $f, g : \mathbb{N} \longrightarrow \mathbb{N}$ задаются как $f(n) = n^2$ и $g(n) = n + 1$, то $(g \circ f)(n) = n^2 + 1$, в то время как $(f \circ g)(n) = (n + 1)^2$, так что для любого натурального n значения функций $f \circ g$ и $g \circ f$ различны.

4. Композиция с постоянным отображением. Пусть $f : X \longrightarrow Y$ – произвольное отображение, а $\mathrm{co}_z : Y \longrightarrow Z$ – постоянное отображение. Чему равна композиция $\mathrm{co}_z \circ f$? А чему равна композиция $f \circ \mathrm{co}_x$, для постоянного отображения $\mathrm{co}_x : U \longrightarrow X$? Сравните эти композиции в случае, когда $U = X = Y = Z$, а $x = z$.

Ответ. Первая из них равна $\mathrm{co}_z : X \longrightarrow Z$, а вторая $\mathrm{co}_{f(x)} : U \longrightarrow Y$. Ясно, что co_x и $\mathrm{co}_{f(x)}$ это, вообще говоря, совсем не одно и то же, по крайней мере если X содержит не менее двух элементов.

Вообще, говорят, что отображение $g : X \longrightarrow Y$ является **левым нулем** относительно композиции, если для любого отображения $f : X \longrightarrow X$ выполняется равенство $g \circ f = g$. Аналогично, g называется **правым нулем**, если для любого отображения $h : Y \longrightarrow Y$ выполняется равенство $h \circ g = g$.

Задача. Опишите все левые нули относительно композиции. При каком условии в $\mathrm{Map}(X, Y)$ существует правый нуль относительно композиции?

Решение. Если g левый нуль, то для любой постоянной функции $\mathrm{co}_x : X \longrightarrow X$ имеет место равенство $g = g \circ \mathrm{co}_x = \mathrm{co}_{f(x)}$, так что g является постоянной функцией, причем, как мы только что видели, постоянные функции действительно являются левыми нулями. С другой стороны, если g правый нуль, то для любой постоянной функции $\mathrm{co}_y : Y \longrightarrow Y$ имеет место равенство $g = \mathrm{co}_y \circ g = \mathrm{co}_y$, в частности, для любых двух $y, z \in Y$ имеем $\mathrm{co}_y = \mathrm{co}_z$, а это возможно только если $|Y| = 1$.

4. Нули в категории множеств с отмеченной точкой. Как мы только что убедились, двусторонних нулей в категории множеств и отображений, вообще говоря, нет. Категория множеств с отмеченной точкой устроена в этом отношении значительно лучше.

Задача. Покажите, что постоянное отображение $0_{XY} = c_* : X \longrightarrow Y$, переводящее все элементы множества X в выделенную точку $*_Y$, является левым

и правым нулем относительно композиции. Точнее, для любого отображения $f : U \longrightarrow X$ имеет место равенство $0_{UY} = 0_{XY} \circ f$, а для любого отображения $g : Y \longrightarrow Z$ имеет место равенство $0_{XZ} = g \circ 0_{XY}$.

Задача. Пусть K – некоторое поле, $f : K \longrightarrow K$ и $a \in K$. Когда f коммутирует со сдвигом на a?

Решение. Ясно, что $t_0 = \mathrm{id}_K$ – тождественное отображение и оно коммутирует с любым f. В общем случае $(f \circ t_a)(x) = f(x + a)$, в то время как $(t_a \circ f)(x) = f(x) + a$. Таким образом, для того, чтобы f коммутировала с t_a, необходимо выполнение функционального уравнения $f(x+a) = f(x)+a$. Ясно, что решениями этого уравнения являются в точности функции вида $g+\mathrm{id}$, где g периодическая функция с периодом a.

§ 27. Итерации отображений

Последовательное n-кратное применение отображения $f : X \longrightarrow X$ называется n-й **итерацией** f и обозначается $f^{\circ n} = f \circ \ldots \circ f$ (отображение f применяется n раз). Согласно этому определению, $f^{\circ 0} = \mathrm{id}_X$, $f^{\circ 1} = f$. Например, во многих вопросах теории сложности вычислений и в некоторых вопросах теории чисел возникают кратные экспоненты и кратные логарифмы:

$$\exp^n(x) = \exp(\exp^{n-1}(x)), \qquad \ln^n(x) = \ln(\ln^{n-1}(x)).$$

Рассмотрим итерации функции $f : x \mapsto \frac{1}{1+x}$, вот, например, как выглядит $f^{\circ 17}$:

$$\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+x}}}}}}}}}}}}}}}}$$

Разумеется, этот *аутпут* не написан от руки, а получен с помощью

```
recip[x_]:=1/(1+x);      TeXForm[Nest[recip,x,17]]
```

Вообще, команда `Nest[f,x,n]` вычисляет значение $f^{\circ n}(x)$. В `Mathematica` есть и другая команда, `NestList[f,x,m]`, связанная с итерациями функции f, которая генерирует *список* значений $(x, f(x), f^2(2), \ldots, f^n(x))$. Вот, например, что мы получим при помощи `TeXForm[NestList[recip,x,5]]`:

$$x, \quad \frac{1}{1+x}, \quad \frac{1}{1+\frac{1}{1+x}}, \quad \frac{1}{1+\frac{1}{1+\frac{1}{1+x}}}, \quad \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+x}}}}, \quad \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+x}}}}}$$

Задача. Покажите, что $f^{\circ(m+n)} = f^{\circ m} \circ f^{\circ n}$

Указание. Заметьте, что $f^{\circ n} = f^{\circ(n-1)} \circ f$ и воспользуйтесь индукцией.

Определение. *Говорят, что $f : X \longrightarrow X$ – отображение* **конечного порядка**, *если найдется такое $n \in \mathbb{N}$, что $f^{\circ n} = \mathrm{id}_X$. Если такого натурального n не существует, то говорят, что порядок f бесконечен.*

Задача. Докажите, что если $f^{\circ n} = \mathrm{id}_X$, то f – биекция.

Задача. Вычислите n-ю итерацию отображения $x \mapsto x/\sqrt{1+x^2}$.

Ответ. $x \mapsto x/\sqrt{1+nx^2}$.

Замыкание, внутренность, граница. В топологическом пространстве X заданы различные отображения $2^X \longrightarrow 2^X$, наиболее известными из которых являются отображения замыкания Cl, внутренности Int и границы Fr. Известно, что $\mathrm{Cl}^{\circ 2} = \mathrm{Cl}$ и $\mathrm{Int}^{\circ 2} = \mathrm{Int}$, но, вообще говоря, $\mathrm{Fr}^{\circ 2} \neq \mathrm{Fr}$. В то же время $\mathrm{Fr}^{\circ 3} = \mathrm{Fr}^{\circ 2}$.

Определение. *Пусть $f \in \mathrm{Map}(X, X)$ и $x \in X$. Тогда множество $x^{\langle f \rangle} = \{f^{\circ n}(x), x \in \mathbb{N}_0\}$ называется* **полуорбитой** *точки x под действием отображения f.*

Мы не называем $x^{\langle f \rangle}$ орбитой, так как две орбиты должны либо не пересекаться, либо совпадать. В то же время две полуорбиты могут пересекаться нетривиальным образом, не будучи равными.

§ 28. Обратное отображение

Тождественные отображения действительно ведут себя как нейтральные элементы для композиции функций, но отсутствие коммутативности накладывает свой отпечаток. А именно, для отображений из $\mathrm{Map}(X, Y)$ тождественное отображение id_X выступает как **правая единица**, а id_Y – как **левая единица**. Иными словами, для любого $f \in \mathrm{Map}(X, Y)$ имеем $f \circ \mathrm{id}_X = f = \mathrm{id}_Y \circ f$. По отношению к отображениям X в себя id_X является уже **двусторонней единицей**.

Самым важным свойством биективных отображений является то, что они обратимы. Иначе говоря, в этом случае сопоставление $y \mapsto f^{-1}(y)$ задает биективное отображение $f^{-1} : Y \longrightarrow X$, называемое отображением, **обратным** к f, см. ниже. При этом $(f^{-1})^{-1} = f$, так что в действительности f и f^{-1} совершенно равноправны. Для обозначения биекций иногда используется специальная стрелка, подчеркивающая симметрию X и Y: $X \longleftrightarrow Y$.

Пусть теперь $f \in \mathrm{Map}(X, Y)$ – любое отображение. Тогда f называется **обратимым слева**, если существует такое $g \in \mathrm{Map}(Y, X)$, что $g \circ f = \mathrm{id}_X$ (любое такое g называется **левым обратным** к f). Аналогично, f называется **обратимым справа**, если существует такое $g \in \mathrm{Map}(Y, X)$, что $f \circ g = \mathrm{id}_Y$ (любое такое g называется **правым обратным** к f). Отображение f называется **обратимым** (иногда для полной определенности говорят **двусторонне обратимым**), если оно обратимо как слева, так и справа.

Легко видеть (подробнее об этом см. § 7), что если f двусторонне обратимо, то левый и правый обратный к нему определены однозначно и совпадают между собой. Их общее значение обозначается f^{-1} и называется отображением обратным к f. Это в точности отображение, определенное выше посредством прообразов.

Теорема. *Для любых двух биекций f и g, для которых определена композиция, выполняется равенство $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$*

Курьез: когда $f^{-1} = 1/f$? Если $f : \mathbb{R} \longrightarrow \mathbb{R}$ – вещественнозначная функция вещественного аргумента, не обращающаяся в 0, то символу f^{-1} можно было бы придать еще один смысл, а именно, $1/f$. Здесь, как обычно, $(1/f)(x) = 1/f(x)$. Можно спросить себя, для каких функций $f^{-1} = 1/f$? Разумеется, на всей вещественной оси таких функций f не существует – ведь функция f не принимает значения 0 и, следовательно, f^{-1} не существует. Поэтому слегка изменим первоначальный вопрос и спросим, существуют ли функции $f : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ с этим свойством? Оказывается, такие функции существуют (см. [??], [??], [??]), но их настолько мало, и они устроены настолько специальным образом, что встретиться с ними практически невозможно. Одно очевидное ограничение на функции с этим свойством содержится в задаче в конце следующего пункта.

Задача. Докажите, что если для функции $f : \mathbb{R}_{>0} \longrightarrow \mathbb{R}_{>0}$ выполняется равенство $f^{-1} = 1/f$, то $(f \circ f)(x) = 1/x$ для любого $x \in \mathbb{R}_{>0}$. В частности, $f \circ f \circ f \circ f = \mathrm{id}$.

Примеры обратных отображений. Вот несколько очевидных примеров.

• Обратным к сдвигу t_a является сдвиг t_{-a}.

• Обратным к растяжению d_a является растяжение $d_{a^{-1}}$.

• Обратной функцией к возведению в квадрат $\mathbb{R}_+ \longrightarrow \mathbb{R}_+$, $x \mapsto x^2$, является извлечение квадратного корня $x \mapsto \sqrt{x}$.

Обратные тригонометрические функции. Если функция f не инъективна, в элементарной математике всегда стараются ограничить ее куда-то, где она уже будет инъективной и называют ‘обратной’ к функции f функцию обратную к подходящему *сужению* функции f. Именно так строятся в школьном курсе ‘обратные’ к тригонометрическим функциям.

• Ограничения функции cos на отрезок $[0, \pi]$ устанавливает биекцию этого отрезка на $[-1, 1]$. Обратная функция $\arccos : [-1, 1] \longrightarrow [0, \pi]$ называется арккосинусом.

• Ограничения функции cos на отрезок $[-\pi/2, \pi/2]$ устанавливает биекцию этого отрезка на $[-1, 1]$. Обратная функция $\arcsin : [-1, 1] \longrightarrow [-\pi/2, \pi/2]$ называется арксинусом.

• Ограничения функции tg на интервал $(\pi/2, \pi/2)$ устанавливает биекцию этого интервала с вещественной осью $\mathbb{R}$. Обратная функция $\mathrm{arctg} : \mathbb{R} \longrightarrow (\pi/2, \pi/2)$ называется арктангенсом.

Совершенно аналогично определяются и обратные гиперболические функции. В действительности, конечно, описанные выше функции задают одну из ветвей многозначных функций, связанных с комплексным логарифмом и мы вернемся к этому в Книге IV.

§ 29. Отображения в прямое произведение

Следующий факт является характеристическим свойством прямого произведения.

Теорема. *Для любых трех множеств X, Y, Z имеет место равенство*

$$\mathrm{Map}(X, Y \times Z) = \mathrm{Map}(X, Y) \times \mathrm{Map}(X, Z).$$

Задача. Верно ли, что

$$\mathrm{Inj}(X, Y \times Z) = \mathrm{Inj}(X, Y) \times \mathrm{Inj}(X, Z).$$

Ответ. Нет. Инъективных отображений в прямое произведение значительно *больше*, чем пар инъективных отображений в сомножители. Например, если множества X, Y и Z конечны, причем порядок X больше порядка каждого из множеств Y и Z, но меньше порядка их произведения, то инъективных отображений X в Y и Z вообще не существует (принцип Дирихле), а в $Y \times Z$ – существуют. Таким образом, в этом случае правая часть пуста, а левая – нет.

Задача. Существует ли прямое произведение в категории множеств и инъективных отображений?

Ответ. Нет. Если $\{*\}$ – синглетон, то для любого множества Z имеем

$$\mathrm{Inj}(\{*\}, Z) = \mathrm{Map}(\{*\}, Z) \cong Z.$$

Поэтому если прямое произведение Z двух множеств X и Y в категории множеств и инъективных отображений существует, то

$$Z \sim \mathrm{Inj}(\{*\}, Z) = \mathrm{Inj}(\{*\}, X) \times \mathrm{Inj}(\{*\}, Y) \cong X \times Y,$$

а мы только что видели, что это невозможно.

Задача. Верно ли, что

$$\mathrm{Sur}(X, Y \times Z) = \mathrm{Sur}(Z, Y) \times \mathrm{Sur}(X, Z)?$$

Ответ. Нет. Сюръективных отображений на прямое произведение значительно *меньше*, чем пар сюръективных отображений на сомножители. Например, если множества X, Y и Z конечны, причем порядок X больше порядка каждого из множеств Y и Z, но меньше порядка их произведения, то сюръективных отображений X на $Y \times Z$ вообще не существует, а сюръективные отображения X на каждое из множеств Y и Z существуют. Таким образом, в этом случае левая часть пуста, а правая – нет.

§ 30. Прямое произведение отображений

Сейчас мы вернемся к функториальность прямого произведения, о которой шла речь в Главе 3.

Определение. *Пусть $f : X \longrightarrow U$ и $g : Y \longrightarrow V$ суть два отображения. Их* **прямым произведением** *называется отображение $f \times g : X \times Y \longrightarrow U \times V$, заданное посредством $(x, y) \mapsto (f(x), g(y))$.*

Задача. Докажите, что прямое произведение отображений взаимно дистрибутивно относительно композиции.

Иными словами, если даны отображения

$$X_1 \xrightarrow{f_1} Y_1 \xrightarrow{g_1} Z_1 \qquad \text{и} \qquad X_2 \xrightarrow{f_2} Y_2 \xrightarrow{g_2} Z_2,$$

то тогда

$$(g_1 \times g_2) \circ (f_1 \times f_2) = (g_1 \circ f_1) \times (g_2 \circ f_2).$$

Обобщите на любое число сомножителей.

Задача. Докажите, что если даны отображения

$$X \xrightarrow{f_1} Y_1 \xrightarrow{g_1} Z_1 \qquad \text{и} \qquad X \xrightarrow{f_2} Y_2 \xrightarrow{g_2} Z_2,$$

то тогда

$$(g_1 \times g_2) \circ (f_1, f_2) = (g_1 \circ f_1, g_2 \circ f_2).$$

Задача. Верно ли, что прямое произведение двух инъекций является инъекцией? Прямое произведение двух сюръекций является сюръекцией?

Задача. Пусть над даны два отображения f и g и два подмножества $A \subseteq C(f)$ и $B \subseteq C(g)$. Верно ли, что

$$(f \times g)^{-1}(A \times B) = f^{-1}(A) \times g^{-1}(B).$$

§ 31. Склейка и копроизведение отображений

Определение. *Пусть $f : X \longrightarrow Z$ и $g : Y \longrightarrow Z$ суть два отображения таких, что $f|_{X\cap Y} = g|_{X\cap Y}$. Тогда отображение $f \uplus g : X \cup Y \mapsto Z$, определенное посредством*

$$(f \uplus g)(x) = \begin{cases} f(x) & \text{если } x \in X, \\ g(x) & \text{если } x \in Y, \end{cases}$$

называется **склейкой** *отображений f и g.*

Иными словами, график склейки $f \uplus G$ – это просто *объединение* графиков отображений f и g – *при условии*, что это объединение действительно является графиком некоторого отображения. При этом равенство $f|_{X\cap Y} = g|_{X\cap Y}$ как раз и гарантирует, что приведенная в этом определении формула задает отображение. Если это условие не выполнено, то найдется такое $x \in X \cap Y$, что $f(x) \neq g(x)$ и тогда эта формула является корректным определением отображения так как неясно, чему равно значение $f \uplus g$ в точке x. Если X и Y дизъюнктны, то это условие выполнено автоматически, так что можно склеить любые два отображения $f : X \longrightarrow Z$ и $g : Y \longrightarrow Z$. В этом случае склейка обычно называется копроизведением.

Определение. *Пусть $f : X \longrightarrow Z$ и $g : Y \longrightarrow Z$ суть два отображения. Тогда отображение $f \coprod g : X \coprod Y \mapsto Z$, определенное посредством*

$$(f \coprod g)(x) = \begin{cases} f(x) & \text{если } x \in X, \\ g(x) & \text{если } x \in Y, \end{cases}$$

называется **копроизведением** *отображений f и g.*

Ясно, что и обратно, отображению $h \in \mathrm{Map}(X \coprod Y, Z)$ можно сопоставить пару $(h|_X, h|_Y)$ составленную из ограничений h на X и Y.

Теорема. *Для любых трех множеств X, Y, Z имеет место равенство*

$$\mathrm{Map}(X \coprod Y, Z) = \mathrm{Map}(X, Z) \times \mathrm{Map}(Y, Z).$$

Доказательство. Нам нужно проверить, что сопоставления $h \mapsto (h|_X, h|_Y)$ и $(f, g) \mapsto f \coprod g$ взаимно обратны. В самом деле, ясно, что $h = h|_X \coprod h|_Y$ и, обратно, $(f \coprod g)|_X = f$ и $(f \coprod g)|_Y = g$.

Задача. Верно ли, что

$$\mathrm{Inj}(X \coprod Y, Z) = \mathrm{Inj}(X, Z) \times \mathrm{Inj}(Y, Z)?$$

Ответ. Нет, инъективных отображений копроизведения значительно *меньше*, чем пар инъективных отображений из X и Y в Z. Например, если X, Y и Z конечны, причем порядок Z больше, чем порядок каждого из множеств X и Y, но меньше, чем сумма их порядков, то левая часть пуста, а правая – нет.

Задача. Верно ли, что

$$\mathrm{Sur}(X \coprod Y, Z) = \mathrm{Sur}(X, Z) \times \mathrm{Sur}(Y, Z)?$$

Ответ. Нет, сюръективных отображений копроизведения значительно *больше*, чем пар сюръективных отображений из X и Y в Z. Например, если X, Y и Z конечны, причем порядок Z больше, чем порядок каждого из множеств X и Y, но меньше, чем сумма их порядков, то правая часть пуста, а левая – нет.

§ 32. Инъекции = мономорфизмы = коретракции

Оказывается, инъективные отображения можно естественно охарактеризовать в терминах композиции, не рассматривая образы индивидуальных элементов.

Определение. *Отображение $f : X \longrightarrow Y$ называется* **мономорфизмом**, *если на f можно* **сокращать слева**, *иными словами, если для любых двух отображений $g_1, g_2 : Z \longrightarrow X$ из равенства $f \circ g_1 = f \circ g_2$ вытекает, что $g_1 = g_2$.*

Определение. *Отображение $f \in \mathrm{Map}(X, Y)$ называется* **обратимым слева** *или* **коретракцией**, *если существует такое $g \in \mathrm{Map}(Y, X)$, что $g \circ f = \mathrm{id}_X$, любое такое g называется* **левым обратным** *к f.*

Теорема. *Для любого отображения $f : X \longrightarrow Y$ следующие утверждения эквивалентны*

1) *f инъективно,*
2) *f мономорфизм,*
3) *f обратимо слева.*

Доказательство. Импликация 3) $\Longrightarrow$ 2) тривиальна. В самом деле, пусть $h : Y \longrightarrow X$ – левый обратный к f, то есть $h \circ f = \mathrm{id}_X$. Тогда рассматривая композицию равенства $f \circ g_1 = f \circ g_2$ с h и воспользовавшись ассоциативностью композиции, мы видим, что из этого равенства вытекает, что $\mathrm{id}_X \circ g_1 = \mathrm{id}_X \circ g_2$, или, что то же самое, $g_1 = g_2$.

Импликацию 2) $\Longrightarrow$ 1) можно усмотреть следующим образом. Предположим, что f не является инъективным. Тогда найдутся элементы $x \neq y \in X$ такие, что $f(x) = f(y)$. Пусть теперь g_1 и g_2 – два отображения синглетона $Z = \{*\}$ в X, такие, что $g_1(*) = x$, а $g_2(*) = y$. Тогда $f \circ g_1(*) = f(x) = f(y) = f \circ g_2(*)$,

так что $f \circ g_1 = f \circ g_2$. Однако, очевидно, $g_1 \neq g_2$, так что f не является мономорфизмом.

Покажем, наконец, что 1) $\Longrightarrow$ 3). В самом деле, если f инъективно, то левый обратный к нему можно построить, *например*, следующим образом (в общем случае левый обратный совершенно не обязан быть единственным!). Зафиксируем какой-то элемент $z \in X$ и определим отображение $h : Y \longrightarrow X$ полагая

$$h(y) = \begin{cases} x & \text{если } f(x) = y, \\ z, & \text{если } y \notin \mathrm{Im}(f). \end{cases}$$

Так как f инъективно, для каждого $y \in \mathrm{Im}(f)$ существует *ровно одно* такое $x \in X$, что $f(x) = y$, так что этим действительно определяется *отображение* $h : Y \longrightarrow X$. Ясно, что $h \circ f = \mathrm{id}_X$.

§ 33. Сюръекции = эпиморфизмы = ретракции

В теории **ZFC** сюръективные отображения также можно естественно охарактеризовать в терминах композиции, не рассматривая образы индивидуальных элементов. Впрочем, эта характеризация **в точности** эквивалентна аксиоме выбора. В действительности, характеризация сюръективных отображений, о которой пойдет речь ниже, и была первой явной формулировкой аксиомы выбора, предложенной Беппо Леви.

Определение. *Отображение $f : X \longrightarrow Y$ называется* **эпиморфизмом**, *если на f можно* **сокращать справа**, *иными словами, если для любых двух отображений $g_1, g_2 : Y \longrightarrow Z$ из равенства $g_1 \circ f = g_2 \circ f$ вытекает, что $g_1 = g_2$.*

Определение. *Отображение $f \in \mathrm{Map}(X, Y)$ называется* **обратимым справа** *или* **ретракцией**, *если существует такое $g \in \mathrm{Map}(Y, X)$, что $f \circ g = \mathrm{id}_Y$, любое такое g называется* **правым обратным** *к f.*

Правое обратное отображение к f называется также **сечением** этого отображения. Оно сопоставляет каждому элементу $y \in Y$ *какой-то* прообраз этого элемента.

Аксиома Леви. *Сюръективное отображение обратимо справа.*

Теорема. *Для любого отображения $f : X \longrightarrow Y$ следующие утверждения эквивалентны*

1) *f сюръективно,*

2) *f эпиморфизм,*

3) *f обратимо справа.*

Доказательство. Импликация 3) $\Longrightarrow$ 2) очевидна. В самом деле, пусть $h : Y \longrightarrow X$ – правый обратный к f, то есть $f \circ h = \mathrm{id}_Y$. Тогда рассматривая композицию h с равенством $g_1 \circ f = g_2 \circ f$ и воспользовавшись ассоциативностью композиции, мы видим, что из этого равенства вытекает, что $\gamma_1 \circ \mathrm{id}_Y = \gamma_2 \circ \mathrm{id}_Y$, или, что то же самое, $g_1 = g_2$.

Импликацию 2) $\Longrightarrow$ 1) можно проверить, например, следующим образом. Предположим, что f не является сюръективным. Тогда найдется элемент $y \in X$ такой, что $y \notin \mathrm{Im}(f)$. Пусть теперь g_1 и g_2 – два отображения X в трехэлементное множество $\{0, 1, 2\}$, такие, что $g_1(x) = g_2(x) = 0$ для всех $x \in X$,

$x \neq y$, а значения этих отображений в точке y различны, $g_1(y) = 1$ и $g_2(y) = 2$. Так как $y \notin \mathrm{Im}(f)$, то для любого $z \in X$ имеем $g_1 \circ f(z) = 0 = g_2 \circ f(z)$, так что $g_1 \circ f = g_2 \circ f$. Однако, $g_1(y) = 1 \neq 2 = g_2(y)$, так что, $g_1 \neq g_2$, а это значит, что f не является эпиморфизмом.

Наконец, импликация 1) $\Longrightarrow$ 3) – это в точности аксиома Леви.

§ 34. Функции нескольких аргументов

Предположим, теперь, что $X \subseteq X_1 \times \ldots \times X_n$. В этом случае значение $f((x_1, \ldots, x_n))$ отображения f на n-ке $(x_1, \ldots, x_n)$ обычно обозначается просто $f(x_1, \ldots, x_n)$ и f рассматривается как '**функция** n **аргументов**' (или 'n **переменных**'). Вот простейшие примеры функций нескольких аргументов.

• **Проекции.** Пусть $X \times Y$ – произведение множеств X и Y. В предыдущей главе нам уже встречались отображения $\mathrm{pr}_1 : X \times Y \longrightarrow X$, $(x, y) \mapsto x$ и $\mathrm{pr}_2 : X \times Y \longrightarrow Y$, $(x, y) \mapsto y$.

• **Перестановки сомножителей.** Пусть снова $X \times Y$ – произведение множеств X и Y. Тогда $\mathrm{sw} : X \times Y \longrightarrow Y \times X$, $(x, y) \mapsto (y, x)$.

• **Расстояние.** Метрические пространства определяются заданием отображения $d : X \times X \longrightarrow \mathbb{R}_+$, называемого **расстоянием**, удовлетворяющего некоторым свойствам (которые подробно обсуждаются в Гл. ?). • **Алгебраические операции.** Бинарная алгебраическая операция есть по определению отображение $X \times X \longrightarrow X$. Примерами таких операций являются сложение и умножение целых чисел, т.е. отображения $\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$, определенные посредством $(x, y) \mapsto x + y$ и $(x, y) \mapsto xy$. Алгебраические операции подробно обсуждаются в Главе 1.

Некоторые функции, связанные с порядком.

• **Дельта-функция.** Функция $\delta : X \times X \longrightarrow \mathbb{Z}$ определенная посредством

$$\delta(x, y) = \begin{cases} 1 & x = y \\ 0 & x \neq y \end{cases}$$

называется **дельта-функцией**. Это характеристическая функция $\delta = \chi_\Delta$ диагонали $\Delta = \{(x, x) \mid x \in X\}$. Иногда значение $\delta(x, y)$ дельта-функции записывается как δ_{xy}. Это обозначение особенно часто используется для случая $X = \underline{n}$. Дельта-функция $\delta : \underline{n} \times \underline{n} \longrightarrow \mathbb{Z}$, $(i, j) \mapsto \delta_{ij}$ обычно называется **дельтой Кронекера**.

• **Дзета-функция.** Функция $\zeta : X \times X \longrightarrow \mathbb{Z}$ определенная посредством

$$\zeta(x, y) = \begin{cases} 1 & x \leq y \\ 0 & x > y \end{cases}$$

называется **дзета-функцией**. Это характеристическая функция $\zeta = \chi_Z$ графика $Z = \{(x, y) \in X^2 \mid x \leq y\}$ отношения '$\leq$'. Эту комбинаторную дзета-функцию не следует путать с арифметической ζ-функцией (ζ-функция Римана и ее обобщения).

Глава 5. Сравнение множеств по мощности

To see the world in a grain of sand,
And a heaven in a wild flower;
Hold infinity in the palm of your hand,
And eternity in an hour.

William Blake

Однако один лишь анализ еще не ведет нас к глубочайшему постижению сущности бесконечного. Этой цели скорее может способствовать научная дисциплина, стоящая ближе к общефилософскому подходу и призванная представить в новом свете весь комплекс вопросов, касающихся бесконечного. Этой дисциплиной является учение о множествах, создателем которого был Георг Кантор, и здесь мы рассмотрим только то действительно единственное в своем роде и оригинальное, что составляет истинное ядро канторовского учения, – его *теорию трансфинитных чисел*. Она представляется мне достойным наибольшего удивления цветком математического духа и вообще одним из высших достижений трезвого человеческого разума.

Давид Гильберт[209]

Основой арифметики Тлена является понятие бесконечных чисел. Особая важность придается понятиям большего и меньшего, которые нашими математиками обозначаются через $>$ и $<$. Математики Тлена утверждают, что сам процесс счета изменяет количество и превращает его из неопределенного в определенное. Тот факт, что несколько индивидуумов, подсчитывая одно и то же количество, приходят к одинаковому результату, представляет для психологов пример ассоциации идей или хорошего упражнения памяти.

Х.Борхес “Тлен, Укбар, Орбис Терциус”

В нашем мире Действия (Асия), так же как и в высших мирах Созидания (Иецира) и Творения (Брия), есть различие между субъектом и объектом, между совершающим действие и тем, над кем оно совершается. В то же время в высшем мире Эманации (Ацилут), в котором сфирот не отделены от своего источника в Б-жестве, этого различия нет. Поэтому явления в нижних мирах могут обладать определенностью, отдельностью. Даже ангел в мире творения (Брия), совершенное орудие Б-жественной воли, это все-таки существо со своим “Я”. Только в мире Эманации (Ацилут) нет границы между Творцом и творением, и Б-г и Его мир — едины. Следовательно, все, что мы можем так или иначе различить, каким бы великим оно ни было — не Б-г.

Адин Штайнзальц. Творящее слово

Бессмертная заслуга Георга Кантора состоит вовсе не в том, что он ввел в математический обиход термин ‘множество’, и не в том, что он изучил булевы операции над множествами – как сами эти операции, так и их свойства были хорошо поняты к началу XVIII века. Главным достижением Кантора – тем раем, который он **создал** для математиков – явилось признание бесконечных множеств как полноправных математических сущностей. Однако самая суть теории Кантора, его величайшее открытие, состоит в возможности **сравнения** бесконечностей.

[209]Д.Гильберт, О бесконечном. стр.436. – в книге: Д.Гильберт, Избранные Труды, т.I. – Факториал, М., 1998, с.431–448.

Первая из апорий Зенона, 'мера' редко цитируется. Между тем, с математической точки зрения она представляется мне наиболее интересной из всех, так как в ней впервые говорится о различии между счетными множествами и множествами мощности континуума. Замечательно, что более, чем за две тысячи лет вплоть до открытия Кантора, никто так и не смог осмыслить этого различия. Эта апория доказывает, что прямая не может состоять из точек. В самом деле, аргументирует Зенон. Если мера точки 0, то из точек нельзя составить отрезок, мера которого больше 0. Если же мера точки > 0, то мера любого отрезка бесконечна. Как решается эта апория в канторовской математике?

Кантор к

Мы будем использовать лишь две бесконечные мощности. Напомним, что множество A называется **счетным**, если оно равномощно $\mathbb{Z}$. В этом случае мы пишем $|A| = \aleph_0$ (произносится 'алеф-ноль'). Множество A называется **континуальным**, если оно равномощно $\mathbb{R}$. Мощность континуума будет обозначаться через $\mathfrak{c}$. **Континуум-гипотеза** утверждает, что $\mathfrak{c} = \aleph_1 = 2^{\aleph_0}$, но мы не будем нуждаться в этом предположении.

§ 1. Эквивалентность, мощность множества

> Cantor's continuum problem is simply the question: How many points are there on a straight line in Euclidean space? In other terms, the question is: How many different sets of integers do there exist? This question, of course, could arise only after the concept of "number" had been extended to infinite sets; hence it might be doubted if this extension can be effected in a uniquely determined manner and if, therefore, the statement of the problem in the simple terms used above is justified. Closer examination, however, shows that Cantor's definition of infinite numbers really has this character of uniqueness, and that in a very striking manner.
>
> Kurt Gödel[210]

1. Эквивалентность множеств. Сейчас мы определим понятие **изоморфизма** в категории множеств, которое описывает, когда два множества одинаково устроены *как множества*.

Определение. *Говорят, что множества A и B* **эквивалентны** *или* **равномощны** *и пишут $A \sim B$ или $|A| = |B|$, если существует биективное отображение из A в B.*

Таким образом, по определению два множества эквивалентны в том и только том случае, когда $\mathrm{Bij}(A, B)$ непусто. Легко видеть, что эквивалентность множеств действительно является **эквивалентностью**, в том смысле, который обычно приписывается этому слову. Иными словами, это означает, что эквивалентность множеств обладает следующими свойствами:

1) **Рефлексивность**: $A \sim A$;

2) **Симметричность**: $A \sim B \Longrightarrow B \sim A$;

3) **Транзитивность**: $A \sim B \ \ \& \ \ B \sim C \Longrightarrow A \sim C$.

Все эти свойства моментально усматриваются из определения. Первое из них следует из того, что $\mathrm{id}_A \in \mathrm{Bij}(A, A)$ и, поэтому, $\mathrm{Bij}(A, A)$ всегда непусто;

[210]K.Gödel, What is Cantor's continuum problem? – Amer. Math. Monthly, 1947, vol.54, p.515–525.

второе – из того, что если $\mathrm{Bij}(A,B)$ непусто и f – какой-то элемент этого множества, то обратное отображение f^{-1} принадлежит $\mathrm{Bij}(B,A)$; и, наконец, третье – из того, что если $f \in \mathrm{Bij}(A,B)$ и $g \in \mathrm{Bij}(B,C)$, то их композиция $g \circ f$ принадлежит $\mathrm{Bij}(A,C)$.

2. Мощность множества. Фигурирующие формуле $|A| = |B|$ выражения $|A|$ и $|B|$ называются **мощностями** множеств A и B соответственно. Равномощность A и B означает, что их мощности равны. Мы не хотим пока уточнять, что такое мощность, сделать это возможно, но *далеко не просто*. Главное, любое такое уточнение не только не сделает это понятие более ясным, но, наоборот, окончательно запутает начинающего.

В Главе 5 мы уже имели дело с мощностями конечных множеств. Если множество X конечно, то $|X|$ обозначает **число элементов** множества X, являющееся натуральным числом или нулем. Формула $|X| = n$ означает, что множество X содержит n элементов или, **что то же самое**, что существует биекция между X и начальным отрезком натурального ряда $\underline{n}$ длины n. Это значит, что мы вообще могли бы обойтись без упоминания 'числа элементов' множества X, и писать просто $X \sim \underline{n}$, хотя это, видимо, иногда было бы менее удобно (впрочем, удобство и неудобство есть исключительно вопрос привычки).

Интуитивно и для бесконечного множества X мощность есть 'число элементов' этого множества, только для бесконечного множества это 'число' уж никак не является натуральным числом – или вообще каким-нибудь 'числом', рассматривавшимся в математике до Кантора. Именно Кантор ввел новые 'бесконечные' числа, называемые **кардинальными числами** или, сокращенно, **кардиналами**, которые измеряют мощности (не обязательно конечных) множеств. Впрочем, подход Кантора достаточно сложен и требует предварительного рассмотрения порядков на множестве X и введения **ординальных чисел** или, сокращенно, **ординалов**. Сегодня даже большинство профессиональных математиков (не специалистов по теории множеств) не владеет тонкостями этого подхода.

Комментарий. Существуют и другие понимания мощности, отличные от Канторовского. Например, логики и философы во главе с Фреге, Расселом и Уайтхедом отождествляли мощность множества с классом всех эквивалентных ему множеств и считали, что **то общее**, что есть у всех равномощных множеств, состоит в том, что они принадлежат одному и тому же классу. Ясно, что это весьма громоздкая конструкция. Для любого непустого множества класс всех эквивалентных ему множеств сам не является множеством, т.е. является собственно классом. Скажем, для того, чтобы определить число 1, мы должны рассмотреть **все** мыслимые одноэлементные множества, например, все одноэлементные множества вещественных чисел, все множества, единственными элементами которых являются множества вещественных чисел и т.д. Вряд ли подобный подход к определению числа 1 найдет много сторонников среди преподавателей математики в детском саду.

Впрочем, для наших ближайших целей – да и вообще для большинства приложений этого понятия в обычной математике – не имеет абсолютно **никакого** значения, что такое мощности 'на самом деле'. Достаточно научиться **оперировать** с мощностями: сравнивать множества по мощности, т.е. быть в состоянии записывать равенства и неравенства вида $|A| = |B|$, $|A| > |B|$, $|A| < |B|$, складывать и умножать мощности, т.е. быть в состоянии решить, верно ли, что $|A| + |B| = |C|$ или $|A| \cdot |B| = |C|$ и тому подобное. С точки зрения этого инструментального подхода формула $|A| = |B|$ является просто другой записью отношения $\mathrm{Bij}(A,B) \neq \varnothing$, а, скажем, формула $|A| \leq |B|$ – другой записью

отношения $\mathrm{Inj}(A, B) \neq \varnothing$, которое мы обсуждаем в § 3.

§ 2. Бесконечные множества

There is an infinite set A that is not too big.
John von Neumann

Aleph-null bottles of beer on the wall,
Aleph-null bottles of beer,
You take one down, and pass it around,
Aleph-null bottles of beer on the wall.

Постараемся, прежде всего, понять, чем бесконечные множества отличаются от конечных.

1. Конечные и бесконечные множества. Напомним, что множество называется **конечным**, если оно либо пусто, либо эквивалентно какому-то из множеств $\underline{n}$, $n \in \mathbb{N}$. Множество, не являющееся конечным, называется **бесконечным**[211]. Приведенное определение конечных и бесконечных множеств не является *внутренним*, поскольку оно апеллирует к существованию биекций множества X с отрезками натурального ряда. Постараемся охарактеризовать условие бесконечности множества в терминах самого этого множества. Наиболее известная из таких характеризаций, известная как бесконечность по Дедекинду, восходит к Галилею и Больцано. Существует другие внутренние характеризации бесконечности: бесконечность по Расселу, по Цермело, etc. Мы обсудим два из этих определений: по Дедекинду-2 и по Тарскому.

2. Парадокс Галилея. Галилео Галилей[212] отмечал следующий факт, который он считал парадоксальным, потому что он противоречит постулату Эвклида "целое больше части". Между множеством натуральных чисел и множеством их квадратов можно установить взаимно однозначное соответствие: $1 \mapsto 1$, $2 \mapsto 4$, $3 \mapsto 9$, ..., таким образом натуральных чисел $1, 2, 3, \ldots$ столько же, сколько их квадратов $1, 4, 9, \ldots$, хотя, очевидно, множество квадратов является собственной частью множества натуральных чисел. Впрочем, Клини[213] указывает, что этот парадокс отмечался задолго до Галилея, чуть ли не Плутархом и Проклом и уж, в любом случае, не позже XII века[214].

Различными авторами было предложено много популярных версий этого парадокса. Вот самая известная из них:

Парадокс Тристрама Шенди. Тристраму Шенди нужен год, чтобы описать один день своей жизни. Тем не менее, если Тристрам Шенди будет жить вечно, то каждый день его жизни будет описан.

3. Множества бесконечные по Дедекинду. Мы то, конечно, понимаем, что здесь нет никакого противоречия, так как именно свойство быть эквивалентным собственной части есть характеристическое свойство бесконечных множеств, положенное в основу **определения** бесконечности Больцано, а затем Дедекиндом.

---

[211] Это принятое сегодня словоупотребление. В действительности, Кантор и Дедекинд предпочитали называть такие множества **трансфинитными** (transfinit). Термин **бесконечный** (unendlich, eigentlich unendlich, absolut unendlich) использовался ими в специальных контекстах и в более сильном смысле, чем просто отсутствие конечности.

[212] **Галилео Галилей (1564–1641)**

[213] С.К.Клини, Математическая логика. – Мир, М., 1973, т.1–480. стр.207.

[214] J.Thomas, A 12th century paradox of the infinite. – J. Symb. Logic, 1958, vol.23, p.133–134.

Определение. *Множество X называется* **бесконечным по Дедекинду**, *если в нем существует собственное подмножество Y эквивалентное X.*

Некоторые авторы называют множества, бесконечные по Дедекинду, ***D*-бесконечными**. Иными словами, множество бесконечно в смысле этого определения в том и только том случае, когда $\mathrm{Inj}(X,X) \neq \mathrm{Bij}(X,X)$. Мы подробно обсуждаем связь этого определения с обычным определением в § ?, однако уже сейчас отметим, что это определение эквивалентно обычному лишь в предположении аксиомы выбора. В общем же случае множество X бесконечно по Дедекинду лишь если $|X| \geq \aleph_0$.

4. Второе определение Дедекинда. Дедекинду принадлежит еще одна внутренняя характеризация конечности, называемая обычно **вторым определением Дедекинда**.

Определение. *Говорят, что множество* **конечно в смысле Дедекинда-2**, *если существует такое инъективное отображение $\phi : X \longrightarrow X$, которое не переводит в себя ни одно непустое собственное подмножество X.*

Довольно легко убедиться в том, что это определение эквивалентно обычному определению конечности.

Теорема. *Множество в том и только том случае конечно в смысле Дедекинда-2, когда оно конечно в обычном смысле.*

Доказательство. Ясно, что пустое множество конечно в смысле Дедекинда-2. С другой стороны, любое непустое конечное множество X эквивалентно множеству $\underline{n}$ для какого-то натурального n. Определим биекцию множества $\underline{n}$ на себя посредством $1 \mapsto 2 \mapsto 3 \mapsto \ldots \mapsto n \mapsto 1$. С точки зрения перестановок, это так называемый **длинный цикл**, в табличной записи

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 2 & 3 & 4 & \ldots & n & 1 \end{pmatrix},$$

а с точки зрения компьютерной алгебры – это команда `RotateRight`. Ясно, что если $Y \subseteq X$ – непустое подмножество, инвариантное относительно ϕ и $x \in Y$, то Y содержит все образы x под действием последовательных итераций $\phi^{\circ i}$ и, следовательно, $Y = X$.

Обратно, предположим, что множество X бесконечно и $x \in X$. Пусть ϕ – любая инъекция X в себя. Рассмотрим последовательность образов $\phi^{\circ n}(x)$ элемента x под действием итераций ϕ. Имеется две возможности. Либо среди элементов $\phi^{\circ n}(x)$, $n \in \mathbb{N}_0$, есть хотя бы два одинаковых, либо они все различны.

В первом случае, пусть, скажем $\phi^{\circ m}(x) = \phi^{\circ n}(x)$ для некоторых $m < n$. Так как ϕ – а, тем самым, и $\phi^{\circ m}$ – инъекция, то $x = \phi^{\circ(n-m)}(x)$. Рассмотрим множество $Y = \{x, \phi(x), \ldots, \phi^{\circ(n-m-1)}(x)\}$. Оно конечно и тем самым, является непустым собственным подмножеством в X. Ясно, что Y инвариантно относительно ϕ.

С другой стороны, если все элементы $\phi^{\circ n}(x)$, $n \in \mathbb{N}_0$, различны, то рассмотрим множество $Y = \{\phi(x), \phi^{\circ 2}(x), \phi^{\circ 3}(x), \ldots\}$. Ясно, что это множество инвариантно относительно ϕ. С другой стороны, оно является собственным подмножеством X так как $x \notin Y$. Тем самым для любого инъективного отображения ϕ бесконечного множества X в себя мы построили собственное непустое инвариантное подмножество $Y \subset X$.

5. Множества бесконечные по Тарскому. Еще одна замечательная внутренняя характеризация конечных множеств была предложена Альфредом Тарским[215] в 1922 году.

Определение. *Множество X называется* **конечным по Тарскому**, *если любое непустое подмножество в 2^X имеет* **минимальный элемент** *относительно включения.*

---

[215] **Альфред Тарский** (14.01.1901, Варшава – ??) – польский алгебраист, логик и философ. Основные ранние работы относятся к основаниям математики и теории множеств. В 1939 году эмигрировал в США, где основал школу теории моделей в Беркли. В нашем курсе упоминаются парадокс Банаха-Тарского и теорема Тарского о характеризации алгебраически замкнутых полей.

Иными словами, для любого $S \subseteq 2^X$, $S \neq \varnothing$, существует такое $Y \in U$, что для любого $Z \in U$ из включения $Z \subseteq Y$ вытекает $Z = Y$.

Задача. Докажите, что множества конечные в смысле Тарского можно определить двойственным образом, как такие множества, для которых каждое непустое подмножество в 2^X имеет **максимальный элемент** относительно включения. Иными словами, для любого $S \subseteq 2^X$, $S \neq \varnothing$, существует такое $Y \in U$, что для любого $Z \in U$ из включения $Y \subseteq Z$ вытекает $Z = Y$.

Решение. Определим отображение Comp множества 2^{2^X} в себя, которое каждому подмножеству $S \subseteq 2^X$ сопоставляет подмножество $\mathrm{Comp}(S)$, состоящее из дополнений к элементам множества S:

$$\mathrm{Comp}(S) = \{X \setminus Y \mid Y \in S\}.$$

Тогда $\mathrm{Comp}(S)$ непусто вместе с S и, так как переход к дополнению обращает включение, в том и только том случае содержит минимальный элемент, когда S содержит максимальный элемент.

Таким образом, множество **бесконечно по Тарскому** в том и только том случае, когда его булеан 2^X содержит такое непустое подмножество S, которое не содержит минимального (или максимального) элемента. Тарский показал, что его определение эквивалентно обычному определению.

Теорема. *Множество в том и только том случае конечно в смысле Тарского, когда оно конечно в обычном смысле.*

Доказательство. Пусть вначале множество X конечно в обычном смысле, причем $|X| = n$, а S – непустое подмножество в 2^X. Рассмотрим отображение $\mathrm{Card} : S \longrightarrow \mathbb{N}_0$, сопоставляющее каждому подмножеству $Y \in S$ его порядок $|Y|$. Образ этого отображения $T = \mathrm{Im}(\mathrm{Card}\,|_S)$ содержится в $\{0, \ldots, n\}$ и непуст. Следовательно, T имеет наибольший и наименьший элементы, скажем, l и m. Тогда любое $Y \in S$ такое, что $|Y| = l$ является минимальным элементом S, а любое $Z \in S$ такое, что $|Z| = m$ – максимальным элементом. Таким образом, множество, конечное в обычном смысле, конечно в смысле Тарского. Кстати, почему мы записали образ отображения Card на S как $\mathrm{Im}(\mathrm{Card}\,|_S)$, а не просто как $\mathrm{Card}(S)$? Вспомните 4–?–?!

С другой стороны, если X бесконечно в обычном смысле и $S \subseteq 2^X$ – множество его конечных подмножеств, то S не имеет максимального элемента. Почему? Да потому, что если $Y \in S$, то $X \setminus Y \neq \varnothing$ и поэтому найдется $y \in X \setminus Y$ так что $Y \cup \{y\}$ по-прежнему конечно и строго содержит Y. По той же причине множество S бесконечных подмножеств – или даже бесконечных подмножеств, имеющих конечное дополнение – не имеет минимального элемента. Поэтому множество, бесконечное в обычном смысле, бесконечно в смысле Тарского.

§ 3. Субвалентность, теорема Кантора-Бернштейна

1. Субвалентность. Неравенство мощностей естественно определить через существование инъективных отображений.

Определение. *Говорят, что множество A* **субвалентно** *B или что* **мощность** *A* **не больше мощности** *B и пишут $|A| \leq |B|$, если существует инъективное отображение $A \longrightarrow B$. Множество A называется* **строго субвалентным** *множеству B, если оно субвалентно но не эквивалентно B. В этом случае говорят также, что* **мощность** *A* **меньше мощности** *B и пишут $|A| < |B|$.*

Иными словами, A субвалентно B если $\mathrm{Inj}(A, B) \neq \varnothing$ или, что то же самое, если существует подмножество $A' \subseteq B$ эквивалентное A. Как обычно, отношение, симметричное субвалентности, записывается посредством $\geq$. Таким образом, по определению $|A| \geq |B|$ означает то же самое, что $|B| \leq |A|$. То же относится и к употреблению знака $>$ для мощностей. Следующие свойства субвалентности очевидны:

1) рефлексивность: $|A| \leq |A|$;

2) транзитивность: если $|A| \leq |B|$ и $|B| \leq |C|$, то $|A| \leq |C|$.

В самом деле, $\mathrm{id}_A \in \mathrm{Inj}(A, A)$ и композиция $g \circ f$ двух отображений $f \in \mathrm{Inj}(A, B)$ и $g \in \mathrm{Inj}(B, C)$ принадлежит $\mathrm{Inj}(A, C)$.

Оказывается, субвалентность, кроме того, и антисимметрична на мощностях, иными словами, если каждое из двух множеств A и B субвалентно второму, то они эквивалентны. Иными словами, если для двух множеств A и B имеют место неравенства $|A| \leq |B|$ и $|B| \leq |A|$, то $|A| = |B|$. Это свойство является уже значительно более глубоким, чем рефлексивность и транзитивность, и составляет содержание знаменитой теоремы Кантора-Бернштейна.

2. Теорема Кантора-Бернштейна. Следуюший результат часто называется еще просто теоремой Кантора, просто теоремой Бернштейна[216], теоремой Шредера[217]-Бернштейна, теоремой эквивалентности и т.д. Это один из центральных результатов всей канторовской теории множеств и одна из первых по настоящему глубоких теорем, которые мы доказываем в этом курсе.

Теорема Кантора-Бернштейна. *Если существуют инъективные отображения $f : A \longrightarrow B$ и $g : B \longrightarrow A$, то существует биективное отображение $h : A \longrightarrow B$.*

Приводимое ниже доказательство основано на принадлежащей Стефану Банаху[218] переработке доказательства Юлиуса Кенига[219]. Интересно отметить, что оно **не использует** аксиому выбора.

Доказательство. Чтобы предъявить биекцию $h : A \longrightarrow B$, мы построим разбиения $A = A_+ \coprod A_- \coprod A_\infty$ и $B = B_+ \coprod B_- \coprod B_\infty$ такие, что $A_+ \sim B_-$, $A_- \sim B_+$ и $A_\infty \sim B_\infty$.

Для этого посмотрим на итерации отображений f и g. Начнем с рассмотрения бесконечной влево цепочки отображений

$$\ldots B \longrightarrow^g A \longrightarrow^f B \longrightarrow^g A,$$

и будем последовательно компоновать входящие в нее отображения. Ясно, что каждый раз при добавлении нового фактора f или g образ получающейся композиции может лишь уменьшиться (см. ?.?), так что мы получаем следующую невозрастающую последовательность подмножеств в A:

$$A \supseteq \mathrm{Im}(g) \supseteq \mathrm{Im}(gf) \supseteq \mathrm{Im}(gfg) \supseteq \mathrm{Im}(gfgf) \supseteq \ldots$$

Условимся считать само множество A нулевым членом последовательности, $\mathrm{Im}(g) = A_1$ – первым, $\mathrm{Im}(gf) = A_2$ – вторым, и так далее, и перепишем эту последовательность в виде $A_0 \supseteq A_1 \supseteq A_2 \supseteq A_3 \supseteq \ldots$. Таким образом, $A_{2i} = \mathrm{Im}((gf)^i)$ и $A_{2i+1} = \mathrm{Im}((gf)^i g)$. Обозначим

---

[216] **Ф.Бернштейн** (1878–1956)

[217] **Э.Шредер** (1841–1902)

[218] **Стефан Банах** (30.03.1892, Краков – 31.08.1945, Львов) – крупнейший польский математик, создатель функционального анализа и замечательной львовской математической школы. Банах учился в Ягеллонском университете в Кракове и во Львовском политехническом институте, но ни одного из них не окончил. В 1922 году защитил диссертацию и был назначен экстраординарным, а потом и ординарным професором во Львове. Основные работы относятся к теории топологических векторных пространств, теории меры и теории вещественных функций, хотя он интересовался и другими вопросами. В честь него названы банаховы пространства, банаховы алгебры, и т.д. Центральную роль в функциональном анализе играют теоремы Хана-Банаха, Банаха-Штейнгауза и др. В нашем курсе упоминается парадокс Банаха-Тарского. На русский переведена его книга 'Теория линейных операций'. Штейнгауз, Улам и другие оставили живописные воспоминания о Банахе. Одно из самых колоритные связано с Шотландским кафе во Львове, где собирались математики. Улам пишет: 'It was hard to outlast or outdrink Banach during these sessions'.

[219] **Юлиус Кениг** (1849–1913)

теперь через A_∞ пересечение всех членов этой последовательности. Так как нечетные члены последовательности зажаты между ее четными членами, то при образовании пересечения их можно отбросить, ограничившись лишь четными членами. Таким образом,

$$A_\infty = \bigcap A_{2i} = \bigcap \mathrm{Im}((gf)^i).$$

Здесь и дальше все пересечения и объединения берутся по всем $i \in \mathbb{N}_0$. То же, разумеется, относится и к нечетным членам:

$$A_\infty = \bigcap A_{2i+1} = \bigcap \mathrm{Im}((gf)^i g).$$

Для любого $a \in A$, не принадлежащего A_∞, рассмотрим наибольший номер $i = i(a)$ такой, что $a \in A_i$. Этот номер либо четен, либо нечетен. Положим

$$A_+ = \{a \in A \setminus A_\infty \mid 2|i(a)\}, \qquad A_- = \{a \in A \setminus A_\infty \mid 2 \not| i(a)\}.$$

Ясно, что эти определения можно переписать в виде

$$A_+ = \coprod (A_{2i} \setminus A_{2i+1}) = \coprod (\mathrm{Im}((gf)^i) \setminus \mathrm{Im}((gf)^i g)),$$

$$A_- = \coprod (A_{2i+1} \setminus A_{2i+2}) = \coprod (\mathrm{Im}((gf)^i g) \setminus \mathrm{Im}((gf)^{i+1})),$$

и что $A = A_+ \coprod A_- \coprod A_\infty$ представляет собой разбиение A.

Разбиение множества $B = B_+ \coprod B_- \coprod B_\infty$ строится совершенно аналогично с использованием бесконечной влево цепочки отображений

$$\ldots A \longrightarrow^f B \longrightarrow^g A \longrightarrow^f B.$$

При этом $B_{2i} = \mathrm{Im}((fg)^i)$, $B_{2i+1} = \mathrm{Im}((fg)^i f)$ и

$$B_\infty = \bigcap B_{2i} = \bigcap B_{2i+1} = \bigcap \mathrm{Im}((fg)^i) = \bigcap \mathrm{Im}((fg)^i f)$$

$$B_+ = \coprod (B_{2i} \setminus B_{2i+1}) = \coprod (\mathrm{Im}((fg)^i) \setminus \mathrm{Im}((fg)^i f)),$$

$$B_- = \coprod (B_{2i+1} \setminus B_{2i+2}) = \coprod (\mathrm{Im}((fg)^i f) \setminus \mathrm{Im}((fg)^{i+1})).$$

Легко видеть, что для любого $i \in \mathbb{N}_0$ выполняются равенства

$$f(A_{2i}) = f(\mathrm{Im}((gf)^i)) = \mathrm{Im}(f(gf)^i) = \mathrm{Im}((fg)^i f) = B_{2i+1}$$

$$f(A_{2i+1} = f(\mathrm{Im}((gf)^i g)) = \mathrm{Im}(f(gf)^i g) = \mathrm{Im}((fg)^{i+1}) = B_{2i+2}.$$

Таким образом, для любого i имеем $f(A_i) = B_{i+1}$. Совершенно аналогично можно убедиться и в том, что $g(B_i) = A_{i+1}$.

Теперь совершенно ясно, как завершить доказательство. Так как $f(A_i) = B_{i+1}$ и $g(B_i) = A_{i+1}$, то ограничения f и g на A_∞ и B_∞ являются взаимно обратными биекциями, ограничение f на A_+ является биекцией A_+ на B_- а ограничение g на B_+ является биекцией B_+ на A_-. Таким образом, биекция $h : A \longrightarrow B$ может быть определена следующей формулой:

$$h(a) = \begin{cases} f(a), & a \in A_+, \\ g^{-1}(a), & a \in A_-, \\ f(a) = g^{-1}(a), & a \in A_\infty. \end{cases}$$

4. Теорема Кантора-Бернштейна и сравнение мощностей. Если бы мощности образовывали множество, мы сказали бы, что субвалентность задает частичный порядок на мощностях. Однако из теоремы Кантора-Бернштейна *не следует*, что этот порядок линеен, т.е. что две любые мощности сравнимы.

Тот факт, что для любых двух множеств A и B имеет место ровно одна из двух возможностей $|A| < |B|$, $|A| = |B|$ или $|A| > |B|$ называется **законом трихотомии**. Из теоремы Кантора-Бернштейна следует лишь, что первая и третья из этих возможностей не могут реализовываться *одновременно*, но она не исключает существования двух множеств A и B таких, что как $\mathrm{Inj}(A, B)$, так и $\mathrm{Inj}(B, A)$ пусто. В действительности, в теории **ZF невозможно** доказать, что из любых двух множеств по крайней мере одно субвалентно другому. Существуют модели **ZF**, так называемые **модели Йеха**, для которых порядок на бесконечных кардиналах любой наперед заданный. В следующем параграфе мы убедимся, что в теории **ZFC** ситуация существенно проще.

§ 4. Супервалентность

В этом параграфе мы вынуждены предполагать, что читатель сладеет понятием фактормножества по отношению эквивалентности. Читатель, не знакомый с этим понятием, может вернуться к чтению этого параграфа после знакомства с Главой ?.

1. Супервалентность. Неравенство мощностей можно определить и по другому, через сюръективные отображения.

Определение. *Говорят, что множество A* **супервалентно** *B и пишут $|A| \geq^* |B|$, если либо B пусто, либо существует сюръективное отображение $A \longrightarrow B$. Говорят, что A* **строго супервалентно** *B и пишут $|A| >^* |B|$, если A супервалентно, но не эквивалентно B.*

Иными словами, A супервалентно $B \neq \varnothing$ если $\mathrm{Sur}(A, B) \neq \varnothing$ или, что то же самое, если существует такое отношение эквивалентности $\sim$ на A, что $A/\sim$ эквивалентно B. Отношение, симметричное супервалентности обозначается через $\leq^*$, а отношение, симметричное строгой супервалентности – через $<^*$. Например, $|A| <^* |B|$ по определению означает то же самое, что $|B| >^* |A|$. Следующие свойства супервалентности очевидны:

1) рефлексивность: $|A| \geq^* |A|$;

2) транзитивность: если $|A| \geq^* |B|$ и $|B| \geq^* |C|$, то $|A| \geq^* |C|$.

В этом месте моментально возникает законный вопрос: справедлив ли для супервалентности аналог теоремы Кантора-Бернштейна? Т.е. верно ли, что супервалентность антисимметрична на мощностях: если $|A| \geq^* |B|$ и $|B| \geq^* |A|$, то $|A| = |B|$? Иными словами, следует ли из существования сюръективного отображения A на B и существования сюръективного отображения B на A существование биекции между A и B? Кроме того, верно ли, что супервалентность задает на мощностях тот же порядок, что и субвалентность, т.е. $|A| \geq^* |B|$ в том и только том случае, когда $|B| \leq |A|$? Иными словами, вытекает ли из существования сюръективного отображения A на B существование инъективного отображения B в A? В теории множеств **ZF** без аксиомы выбора ответ на все эти вопросы **отрицателен**.

2. Связь супервалентности с субвалентностью. В теории с аксиомой выбора ситуация значительно проще.

Теорема. *В теории* **ZFC** *имеет место эквивалентность*

$$|A| \leq |B| \quad \Longleftrightarrow \quad |B| \geq^* |A|.$$

Доказательство. Как мы увидим в следующей задаче, доказательство импликации $\Longrightarrow$ элементарно и **не зависит от аксиомы выбора**. Ну а вот обратная импликация $\mathrm{Sur}(A, B) \neq \varnothing \Longrightarrow \mathrm{Inj}(B, A) \neq \varnothing$, как раз и является первоначальной формулировкой аксиомы выбора (**аксиома Леви**).

Эта теорема утверждает, что в системе **ZFC** множество A в том и только том случае субвалентно B, когда B супервалентно A. Это позволяет нам в дальнейшем писать без всяких церемоний $|B| \geq |A|$ вместо $|B| \geq^* |A|$, не опасаясь двусмысленности. Тем не менее, кое-что про связь супервалентности с субвалентностью можно доказать и без аксиомы выбора.

Задача. Докажите, *не используя аксиому выбора*, что если $|A| \leq |B|$, то $|B| \geq^* |A|$ и, в другую сторону, если $|B| \geq^* |A|$, то $|2^A| \leq |2^B|$.

Решение. Первое утверждение очевидно, в самом деле, если оно A пусто, то B супервалентно ему по определению, а если A непусто и $f \in \mathrm{Inj}(A, B)$, то выберем элемент $a \in A$ и определим отображение $g : B \longrightarrow A$, полагая $g(x) = f^{-1}(x)$, если $x \in \mathrm{Im}(f)$ и $g(x) = a$ в противном случае. Ясно, что g сюръективно. Для доказательства второго утверждения нужно воспользоваться тем, что функтор степени является антиэквивалентностью категорий и, следовательно, меняет местами мономорфизмы и эпиморфизмы. В самом деле, в Задаче ?.? показано, что если $f : B \longrightarrow A$ – сюръекция, то $f^{-1} : 2^A \longrightarrow 2^B$ – инъекция.

§ 5. Закон трихотомии

1. Трихотомия. Утверждение, что для любых двух вещей x и y имеет место **ровно** одна из **двух** возможностей называется обычно **дихотомией**, а ровно одна из **трех** возможностей – **трихотомией**. Примером такой ситуации является сформулированный Кантором и доказанный Цермело **закон трихотомии**.

Закон трихотомии. *В теории* **ZFC** *для любых двух множеств X и Y имеет место ровно одна из трех возможностей $|X| < |Y|$, $|X| = |Y|$ или $|X| > |Y|$.*

Таким образом, в предположении аксиомы выбора любые две мощности сравнимы, т.е. порядок на мощностях, заданный субвалентностью, является **линейным**.

2. Лемма Куратовского-Цорна. Все обычные доказательства закона трихотомии опираются на переформулировки аксиомы выбора в терминах упорядоченных множеств, которые мы обсуждаем в Главе ?. Первоначальное доказательство Цермело опиралось на теорему Цермело о полном упорядочении. Мы приведем современное доказательство, основанное на лемме Куратовского-Цорна[220]. Во-первых, это доказательство представляется мне наиболее естественным, а, во-вторых, оно хорошо иллюстрирует то, как аксиома выбора обычно используется в алгебре. Все понятия, фигурирующие в следующем утверждении, определяются в Главе ?, а его эквивалентность аксиоме выбора доказывается в Главе ?.

Лемма Куратовского-Цорна. *Пусть Z непустое частично упорядоченное множество в котором каждая цепь имеет верхнюю грань. Тогда в Z существует хотя бы один максимальный элемент.*

3. Доказательство закона трихотомии. Достаточно показать, что для любых двух множеств X, Y имеет место хотя бы одно из неравенств $|X| \leq |Y|$ $|Y| \leq |X|$. Рассмотрим множество Z троек (A, B, f), где $A \subseteq X$, $B \subseteq Y$, $f \in \mathrm{Bij}(A, B)$. Прежде всего заметим, что множество Z непусто, в самом деле, $(\varnothing, \varnothing, \varnothing) \in Z$. Введем на этом множестве следующий порядок, скажем, что $(A, B, f) \leq (C, D, g)$, если $A \subseteq C$, $B \subseteq D$ и $f = g|_A$. Ясно, что описанное отношение действительно задает порядок на множестве Z.

Этот порядок обладает тем свойством, что любая возрастающая цепочка имеет точную верхнюю грань. В самом деле, пусть (A_i, B_i, f_i), $i \in \mathbb{N}$, такая цепочка. Положим $A = \cup A_i$, $B = \cup B_i$ и определим отображение $f : A \longrightarrow B$, полагая $f(x) = f_i(x)$, где i – наименьший индекс такой, что $x \in A_i$. Ясно, что

[220]**Макс Цорн**

тогда для любого j, такого, что $x \in A_j$, выполняется равенство $f(x) = f_j(x)$. Легко видеть, что f сюръективно, действительно, если $y \in B_i$, то $y = f_i(x) = f(x)$ для некоторого $x \in A_i$. Легко проверить, что f инъективно. В самом деле, если $f(x) = f(y)$ для некоторых $x, y \in A$, то рассмотрим наименьшие индексы i и j такие, что $x \in A_i$ и $y \in A_j$, соответственно. Пусть $h = \max(i, j)$, тогда $x, y \in A_h$ и, значит, $f_h(x) = f_h(y)$, так что, окончательно, $x = y$.

Таким образом, по лемме Куратовского-Цорна Z имеет максимальный элемент. Пусть (A, B, f) – какой-то максимальный элемент множества Z. Покажем, что тогда $A = X$ или $B = Y$. В самом деле, предположим, вопреки ожиданиям, что $A \subset X$ и $B \subset Y$. Тогда найдутся $x \in X \setminus A$ и $y \in Y \setminus B$. Определим тройку (C, D, g), полагая $C = A \cup \{x\}$, $D = D \cup \{y\}$, и $g(z) = f(z)$ для $z \in X$, а $f(x) = y$. Ясно, что $(C, D, g) \in Z$, причем $(C, D, g) > (A, B, f)$. Это значит, что тройка (A, B, f) не является максимальной. Полученное противоречие показывает, что $A = X$ или $B = Y$. В первом случае $|X| \leq |Y|$, а во втором $|Y| \leq |X|$

4. Эквивалентность закона трихотомии аксиоме выбора. Как мы видели, доказательство закона трихотомии совершенно элементарно, гораздо более глубоким является утверждение, что верно и обратное, т.е. трихотомия влечет аксиому выбора и, значит, **эквивалентна** аксиоме выбора.

Теорема Гартогса. *Аксиома выбора эквивалентна тому, что для любых двух множеств X и Y имеет место ровно одна из трех возможностей $|X| < |Y|$, $|X| = |Y|$ или $|X| > |Y|$.*

Обычное доказательство этой теоремы использует теорему Цермело о полном упорядочении, мы отложим доказательство этой эквивалентности до Главы ?. Аналогичное утверждение для супервалентности также справедливо.

Теорема Линденбаума. *Аксиома выбора эквивалентна тому, что для любых двух множеств X и Y имеет место ровно одна из трех возможностей $|X| <^* |Y|$, $|X| = |Y|$ или $|X| >^* |Y|$.*

§ 6. Теорема Кантора

Установим еще один ключевой результат Канторовской теории множеств.

Теорема Кантора. *Мощность множества 2^X строго больше, чем мощность множества X.*

Доказательство. Ясно, что отображение $X \longrightarrow 2^X$, которое сопоставляет каждому элементу $x \in X$ одноэлементное множество $\{x\} \in 2^X$ инъективно, поэтому мощность X не превосходит мощности 2^X.

Покажем, что не существует сюръективного отображения $X \longrightarrow 2^X$. В самом деле, пусть $f : X \longrightarrow 2^X$ – любое отображение. Рассмотрим множество $Y = \{x \in X \mid x \notin f(x)\}$. Покажем, что тогда $Y \notin f(X)$. В самом деле, предположим, что существует $y \in Y$ такое, что $f(y) = Y$. Тогда имеет место альтернатива: либо $y \in Y$, либо $y \notin Y$. По определению Y, если $y \in Y = f(y)$, то $y \notin Y$. Обратно, если $y \notin Y = f(y)$, то, снова по определению Y имеем $y \in Y$. Полученное противоречие показывает, что не существует такого $y \in X$, что $f(y) = Y$.

Для того, кто понял идею этого доказательства не составит труда решить следующую задачу.

Задача. Докажите, что для любого множества X и для любого множества Y, такого, что $|Y| \geq 2$, мощность множества $\mathrm{Map}(X, Y)$ строго больше мощности множества X.

Геометрическое доказательство теоремы Кантора. В [КуМо] приводится следующее геометрическое истолкование вышеприведенного доказательства. Рассмотрим множество $X \times X$. Рассмотрим множество $R = \{(x, y) \mid y \in f(x)\}$. Тогда $f(x)$ – это в точности проекция на ось ординат тех точек из R, абсцисса которых равна x. Пусть теперь Y – проекция на ось ординат тех точек диагонали $\Delta = \{(x, x) \mid x \in X\}$, которые не принадлежат R. Из этого геометрического представления очевидно, что $y \neq f(x)$ ни для одного $x \in X$. В самом деле, если $(x, x) \in R$, то $x \in f(x)$, но $x \notin Y$. Если же $(x, x) \notin R$, то $x \notin f(x)$, но $x \in Y$.

Парадокс Кантора. *Если X – множество всех множеств, то, очевидно, $2^X = X$, так что, в частности, $|2^X| = |X|$. С другой стороны по теореме Кантора $|2^X| > |X|$.*

Это противоречие влечет такое следствие.

Следствие. *Не существует множества всех множеств.*

§ 7. Счетная мощность

> To illustrate the use of the axiom of choice let me consider some banality like the following: everyone knows that the union of countably many countable sets is countable. This is used in real analysis all over and most people do not even realize that the proof uses the axiom of choice.
>
> Thomas J.Jech

1. Счетные множества. В действительности в обычной математике достаточно использовать лишь две–три бесконечных мощности.

Определение. *Множество называется* **счетным**, *если оно эквивалентно множеству $\mathbb{N}$ натуральных чисел.*

Сейчас мы покажем, что объединение конечного числа счетных множеств счетно.

Теорема. *Объединение двух счетных множеств счетно.*

Доказательство. Ясно, что $A \cup B$ не менее, чем счетно. Пусть $f : \mathbb{N} \longrightarrow A$ $g : \mathbb{N} \longrightarrow B$ – биекции $\mathbb{N}$ на A и B, соответственно. Определим отображение $f \cup g : \mathbb{N} \longrightarrow A \cup B$, полагая $f \cup g(n) = f((n+1)/2)$, если n нечетно и $f \cup g(n) = g(n/2)$, если n четно. Тогда отображение $f \cup g$ сюръективно и, следовательно, по аксиоме выбора, мощность $A \cup B$ не превосходит $\aleph$.

Замечание. В этом доказательстве мы воспользовались аксиомой выбора, но на самом деле этот результат не зависит от аксиомы выбора. Достаточно заметить, что при помощи обратных отображений f^{-1} и g^{-1} можно явно построить инъекцию $A \cup B \longrightarrow \mathbb{N}$.

Задача. Докажите, что множество целых чисел $\mathbb{Z}$ счетно.

Решение. Представим $\mathbb{Z}$ как объединение двух множеств $\mathbb{N}_0$ и $-\mathbb{N} = \{-n \mid n \in \mathbb{N}\}$, каждое из которых, очевидно, эквивалентно $\mathbb{N}$.

Задача. Докажите, что объединение конечного числа счетных множеств счетно.

Указание. Действуйте по индукции, либо явно постройте сюръективное отображение $\mathbb{N} \longrightarrow A_1 \cup \ldots \cup A_n$, обобщающее отображение $f \cup g$, построенное в теореме.

2. Произведение конечного числа счетных множеств. Следующий факт будет часто использоваться в дальнейшем. Замечательно, что он не зависит от аксиомы выбора.

Теорема. *Декартово произведение двух счетных множеств счетно.*

Доказательство. Пусть $f : \mathbb{N} \longrightarrow A$ и $g : \mathbb{N} \longrightarrow B$ – биекции $\mathbb{N}$ на A и B, соответственно. Каждое натуральное число $n \in \mathbb{N}$ однозначно представляется в виде $n = 2^{l-1}(2m-1)$, где $l, m \in \mathbb{N}$, причем отображение $n \mapsto (l, m)$ представляет собой биекцию $\mathbb{N} \mapsto \mathbb{N} \times \mathbb{N}$. Определим отображение $f * g : \mathbb{N} \longrightarrow A \times B$, полагая $f * g(n) = (f(l), g(m))$. Тогда отображение $f * g$ биективно и, следовательно, мощность $A \cup B$ равна $\aleph_0$.

На самом деле, очевидно, достаточно построить **инъективное** отображение $\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, а сделать это совсем просто, можно положить, например, $(m, n) \mapsto 2^m 3^n$. Существует и много различных способов определить биективное отображение $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$. Например, можно положить

$$f(m, n) = \binom{m+n-1}{2} + m$$

(см. [КуМо], с.103).

Задача. Изобразите это отображение на картинке.

Ответ. Проще изобразить *обратное* к нему отображение: расположим пары (m, n) натуральных чисел в первом квадранте и будем нумеровать их по диагоналям начиная с первой, в направлении с Юго-Востока на Северо-Запад. Это так называемый **диагональный процесс Коши** (Cauchysche Diagonalverfahren).

Задача. Декартово произведение конечного числа счетных множеств счетно.

Решение. Используйте индукцию или определите инъекцию $\mathbb{N} \times \ldots \times \mathbb{N} \longrightarrow \mathbb{N}$, полагая $(n_1, \ldots, n_t) \mapsto p_1^{n_1} \cdot \ldots \cdot p_t^{n_t}$, где $p_1, \ldots, p_t$ суть первые t простых чисел.

4. Счетность счетного объединения счетных множеств. А вот доказать следующую теорему без использования аксиомы выбора *не удастся*. Дело в том, что без аксиомы выбора соответствующий факт безнадежно неверен. Феферман и Леви построили такую модель системы **ZF**, в которой множество вещественных чисел является счетным объединением счетных множеств!

Теорема. *В теории* **ZFC** *объединение счетного числа счетных множеств счетно.*

Доказательство. Пусть A_i, $i \in \mathbb{N}$, – счетное семейство счетных множеств. Как и раньше множество $\bigcup A_i$ по крайней мере счетно и нам нужно лишь доказать, что оно не более, чем счетно. Рассмотрим множество $X_i = \mathrm{Bij}(\mathbb{N}, A_i)$ биекций из $\mathbb{N}$ в A_i. Тогда согласно аксиоме выбора существует отображение $f : \mathbb{N} \longrightarrow \bigcup X_i$ такое, что $f(i) = f_i \in X_i$. Построим теперь отображение F :

$\mathbb{N} \times \mathbb{N} \longrightarrow \bigcup X_i$, полагая $F(i,j) = f_i(j) \in A_i$. Так как каждое f_i сюръективно, то F тоже сюръективно и, значит, снова по аксиоме выбора, мощность $\bigcup A_i$ не больше $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$.

Комментарий. В одной статье 1921 года Анри Лебег утверждал, что счетность счетного объединения счетных множеств не зависит от аксиомы выбора: "Supposons, par exemple, qu'il s'agisse de prouver que la somme d'une infinité dénombrable d'ensembles dénombrables est une ensemble dénombrable. ... Il me semble que ceux qui voient dans ces démonstrations l'emploi de l'axiome de Zermelo, donnent aux énoncés une sens "idéaliste", alors que je ne conçois que le sens "empiriste"." Как показывает только что упомянутая **модель Фефермана-Леви**, 'доказательство', которое Лебег приводит в подтверждение независимости этого результата от аксиомы выбора, содержит ошибку. Впрочем, как замечает Серпиньский, спустя 17 лет Лебег, похоже, сам признал эту ошибку [Se], p.122.

6. Конечные последовательности элементов счетного множества. Покажем теперь, что множество конечных подмножеств счетного множества счетно.

Задача. Докажите, что множество всех конечных последовательностей элементов счетного множества счетно.

Решение. Достаточно доказать, что множество конечных последовательностей натуральных чисел счетно. Очевидно, что оно по крайней мере счетно. Построим инъективное отображение из множества последовательностей в $\mathbb{N}$. Пусть $\mathrm{Prim} = \{p_i \mid i \in \mathbb{N}\}$ – множество простых чисел, где p_i обозначает i-е простое число, расположенное в порядке возрастания. Устроим отображение, сопоставляя последовательности натуральных чисел $m_1, \ldots, m_n$ число $p_1^{m_1} \cdot \ldots \cdot p_n^{m_n}$. **Основная теорема арифметики** (см. Гл. 4, § ?) утверждает, что это отображение инъективно, т.е. что разным последовательностям отвечают разные числа. Таким образом, мощность множества конечных последовательностей натуральных чисел не больше, чем мощность множества натуральных чисел, и для завершения доказательства остается лишь сослаться на теорему Кантора-Бернштейна.

Конечно, построенное в предыдущей задаче отображение является лишь одной из возможностей свести изучение последовательностей натуральных чисел к натуральным числам, сейчас мы построим еще одно подобное отображение.

Задача. Докажите, что отображение

$$(n_1, n_2, \ldots, n_m) \mapsto 2^{n_1-1} + 2^{n_1+n_2-1} + \ldots + 2^{n_1+n_2+\ldots+n_m-1}$$

устанавливает биекцию между множеством всех конечных последовательностей натуральных чисел и множеством натуральных чисел.

Задача. Докажите, что множество $\bigwedge(X)$ всех конечных подмножеств счетного множества X счетно.

Решение. Можно предполагать, что $X = \mathbb{N}$. Сопоставив каждому натуральному числу n одноэлементное подмножество $\{n\}$, мы видим, что мощность $\bigwedge(\mathbb{N})$ не меньше мощности $\mathbb{N}$. Обратно, сопоставим каждому конечному подмножеству $Y = \{i_1, \ldots, i_n\}$ последовательность его элементов $i_1, \ldots, i_n$, расположенных в порядке возрастания, $i_1 < \ldots < i_n$. Ясно, что эта последовательность полностью определяет множество Y, так что мощность множества $\bigwedge(\mathbb{N})$

не больше мощности множества конечных последовательностей натуральных чисел.

§ 8. Не каждое бесконечное множество содержит счетное подмножество

Даже чашка риса или чая должна браться в руки должным образом, без малейшей неряшливости и с сохранением должной бдительности.

Юдзан Дайдодзи "Будосёсинсю"

Даже жареного цыпленка следует привязывать.

Ямамото Цунетомо "Хагакурэ"

Доказательство было простым, коротким, но неверным.

Анри Лебег[221]

В этом параграфе мы разберем одну типичную ошибку, которую почти неизбежно совершают все математики-неспециалисты. Лично мне не известно **ни одного** учебника математического анализа, в котором не делалась бы эта ошибка.

1. Всякое бесконечное множество содержит счетное подмножество: доказательство, ... Следующая теорема и ее доказательство воспроизводятся без изменения со стр.14 книги А.Л.Брудно[222].

\quote **Теорема 1.** *Всякое бесконечное множество имеет счетное подмножество.*

Доказательство. Пусть a_1 – какой-нибудь элемент бесконечного множества A, a_2 – какой-нибудь элемент бесконечного множества $A \setminus \{a_1\}$, a_3 – элемент все еще бесконечного множества $A \setminus \{a_1, a_2\}$ и т.д. Попарно различные элементы $a_1, a_2, a_3, \ldots$ составляют счетное подмножество множества A. \unquote

Убедительно? Казалось бы, где в таком коротком и кристально ясном доказательстве можно совершить ошибку? Тем не менее, это рассуждение, безусловно, неполно в одном существенном пункте и получающийся результат, вообще говоря, **неверен**.

2. ... **опровержение,** ... Можно, пожалуй, согласиться с тем, что **если** эта совокупность элементов составляет множество, **то** это множество счетно. Однако тот факт, что эта совокупность элементов действительно можно соединить в множество, как раз и называется аксиомой выбора **AC**. Хорошо, здесь достаточно какой-то ослабленной формы аксиомы выбора, скажем, аксиомы зависимого выбора **DC** или даже аксиомы счетного выбора **CAC**. Но какая-то форма аксиомы выбора безусловно нужна.

Можно было бы считать, что в этом месте автор **использует** аксиому выбора, как нечто само собой разумеющееся, не упоминая об этом. К сожалению, дальнейший текст [??] убеждает, в том, что Александр Львович (как и вообще все аналитики, с которыми мне доводилось обсуждать этот вопрос) верит, что этот факт **не зависит** от аксиомы выбора. Вот что говорится по поводу теоремы трихотомии на стр. 22 цитированной книги: "Остается еще, правда, один неприятный случай для сравнения мощностей: если A не эквивалентно никакому подмножеству B, а B никакому подмножеству A. Тогда мы не можем принять никакого из соотношений $|A| = |B|$, $|A| < |B|$, $|A| > |B|$ и вынуждены называть A и B несравнимыми (по мощности). Если A или B конечно или **счетно**, то этого не может случиться."

Я вынужден с полной ответственностью заявить, что 'этого' **может** случиться, еще как может. В самом деле, существует модель теории **ZF**, построенная П.Коэном, в которой счетная мощность не является наименьшей среди бесконечных мощностей.

---

[221] А.Лебег, Предисловие к книге Н.Н.Лузина "Лекции об аналитических множествах и их приложениях" – Успехи Мат. Наук, 1985, т. 40, N.3, с.9–14, стр.9.

[222] А.Л.Брудно, Теория функций действительного переменного. – Наука, М., 1971, с.1–119.

Теорема Коэна. *С теорией* **ZF** *совместимо утверждение о существовании бесконечного множества вещественных чисел, не содержащего счетного подмножества.*

Бесконечные множества, не содержащие счетного подмножества, часто называются **Дедекиндовыми**; как мы вскоре увидим, это в точности множества бесконечные в обычном смысле, но конечные по Дедекинду. На русском языке доказательство этого (непростого) утверждения, состоящее в явном построении **модели Коэна**, можно найти, например, в книге Томаса Йеха [J], леммы 95 и 96. В действительности, в **модели Йеха** порядок на бесконечных мощностях может быть вообще совершенно произвольным. Тем самым, в теории множеств без аксиомы выбора рушится **весь** элементарный анализ, которому учат на 1-м курсе. Из существования Дедекиндова множества сразу вытекает, что топологическое определение предела и непрерывности (через окрестности) **не эквивалентно** аналитическому (через последовательности).

3. ... **частичная реабилитация** ... Тем не менее, приведенное выше рассуждение не является полностью лишенным смысла. Вот, что оно доказывает **на самом деле**.

Теорема. *Если X бесконечное множество, то для любого $n \in \mathbb{Z}$ множество X содержит подмножество, эквивалентное $\underline{n}$.*

Доказательство. Начинаем рассуждение так же, как в приведенном выше 'доказательстве' и действуем по индукции. Предположим, что мы уже доказали, что X содержит n-элементное подмножество $\{x_1, \dots, x_n\}$. Так как $X \setminus \{x_1, \dots, x_n\}$ все еще бесконечно, то существует $x_{n+1} \in X \setminus \{x_1, \dots, x_n\}$. Тем самым X содержит $(n+1)$-элементное подмножество $\{x_1, \dots, x_{n+1}\}$

Иными словами, для любого бесконечного множества X все множества $\bigwedge^n(X)$, $n \in \mathbb{N}$, непусты. Отсюда **в предположении аксиомы выбора** действительно легко получить *правильное* доказательство Теоремы.

Доказательство Теоремы 1. Пусть X – бесконечное множество. Согласно предыдущей теореме все множества $\bigwedge^n(X)$ непусты. В силу аксиомы выбора существует отображение $\mathbb{N} \longrightarrow \bigwedge(X)$, сопоставляющее каждому $n \in \mathbb{N}$ какой-то элемент $Y_n \in \bigwedge^n(X)$. Рассмотрим множество $Y = \cup Y_n$, $n \in \mathbb{N}$. Будучи счетным объединением конечных множеств, множество Y не более, чем счетно. С другой стороны, так как $Y \supseteq Y_n$, то $|Y| \geq n$ для всех $n \in \mathbb{N}$, так что Y в точности счетно.

4. ... **и вся правда.** А вот, что **на самом деле** можно доказать не используя аксиому выбора.

Теорема. *Следующие утверждения эквивалентны:*

1) *X бесконечно в смысле Дедекинда;*

2) *X содержит счетное подмножество.*

Доказательство. Импликация 2) $\Longrightarrow$ 1) очевидна. В самом деле, пусть $Y \subseteq X$ – счетное подмножество в X. Тогда $X = (X \setminus Y) \coprod Y$. Так как Y уже эквивалентно своему собственному подмножеству Z (парадокс Галилея), то X эквивалентно собственному подмножеству $(X \setminus Y) \coprod Z$.

Импликация 1) $\Longrightarrow$ 2) доказывается чуть сложнее. В самом деле, пусть X эквивалентно своему собственному подмножеству $Y \subset X$. Так как $X \setminus Y \neq \varnothing$, то найжется $x \in X \setminus Y$. А так как X эквивалентно Y, то существует биекция $\phi : X \longrightarrow Y$. Рассмотрим образы точки x под действием последовательных итераций отображения ϕ,

$$x,\ \phi(x),\ \phi^{\circ 2}(x),\ \phi^{\circ 3}(x), \dots$$

и заметим, что все члены этой последовательности попарно различны. В самом деле, если $\phi^{\circ m}(x) = \phi^{\circ n}(x)$ для некоторых $m < n$, то, так как ϕ, а значит и $\phi^{\circ m}(x)$, – биекция, то $x = \phi^{\circ(n-m)}(x)$, что невозможно, так как $x \notin Y$, а $\phi^{\circ(n-m)}(x) \in Y$. Но это значит, что X содержит счетное подмножество $Z = \{x, \phi(x), \phi^{\circ 2}(x), \dots\}$, что и требовалось доказать.

Задача. Объясните, чем это (правильное!) доказательство отличается от приведенного выше (неправильного!) 'доказательства' того, что **всякое** бесконечное множество содержит счетное подмножество.

Решение. Фокус здесь в том, что в нашем случае Z является образом отображения $\omega \longrightarrow X$, $n \mapsto \phi^{\circ n}(x)$, а образ отображения является множеством независимо от аксиомы выбора.

Как уже было отмечено, без аксиомы выбора **невозможно** доказать, что всякое бесконечное множество бесконечно в смысле Дедекинда. Иными словами, в теории **ZF** существуют множества, бесконечные с точки зрения математического обывателя (в том смысле, что они содержат n-элементное подмножество для любого натурального n) но не эквивалентные никакому своему собственному подмножеству и, тем самым, не содержащие ни одного счетного подмножества.

Задача. Докажите, что каждое бесконечное по Дедекинду множество является дизъюнктным объединением двух бесконечных множеств.

Решение. Ну для счетного-то множества это верно.

Предостережение. Без аксиомы выбора **невозможно** доказать, что каждое бесконечное множество обладает этим свойством.

Задача. ([J], § 5) Покажите, что объединение конечного по Дедекинду множества *попарно дизъюнктных* множеств, конечных по Дедекинду, само является конечным по Дедекинду.

Предостережение. Как вытекает из результатов [J], § 27, если не предполагать, что эти множества попарно дизъюнктны, то без аксиомы выбора невозможно доказать даже следующее значительно более слабое утверждение: объединение конечного по Дедекинду множества *конечных* множеств конечно по Дедекинду.

5. Верно ли, что 2^{2^X} бесконечнее, чем X? Как вытекает из теоремы Кантора и Теоремы ?, в предположении аксиомы выбора для любого бесконечного множества X мощность множества 2^X не меньше мощности континуума. Без аксиомы выбора не видно даже никакого простого способа доказать, что множество 2^X по крайней мере счетно! Тем не менее, как заметил Тарский, для множества 2^{2^X} это легко доказать и не используя аксиому выбора.

Задача. Докажите, что для любого бесконечного множества X множество 2^{2^X} бесконечно по Дедекинду.

Решение. Так как множество X бесконечно, то по Теореме ? все множества $\bigwedge^n(X)$ непусты. С другой стороны ясно, что для любых $m \neq n$ множества $\bigwedge^m(X)$ и $\bigwedge^n(X)$ дизъюнктны как подмножества в 2^X. Таким образом, все множества $\bigwedge^n(X)$, $n \in \mathbb{N}$, представляют собой различные элементы 2^{2^X}. Но это значит, что 2^{2^X} содержит счетное подмножество $\{\bigwedge^n(X), n \in \mathbb{N}\}$ и, тем самым, бесконечно по Дедекинду.

6. Неизбежность выбора. Общий философский вывод из этой истории такой. Если в учебнике математического анализа говорится, что тот или иной факт использует аксиому выбора, то этому **всегда** можно верить. К утверждению же, что какой-то факт не зависит от аксиомы выбора, нужно относиться с большим подозрением и во многих случаях подобные утверждения **очевидным образом** неверны. Проследить использование аксиомы выбора в математической литературе совершенно невозможно, поскольку в большинстве случаев оно является **бессознательным**. Часто авторы даже не подозревают, что они используют ту или иную форму аксиомы выбора. Как мы знаем, любая конечная совокупность вещей образует множество. Но в тот момент, когда говорится, что какая-либо **бесконечная** совокупность вещей образует множество, единственным основанием для этого почти всегда является какая-то форма аксиомы выбора.

Для каждого, кто даст себе труд хотя бы поверхностно ознакомиться с аксиоматиками теории множеств, совершенно ясно, что те, кто заявляет, что можно каким-то образом проконтроллировать использование аксиомы выбора в математике, и разделить математику на чистую (не использующую аксиомы выбора) и нечистую (использующую аксиому выбора) – если, конечно, они не преследуют цели сознательно ввести читателя в заблуждение – просто совершенно не знают, о чем говорят. Никакое подобное разделение невозможно именно по той причине, что большинство математиков используют различные эквивалентные формы аксиомы выбора как нечто само собой разумеющееся, не отдавая себе в этом отчета и уж, разумеется, не указывая во введении к статьям, что их результаты основаны на этой аксиоме. В этом смысле ситуация с аксиомой выбора прямо противоположна ситуации, скажем, с гипотезой континуума. Ни один серьезный математик не будет использовать гипотезу континуума, не оговорив специально каждый случай зависимости его результатов от этой аксиомы. Единственный **реалистический** способ изгнать аксиому выбора из математики

состоит в том, чтобы уничтожить **всю** имеющуюся математическую литературу, забыть ее содержание и начать выводить все теоремы из аксиом **ZF** (если при этом нам не удалось забыть сами эти аксиомы) или какой-то другой системы заново. Для полной надежности при этом следует еще по примеру лучшего друга всех китайских ученых императора Цинь Ши Хуана закопать живьем всех представителей нечистой математики, желательно вместе с семьями.

§ 9. Вещественные числа

> В нашем лабиринте три лишних линии, — сказал он наконец. — Мне известен греческий лабиринт, состоящий из одной-единственной прямой линии. На этой линии заблудилось столько философов, что немудрено было запутаться простому детективу.
> — Когда я буду убивать вас в следующий раз, — ответил Шарлах, — я вам обещаю такой лабиринт, который состоит из одной-единственной прямой линии, лабиринт невидимый и непрерывный.
>
> Хорхе Луис Борхес, Смерть и Буссоль (Собр. Соч., т.1, с.387–388)

> Из несчетности множества самих вещественных чисел следует даже, что не существует языка, в котором каждое действительное число имело бы имя. Такая вещь, как, например, бесконечное десятичное разложение, не может, конечно, рассматриваться как *имя* соответствующего вещественного числа, поскольку бесконечное десятичное разложение не может даже быть полностью выписано или включено как часть в какое-нибудь фактически выписанное или произнесенное суждение.
>
> Алонзо Черч[223]

§ 10. Непрерывные дроби

Иногда удобно пользоваться другим представлением вещественных чисел, а именно их представлением в виде правильных непрерывных дробей, конечных или бесконечных. Мы достаточно подробно обсудим конечные непрерывные дроби, так как они тесно связаны с некоторыми вопросами, которые будут рассматриваться в этом курсе в дальнейшем (алгоритм Эвклида, вычисление некоторых определителей и т.д.). В то же время, мы не будем приводить никаких доказательств в случае бесконечных непрерывных дробей. Хотя этот сюжет совершенно элементарен, но доказательства достаточно длинны и используют не алгебраическую, а аналитическую технику. Поэтому мы просто точно сформулируем основной результат о бесконечных непрерывных дробях, который будет использоваться в дальнейшем для построения некоторых биекций. технику и

1. Конечные непрерывные дроби. Выражение вида

$$[q_1, q_2, \dots, q_t] = \cfrac{q_1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \dots}}},$$

где $q_1 \in \mathbb{Z}$, $q_2, \dots, q_t \in \mathbb{N}$, причем $q_t \neq 1$, называется **правильной конечной непрерывной дробью**. Следующие факты хорошо известны из элементарной теории чисел.

Задача. Докажите, что целая часть правильной конечной непрерывной дроби $[q_1, q_2, \dots, q_t]$ равна q_1.

Решение. Для $t = 1$ это очевидно. Для $t \geq 2$ заметьте, что

$$[q_1, q_2, \dots, q_t] = q_1 + \frac{1}{[q_2, \dots, q_t]},$$

причем условие правильности дроби гарантирует, что $[q_2, \dots, q_t] > 1$.

[223] А.Черч, Введение в математическую логику. т.I. – ИИЛ, М.,1960, с.1–484, стр.354.

Задача. Докажите, что любое рациональное число может быть представлено в виде правильной конечной непрерывной дроби.

Решение. Существование такого представления гарантируется **алгоритмом Эвклида**. В самом деле, рассмотрим рациональное число m/n, $m \in \mathbb{Z}$, $n \in \mathbb{N}$. Поделим m с остатком на n; потом поделим n с остатком на остаток r_1, получающийся при первом делении; потом поделим r_1 с остатком на остаток r_2, получающийся при втором делении и т.д., пока не произойдет деления нацело:

$$\begin{aligned} m &= q_1 n + r_1, && 0 \le r_1 < n, \\ n &= q_2 r_1 + r_2, && 0 \le r_2 < r_1, \\ r_1 &= q_3 r_2 + r_3, && 0 \le r_3 < r_2, \\ &\dots \\ r_{t-3} &= q_{t-1} r_{t-2} + r_{t-1}, && 0 \le r_{t-1} < r_{t-2}, \\ r_{t-2} &= q_t r_{t-1}, \end{aligned}$$

где q_i – **неполные частные** алгоритма Эвклида, а r_i – остатки. Теперь разделив первое равенство на n получим $m/n = q_1 + r_1/n = q_1 + 1/(n/r_1)$. Подставляя сюда второе равенство, разделенное на r_1 и так далее, окончательно получим

$$m/n = [q_1, q_2, \dots, q_t].$$

Задача. Докажите, что представление из предыдущей задачи единственно.

Решение. Пусть $[p_1, \dots, p_s] = [q_1, \dots, q_t]$ два представления одного и того же рационального числа x в виде правильных конечных непрерывных дробей, причем $s \le t$. Проведем индукцию по s. В качестве базы индукции возьмем случай $s = 1$, когда утверждение очевидно. В общем случае заметим, что $p_1 = q_1 = \lfloor x \rfloor$ есть целая часть x. Тем самым, $[p_2, \dots, p_s] = [q_2, \dots, q_t]$ и, следовательно, по индукционному предположению, выполняются равенства $s = t$ и $p_i = q_i$ для всех $2 \le i \le s$.

2. Бесконечные непрерывные дроби. Выражение вида

$$[q_1, q_2, q_3, \dots] = \cfrac{q_1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \dots}}},$$

где $q_1 \in \mathbb{Z}$, $q_2, q_3 \dots \in \mathbb{N}$, называется **правильной бесконечной непрерывной дробью**. Можно показать, что для **каждой** такой дроби последовательность **подходящих дробей** $[q_1]$, $[q_1, q_2]$, $[q_1, q_2, q_3]$, $\dots$ имеет предел, называемый **значением** дроби $[q_1, q_2, q_3, \dots]$. При этом значение бесконечной дроби является **иррациональным** числом, причем **каждое** иррациональное число x является значением **единственной** правильной бесконечной непрерывной дроби. Эта бесконечная дробь описывается следующим образом. В качестве q_1 возьмем целую часть числа x, в качестве q_2 – целую часть числа $1/(x - q_1)$, в качестве q_3 – целую часть числа $1/(1/(x - q_1) - q_2)$ и так далее. Так как число x иррационально, этот процесс должен быть бесконечен.

Так как эти утверждения лежат на грани элементарной теории чисел и математического анализа, мы не будем их доказывать (см., например, Гл. 6 книги Михеловича “Теория чисел”, М., Высшая школа, 1967, 336С.), однако для построения явных биекций между некоторыми множествами мощности континуума мы будем использовать следующий результат.

Теорема. *Сопоставление дроби $[q_1, q_2, q_3, \dots]$, $q_1 \in \mathbb{Z}$, $q_2, q_3, \dots \in \mathbb{N}$, ее значения осуществляет биекцию между множеством всех правильных бесконечных непрерывных дробей и множеством всех иррациональных чисел.*

3. Периодические непрерывные дроби. Как мы знаем, рациональные числа изображаются периодическими десятичными дробями. А вот что изображают периодические непрерывные дроби? Значение любой периодической дроби заведомо должно быть иррациональным числом, но что это за числа? Ответ на этот вопрос дается замечательной **теоремой**

Лагранжа: значение любой правильной периодической непрерывной дроби является вещественной квадратической иррациональностью, т.е. имеет вид $m \pm \sqrt{l}/n$, $m \in \mathbb{Z}$, $l, n \in \mathbb{N}$, и, обратно, каждая вещественная квадратическая иррациональность изображается периодической непрерывной дробью.

§ 11. Мощность континуума

> When, in early adolescence, I first saw the proof that the real numbers were uncountable, it seemed the most wonderful thing in the world to me, and I found it quite strange that the rest of the world did not share my enthusiasm.
>
> Judith Roitman, [R], p.vii

1. Эквивалентность двух любых нетривиальных промежутков. Покажем, что два любых промежутка вещественной оси, не пустых и не сводящихся к одной точке, эквивалентны. Пусть вначале $[a, b]$ и $[c, d]$, где $a < b$ и $c < d$, два нетривиальных отрезка вещественной оси. Легко построить много примеров биекций между ними. Например, очевидно, что существует линейная функция, реализующая биекцию между этими отрезками, притом, если потребовать дополнительно, чтобы эта функция была возрастающей – единственная такая функция. В самом деле, через любые две различные точки на плоскости, в частности через точки (a, c) и (b, d), проходит единственная прямая, а именно, прямая, определенная уравнением $y = \dfrac{(d-c)}{(b-a)}(x-a) + c$. Заметим, что то же самое доказательство доказывает и что любые два нетривиальных интервала $]a, b[$ и $]c, d[$ эквивалентны.

Так как полуоткрытые промежутки $]a, b]$ и $[a, b[$ лежат между интервалом $]a, b[$ и отрезком $[a, b]$, то по теореме Кантора-Бернштейна для завершения доказательства того, что любые два нетривиальных промежутка эквивалентны, нам остается лишь показать, что интервал $]a, b[$ эквивалентен отрезку $[a, b]$, причем, так как мы уже знаем, что любые два нетривиальных интервала и любые два нетривиальных отрезка эквивалентны между собой, достаточно доказать, что интервал $]0, 1[$ эквивалентен отрезку $\mathbb{I} = [0, 1]$. Для доказательства этого снова воспользуемся теоремой Кантора-Бернштейна. Ясно, что $]0, 1[\subseteq [0, 1]$, поэтому мощность $]0, 1[$ не больше мощности $[0, 1]$. С другой стороны $[1/3, 2/3]$ – нетривиальный отрезок, содержащийся в $]0, 1[$, по уже доказанному он эквивалентен $[0, 1]$ и, значит, мощность $]0, 1[$ не меньше мощности $[0, 1]$. По теореме Кантора-Бернштейна эти мощности равны.

2. Конструктивные извращения. Мы только что использовали теорему Кантора-Бернштейна вместо того, чтобы явно построить биекции между $[0, 1]$, $[0, 1[$, $]0, 1]$ и $]0, 1[$. Подобная ситуация в высшей степени типична: если даны два множества A и B, относительно которых мы *подозреваем*, что они эквивалентны, то обычно **значительно** легче построить две инъекции A в B и B и A, чем одну биекцию между A и B. При этом в большинстве случаев подобная явная биекция абсолютно бесполезна и ее конструкция не дает ничего нового, по сравнению с фактом существования биекции, вытекающим из теоремы Кантора-Бернштейна. Поэтому возникающая во многих элементарных руководствах борьба за явное построение биекций в подобных случаях представляется мне по меньшей мере чисто олимпиадной деятельностью, не имеющей никакого отношения к математике большого стиля – а в некоторых случаях просто извращением. Однако сейчас и мы слегка извратимся.

Задача. Построить явные биекции между $[0, 1]$, $[0, 1[$, $]0, 1]$ и $]0, 1[$.

Указание. Обратите внимание, что бесконечные объединения устраняют различие между отрезками и интервалами, например,

$$\cup[1/2^n, 1 - 1/2^n] = \cup]1/2^n, 1 - 1/2^n[= (0, 1),$$

и подумайте, как это можно использовать.

Начало решения. Построим для примера биекцию между $]0,1[$ и $]0,1]$. Так как в $]0,1]$ есть наибольший элемент, а в $]0,1[$ нет, то требуемая биекция не может быть возрастающей (почему?). Это подсказывает, что нужно породить на $]0,1]$ достаточное (ну, хотя бы, счетное) количество разрывов. Ну, например, представить $]0,1]$ в виде бесконечного дизъюнктного объединения

$$]0,1] =]1/2,1] \coprod]1/4,1/2] \coprod]1/8,1/4] \coprod \dots$$

после чего задать биекцию $]0,1]$ на $]0,1[$ руководствуясь известной максимой 'последние станут первыми'. А именно, существует возрастающая линейная функция, отображающая $]1/2,1]$ на $]0,1/2]$, еще одна такая же функция, отображающая $]1/4,1/2]$ на $]1/2,3/4]$, еще одна, отображающая $]1/8,1/4]$ на $]3/4,7/8]$ и т.д. Однако ясно, что

$$]0,1/2] \coprod]1/2,3/4] \coprod]3/4,7/8] \coprod \dots =]0,1[.$$

Постройте в таком же духе остальные биекции.

3. Эквивалентность $\mathbb{R}$ и любого непустого интервала. Так как мы уже показали, что все нетривиальные интервалы эквивалентны, нам достаточно показать эквивалентность какого-нибудь из них с $\mathbb{R}$. Построение биективного соответствия между интервалом $]-1,1[$ и всей вещественной осью совершенно ясно из следующей картинки:

картинка – картинка

В действительности, биекция, описанная этой картинкой, состоит из композиции двух биекций: измерения углов, которое мы производим довольно странным образом, и сопоставления углу его тангенса. Так зачем нам после этого измерять углы? Мы можем просто вспомнить, что, как хорошо известно из тригонометрии (должна же и она когда-нибудь для чего-нибудь пригодиться!), функция tan устанавливает биекцию интервала $]-\pi/2,\pi/2[$ с вещественной осью $\mathbb{R}$.

Задача по тригонометрии. А какая в точности функция описана картинкой ??

Разумеется, можно придумать тысячи других биекций между интервалами вещественной оси и всей осью.

Задача на дифференцирование. Постройте *рациональную* функцию, устанавливающую биекцию между интервалом $]0,1[$ и всей вещественной осью.

Указание. Ясно, что эта функция не может быть непрерывной на отрезке $[0,1]$, иначе она ограничена. Проще всего считать, что она обращается в $-\infty$ в $0+$ и в $+\infty$ в $1-$ ну, скажем, $x \mapsto \dfrac{1}{1-x} - \dfrac{1}{x}$. Устанавливает ли уже эта функция требуемую биекцию или ее нужно как-то подправить?

Задача. Покажите, что функция $x \mapsto \dfrac{x}{1+|x|}$ устанавливает биекцию $\mathbb{R}$ и $(-1,1)$.

Указание. Достаточно проверить, что $x \mapsto \dfrac{x}{1-|x|}$ задает обратное отображение.

4. Несчетность множества вещественных чисел. Каждый элемент интервала $(0,1)$ может быть представлен в десятичной записи как $0, c_1c_2c_3\dots$, где $c_i \in \mathrm{Digit}$, причем, исключены две следующие ситуации: i) все c_i одновременно равны 0 и ii) все c_i, кроме конечного числа, равны 9.

Теорема Кантора. *Множество $\mathbb{R}$ вещественных чисел несчетно.*

Доказательство. Так как $\mathbb{R}$ равномощно интервалу $(0,1)$, то достаточно доказать, что интервал $(0,1)$ несчетен. Предположим, что множество $(0,1)$ счетно и пусть $(0,1) = \{x_1, \dots, x_n, \dots\}$. Представим каждое x_i в десятичной записи как $x_i = 0, c_1^i c_2^i c_3^i \dots$. Построим теперь новое число $x = 0, c_1 c_2 c_3 \dots$ в интервале $(0,1)$ следующим образом. Положим c_i равным

$$c_i = \begin{cases} 1, & c_i^i \neq 1 \\ 2, & c_i^i = 1 \end{cases}$$

Ясно, что число x отлично от всех чисел x_i. В самом деле, для того, чтобы убедиться, что $x \neq x_i$, достаточно посмотреть на его i-ю цифру c_i, которая по самому построению x отлична от c_i^i.

Метод, примененный в доказательстве этой теоремы, называется **Канторовским диагональным процессом** (Cantorsche Diagonalverfahren). Это один из наиболее продуктивных приемов, который применяется в громадном количестве доказательств, поэтому сознательное владение этим методом совершенно необходимо каждому, кто серьезно изучает математику. Когда я в первый раз увидел Канторовское доказательство в 9-м классе школы, оно произвело на меня такое впечатление, что я решил стать математиком.

5. Второе доказательство Кантора. В действительности, Кантор дал еще одно (исторически, по-видимому, первое) столь же замечательное доказательство теоремы о несчетности множества вещественныъ чисел, основанное непосредственно на аксиоме Кантора. Это доказательство носит значительно более общий характер и легко обобщается на широкий класс топологических пространств.

Второе оказательство Теоремы ?. Предположим, что мы занумеровали все точки отрезка $[0,1]$ так что $[0,1] = \{x_1, x_2, x_3, \dots\}$. Выберем любой нетривиальный отрезок $I_1 \subseteq [0,1]$ не содержащий x_1. Теперь возьмем любой нетривиальный отрезок $I_2 \subseteq I_1$, не содержащий x_2 и продолжим действовать таким же образом. В результате мы получим убывающую последовательность вложенных отрезков $I_1 \supseteq I_2 \supseteq I_3 \supseteq \dots$. Рассмотрим пересечение $\cap I_i$, $i \in \mathbb{N}$, этой последовательности. Согласно аксиоме Кантора оно непусто, так что существует точка $x \in \cap I_i$. Ясно, что x не может совпадать ни с одной из точек x_i. В самом деле, $x_i \notin I_i$, в то время как $x \in I_i$. Полученное противоречие показывает, что занумеровать все точки отрезка $[0,1]$ невозможно.

Сам Кантор описывал это доказательство в терминах более близких к первому доказательству и теснейшим образом связанных с построением **канторова множества**. А именно, он *строил* точку x следующим образом. Представим $[0,1]$ в виде объединения трех отрезков $[0,1/3] \cup [1/3,2/3] \cup [2/3,1]$. Заметим, что это не разбиение отрезка $[0,1]$, но так как второй отрезок пересекается с первым лишь по точкам $1/3$ и $2/3$ соответственно, то *по крайней мере* один из этих отрезков не содержит точки x_1. Возьмем этот отрезок в качестве I_1 – в массовом случае таких отрезков два, и мы возьмем *левый*. Повторим эту процедуру, разбив отрезок на три равные части и возьмем в качестве I_2 отрезок, не содержащий x_2, и т.д. В таком виде это доказательство почти текстуально совпадает с первым доказательством, но в троичной системе.

§ 13. Свойства мощности континуума

> Alice laughed: "There's no use trying," she said; "one can't believe impossible things." "I daresay you haven't had much practice," said the Queen. "When I was younger, I always did it for half an hour a day. Why, sometimes I've believed as many as six impossible things before breakfast."
>
> Lewis Carroll, 'Alice in Wonderland'

1. Объединение счетного множества множеств мощности континуума. Для множеств мощности континуума выполняются аналоги утверждений ? и ?.

Теорема. *Объединение конечного числа множеств мощности континуума имеет мощность континуума.*

Доказательство. Пусть $X_1, \dots, X_n$ суть n множеств мощности континуума. Зафиксируем биекцию $f_i :]i-1, i[\longrightarrow X_i$. Тогда отображение $f = f_1 \coprod \dots \coprod f_n$, являющееся склейкой отображений $f_1, \dots, f_n$, является сюръекцией множества $\cup]i-1, i[$, $i \in \underline{n}$, имеющего мощность континуума (почему?), на множество $X = \cup X_i$, $i \in \underline{n}$. Таким образом, мощность X не превосходит мощности континуума.

В этом рассуждении мы использовали аксиому выбора (где?), но здесь ее легко обойти (как?). А вот в следующей задаче обойтись без использования аксиомы выбора невозможно.

Задача. Покажите, что объединение счетного числа множеств мощности континуума снова имеет мощность континуума.

Указание. Множество $\cup]i-1, i[$, $i \in \mathbb{N}$, имеет мощность континуума.

2. Сколько точек в квадрате? В течение трех лет Кантор безуспешно пытался доказать, что мощность множества точек квадрата **больше** множества точек отрезка. Наконец, он обнаружил взаимно однозначное соответствие между ними, т.е. доказал, что *квадрат имеет столько же точек, сколько отрезок*. "Я вижу это соответствие, но я не верю в него", написал он в одном из писем.

Теорема Кантора. *Множество $\mathbb{I}^2$ эквивалентно $\mathbb{I}$.*

Первое доказательство. Рассмотрим единичный отрезок $\mathbb{I} = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$ и единичный квадрат $\mathbb{I}^2 = \{(x, y) \mid x, y \in \mathbb{R},\ 0 \leq x, y \leq 1\}$. Так как $f : \mathbb{I} \longrightarrow \mathbb{I}^2$, $x \mapsto (x, 0)$, задает вложение $\mathbb{I}$ в $\mathbb{I}^2$, то теореме Бернштейна-Кантора достаточно показать, что квадрат имеет не больше точек, чем отрезок. Каждая точка (x, y) квадрата представляется двумя упорядоченными последовательностями цифр $x = 0, i_1 i_2 i_3 \dots$ и $y = 0, y_1 y_2 y_3 \dots$. Образуем новую последовательность $z = 0, x_1 y_1 x_2 y_2 x_3 y_3 \dots$. Ясно, что задание последовательности z полностью определяет исходные последовательности x и y, так что различным точкам квадрата отвечают различные точки отрезка, может быть не все.

Легко видеть, что из теоремы Кантора сразу вытекают такие следствия.

Следствие 1. *Эвклидова плоскость $\mathbb{R}^2$ имеет мощность континуума.*

Следствие 2. *Множество $\mathbb{C}$ комплексных чисел имеет мощность континуума.*

3. Так чем же квадрат отличается от отрезка? Людям, неискушенным в математике, кажется, что в квадрате **больше** точек, чем в отрезке. Это связано с тем, что с наивной (доканторовской) точки зрения понятие **количества** точек, содержащихся в фигуре, связывается с другими инвариантами этой фигуры, например, **мерой** или **размерностью** этой фигуры. Обычно, представляя себе отрезок или квадрат, мы мыслим их не просто как множества, а как множества с дополнительными структурами.

Обычной мерой плоской фигуры является ее **площадь**. Площадь отрезка равна нулю, поэтому он кажется *маленьким*, по сравнению с квадратом, площадь которого положительна. Однако площадь является довольно тонким **аналитическим** инвариантом плоских множеств, связанных с наличием на эвклидовой плоскости каких-то дополнительных структур,

а никак не строением квадрата и отрезка *как множеств*. Таким образом, различие площадей двух фигур означает всего лишь, что невозможно перевести одну из них в другую преобразованием **сохраняющим меру**, например, **движением**.

Еще один смысл, в котором квадрат кажется больше отрезка – это **размерность**. Размерность отрезка равна 1, в то время как размерность квадрата равна 2. Размерность является чрезвычайно сложным **топологическим** инвариантом – чудовищно более сложным, чем считает большинство нематематиков и даже математиков-неспециалистов. Подобно мере она зависит от наличия на множестве каких-то дополнительных структур. Различие размерностей двух фигур означает лишь, что не существует **непрерывных** биективных преобразований, переводящих одну из них в другую. Как легко видеть, отображение, построенное в доказательстве Теоремы ?, не является непрерывным.

Задача по топологии. Покажите, что не существует непрерывной биекции $f : \mathbb{I}^2 \longrightarrow \mathbb{I}$. При этом достаточно даже предполагать, что f раздельно непрерывна по каждой переменной.

Тем не менее даже в том, что касается *непрерывных* отображений ситуация значительно сложнее, чем кажется на первый взгляд. В 1890 году Пеано построил непрерывное **сюръективное** отображение отрезка $\mathbb{I}$ на квадрат $\mathbb{I}^2$ – **кривая Пеано**.

3. А сколько точек в эвклидовом пространстве? Иными словами, Теорема ? утверждает, что декартово произведение двух множеств мощности континуума снова имеет мощность континуума. С использованием операций над мощностями это становится совсем очевидным.

Второе доказательство. Так как объединение двух счетных множеств счетно, то

$$\mathfrak{c} \times \mathfrak{c} = 2^{\aleph} \times 2^{\aleph} = 2^{\aleph\times\aleph} = 2^{\aleph} = \mathfrak{c}.$$

Это наблюдение легко обобщить.

Задача. Докажите, что произведение конечного числа множеств мощности континуума имеет мощность континуума.

Решение. Для конечного числа множеств это сразу вытекает по индукции из Теоремы ?, либо может быть доказано тем же рассуждением, что второе доказательство Теоремы ?.

Следствие. *Эвклидово пространство $\mathbb{R}^n$ имеет мощность континуума.*

4. Мощность множества бесконечных последовательностей. В предположении аксиомы выбора это может быть обобщено еще дальше.

Теорема. *Произведение счетного числа множеств мощности континуума само имеет мощность континуума.*

Доказательство. В силу аксиомы выбора мощность этого произведения равна

$$\mathfrak{c}^{\aleph} = \left(2^{\aleph}\right)^{\aleph} = 2^{\aleph\times\aleph} = 2^{\aleph} = \mathfrak{c}.$$

Предостережение. Без аксиомы выбора эта теорема неверна – произведение счетного числа множеств мощности континуума может быть пустым! Однако всегда можно утверждать, что мощность счетного произведения множеств мощности континуума имеет мощность, **не превосходящую** мощность континуума.

Контрольный вопрос. Где в предыдущем доказательстве использована аксиома выбора?

Ответ. Ну, конечно, в самом начале, когда мы написали, что мощность произведения счетного числа множеств мощности континуум равна $\mathfrak{c}^{\aleph}$.

Следствие. *Множество $\mathbb{R}^{\mathbb{N}}$ бесконечных последовательностей вещественных чисел имеет мощность континуума.*

5. Мощность множества непрерывных функций. Как мы видели в § ? уже мощность множества отображений из $\mathbb{R}$ в $\underline{2}$ строго больше мощности континуума. Тем более это относится к множеству $\mathbb{R}^{\mathbb{R}}$ всех вещественных функций вещественного аргумента. Поэтому на первый взгляд следующее утверждение представляется достаточно удивительным.

Задача. Докажите, что множество непрерывных функций $\mathbb{R} \longrightarrow \mathbb{R}$ имеет мощность континуума.

Решение. Очевидно, что для любого $c \in \mathbb{R}$ постоянная функция $x \mapsto c$ непрерывна на всей вещественной оси, поэтому мощность множества непрерывных функций не меньше мощности континуума. С другой стороны, ясно, что непрерывная функция $f : \mathbb{R} \longrightarrow \mathbb{R}$ полностью определяется своими значениями в рациональных точках. В самом деле, любое вещественное число x может быть представлено как предел последовательности x_i, $i \in \mathbb{N}$, **рациональных** чисел. Аналитическое определение непрерывности как раз и состоит в том, что тогда $f(x)$ является пределом последовательности $f(x_i)$, $i \in \mathbb{N}$. Таким образом, мощность множества непрерывных функций не больше, чем мощность $\mathbb{Q}^{\mathbb{R}}$. Однако это последнее множество находится во взаимно однозначном соответствии с множеством всех последовательностей вещественных чисел, которое, как мы только что видели, имеет мощность континуума.

§ 14. Дальнейшие примеры множеств мощности континуума

1. Множества иррациональных и трансцендентных чисел. Все множество вещественных чисел $\mathbb{R}$ является дизъюнктным объединением множества $\mathbb{Q}$ рациональных чисел и множества $\mathbb{R} \setminus \mathbb{Q}$ **иррациональных** чисел. Как мы знаем, множество рациональных чисел счетно. Если бы множество иррациональных чисел тоже было счетно, то по ?.? отсюда следовало бы, что $\mathbb{R}$ тоже счетно, а как мы только что видели, это не так. Таким образом $\mathbb{R} \setminus \mathbb{Q}$ **несчетно**. С другой стороны, его мощность, очевидно, не превосходит мощности $\mathbb{R}$. В частности, в предположении гипотезы континуума отсюда сразу следовало бы, что $\mathbb{R} \setminus \mathbb{Q}$ имеет мощность континуума.

Разумеется, то же рассуждение можно повторить и для множества **трансцендентных** чисел. А именно, пусть $\overline{\mathbb{Q}}$ представляет собой множество алгебраических чисел. Как мы видели в § ?, это множество счетно. Таким образом, тем более счетным является множество вещественных алгебраических чисел $\mathbb{R} \cap \overline{\mathbb{Q}}$. Но тогда в силу тех же соображений, что и выше, его дополнение $\mathbb{R} \setminus \overline{\mathbb{Q}}$ в множестве $\mathbb{R}$ **несчетно**. Снова в предположении гипотезы континуума отсюда вытекает континуальность множества трансцендентных чисел.

В действительности, однако, тот факт, что мощность множеств иррациональных чисел и трансцендентных чисел равна $\mathfrak{c}$ не зависит ни от гипотезы континуума, ни от аксиомы выбора и может быть доказан несколькими различными способами, как при помощи теоремы Кантора-Бернштейна, так и явным построением биекции с множеством мощности континуума. Сейчас мы это и проделаем, причем по ходу познакомимся и с другими интересными примерами множеств мощности континуум.

2. Пространство Бэра. Декартова степень $X = \mathbb{N}^{\aleph_0}$ называется **пространством Бэра** (при этом обычно подразумевается, что X снабжается некоторой топологией, а именно, Тихоновским произведением дискретных топологий на $\mathbb{N}$, см. Гл. ?). Таким образом, пространство Бэра это множество счетных последовательностей натуральных чисел. Как мы видели в § ?, множество всех конечных последовательностей натуральных чисел счетно.

Теорема. *Пространство Бэра имеет мощность континуума.*

Доказательство. Ясно, что пространство Бэра содержит множество $2^{\aleph_0}$ которое имеет мощность континуума, поэтому его мощность не меньше $\mathfrak{c}$. С другой стороны, по Теореме ? выполняется неравенство $\mathfrak{a}^{\mathfrak{a}} \leq \mathfrak{c}^{\mathfrak{a}} \leq \mathfrak{c}$, так что мощность пространства Бэра не больше мощности континуума.

Другими словами, эта теорема утверждает, что множество $\mathbb{N}^{\mathbb{N}}$ бесконечных последовательностей $(n_i)_{i\in\mathbb{N}}$ натуральных чисел имеет мощность континуума. В принципе в этом нет ничего удивительного, так как мы уже знаем, что уже множество бесконечных последовательностей нулей и единиц имеет мощность континуума. Часто приходится использовать не саму эту теорему, а различные вариации на эту тему, где пространство Бэра возникает в слегка замаскированном виде. Вот два типичных примера, возникающих в приложениях.

Задача. Докажите, что каждое из следующих множеств имеет мощность континуума:

1) Множество строго возрастающих последовательностей натуральных чисел, $n_{i+1} > n_i$;

2) Множество таких последовательностей натуральных чисел, в которых каждый член делит последующий, $n_i | n_{i+1}$.

Решение. Наиболее простой способ состоит, конечно, в том, чтобы использовать теорему Кантора-Бернштейна. Однако несложно и прямо построить биекции между этими множествами и $\mathbb{N}^{\mathbb{N}}$. В первом случае такая биекция задается посредством $(n_i) \mapsto (n_i - n_{i-1})$, а во втором – посредством $(n_i) \mapsto (n_i/n_{i-1})$. Еще одна похожая ситуация встретится нам в конце настоящего параграфа в связи с теоремой Лиувилля.

3. Одна замечательная биекция. Сопоставим элементу $(n_1, n_2, n_3, \dots)$ пространства Бэра непрерывную дробь

$$\cfrac{1}{n_1 + \cfrac{1}{n_2 + \cfrac{1}{n_3 + \dots}}}.$$

Известно, что это отображение является биекцией пространства Бэра на множество иррациональных чисел интервала $]0, 1[$. Таким образом, множество всех иррациональных чисел интервала $]0, 1[$ имеет мощность континуума.

Задача. Докажите, что множество иррациональных чисел интервала $]a, b[$, $a < b$, имеет мощность континуума.

Указание. Для этого совсем не обязательно строить **биекцию** между множеством иррациональных чисел интервала $]0, 1[$ и множеством иррациональных чисел интервала $]a, b[$.

4. Удаление счетного множества из множества мощности континуума. Сейчас мы покажем, что разность множества мощности континуума и счетного множества имеет мощность континуума. Разумеется, фокус здесь состоит в том, чтобы доказать это, не используя аксиому выбора!

Теорема. *Если* $|X| = \mathfrak{c}$ *и* $|Y| = \mathfrak{a}$, *то* $|X \setminus Y| = \mathfrak{c}$.

Доказательство. "Небольшая хитрость" – [J], § 6. Зафиксируем биекцию f множества X с множеством $X \times X$ (см. ?.?). Нам достаточно показать, что $X \times X \setminus f(Y)$ имеет мощность не меньшую мощности континуума. Так как $f(Y)$ счетно, то, тем более, счетна и первая проекция этого множества $\mathrm{pr}_1(f(X))$. Так как само множество X имеет мощность континуума, найдется $x \in X$, не принадлежащее этой проекции. Это значит, что для всех $y \in X$ пара (x, y) не принадлежит $f(Y)$. Поскольку множество пар $\{(x, y) \mid y \in X\}$ эквивалентно X, это и значит, что мощность $X \times X \setminus f(X)$ по крайней мере не меньше мощности континуума.

5. Мощность множества трансцендентных чисел. Применяя эту теорему к ситуации, рассмотренной в пункте 1, получаем такое следствие, впервые доказанное Кантором в 1874 году.

Следствие. *Множество трансцендентных чисел нетривиального интервала* $]a, b[$, $a < b$, *имеет мощность континуума.*

Доказательство Кантора замечательно тем, что оно носит чисто экзистенциальный характер, из него вытекает, что трансцендентные числа **существуют**, поскольку их множество имеет большую мощность, но *ни одного трансцендентного числа при это не предъявляется.*

Комментарий. Значительно менее известно, что из конструктивного доказательства существования трансцендентных чисел, данного Лиувиллем[224] в 1851 году, тоже сразу следует, что мощность множества трансцендентных чисел не меньше мощности континуума. А именно, знаменитая **теорема Лиувилля** утверждает, что иррациональные алгебраические числа не могут хорошо аппроксимироваться последовательностями рациональных чисел. Поэтому всякое иррациональное число, которое хорошо аппроксимируется рациональными числами, обязано быть трансцендентным. Отправляясь от этого наблюдения, Лиувилль строит громадный класс непрерывных дробей $[q_1, q_2, q_3, \dots]$, представляющих трансцендентные числа. А именно, рассмотрим соответствующую последовательность подходящих дробей $[q_1, q_2, \dots, q_t] = m_t/n_t$, где $m_t \in \mathbb{Z}$, $n_t \in \mathbb{N}$, и предположим, что q_t быстро растут, а именно, что для каждого t выполняется неравенство $q_{t+1} > n_t^t$. Несложно проверить, что в этом случае значение непрерывной дроби $[q_1, q_2, q_3, \dots]$ хорошо аппроксимируется подходящими дробями m_t/n_t и, следовательно, обязано быть трансцендентным. Ясно, что на каждом шаге мы запрещаем лишь конечное множество возможностей для $q_t \in \mathbb{N}$, так что уже множество трансцендентных чисел, представимых как значения непрерывных дробей описанного выше типа, имеет мощность $\mathfrak{a}^{\mathfrak{a}} = \mathfrak{c}$. Конечно, доказательство Кантора значительно проще. Метод Лиувилля позволяет строить **много** трансцендентных чисел (как говорит сам Лиувилль, "des classes **trés** etendues"). Тем не менее, доказательство трансцендентности конкретных чисел в каждом случае представляет собой совершенно нетривиальную задачу. Например, трансцендентность e была доказана лишь в 1873 году Эрмитом, а трансцендентность π – лишь в 1882 году Линдеманном.

§ 15. Гипотеза континуума

> Мы констатируем, что такие старые и трудные проблемы, как доказательства аксиомы о параллельных, как квадратура круга или решение уравнений пятой степени в радикалах, получили все же строгое, вполне удовлетворяющее нас решение, хотя и в другом направлении, чем то, которое сначала предполагалось.
>
> Давид Гильберт "Математические Проблемы"

1. Континуум-гипотеза. Как мы знаем, мощность $\mathfrak{c}$ множества $\mathbb{R}$ вещественных чисел строго больше мощности $\aleph_0$ множества $\mathbb{Z}$ целых чисел. В 1878 году Георг Кантор высказал следующую гипотезу

Континуум-гипотеза. *Не существует мощности промежуточной между* $\aleph_0$ *и* $\mathfrak{c}$.

Иными словами, утверждается, что если $\aleph_0 \leq |X| \leq \mathfrak{c}$ для некоторого множества X, то либо $|X| = \aleph_0$, либо $|X| = \mathfrak{c}$. Эта гипотеза называется еще **гипотезой континуума** и обозначается **CH**. В 1900 году на II Международном Математическом Конгрессе в Париже Давид Гильберт назвал эту гипотезу

[224] **Жозеф Лиувилль** (24.03.1809, St.Omer – 08.09.1882, Париж) – один из наиболее значительных математиков XIX века, преподавал в l'Ecole Politechnique, Collège de France и Сорбонне. Кроме имевшего большой резонанс конструктивного доказательства существования трансцендентных чисел, он занимался теорией специальных функций, математической физикой, дифференциальной геометрией. Еще одна его бессмертная заслуга перед математикой состоит в том, что именно он вернул в математический обиход работы Галуа.

первой в своем знаменитом списке 23 нерешенных математических проблем (**проблемы Гильберта**), решение которых должно было значительно стимулировать дальнейшее развитие науки.

2. Непротиворечивость континуум-гипотезы. В 1884 году Кантору показалось, что он может доказать гипотезу континуума, и он даже объявил о ее **положительном** решении: в одной из своих статей того времени он даже написал, что доказательство будет дано в следующей работе. Эта статья заканчивалась словами "Fortsetzung folgt" – "продолжение следует". Однако обещанное продолжение никогда не появилось, вероятно Кантор сам обнаружил ошибку в своем доказательстве. В течение многих десятилетий многие крупнейшие математики безуспешно пытались доказать или опровергнуть эту гипотезу. Вследствие безуспешности всех попыток решения, некоторые математики стали высказывать предположение о ее неразрешимости, т.е. невозможности ее доказательства или опровержения в обычной аксиоматической теории множеств – теории Цермело-Френкеля. Первым крупным прорывом в этом направлении был результат Курта Геделя[225] 1940 года. Он доказал, что если аксиоматика теории множеств (в действительности он, конечно, работал в аксиоматике Геделя-Бернайса, а не Цермело-Френкеля, но в данном случае это не имеет значения) непротиворечива, то она остается непротиворечивой и после добавления аксиомы выбора **AC** и гипотезы континуума **CH** (в действительности даже гораздо более сильной **обобщенной гипотезы континуума GCH**, см. ниже).

3. Независимость континуум-гипотезы. В 1963 году используя развитый им **метод форсинга** американский математик Поль Коэн[226] получил полное решение проблемы, доказав ее независимость от аксиом теории множеств. Точнее, он показал, что, если аксиоматика теории множеств непротиворечива, то присоединяя к ней любую комбинацию аксиомы выбора, континуум-гипотезы и их отрицаний, мы снова получаем непротиворечивую систему. Это значит, что, как предполагая справедливость аксиомы выбора, так и предполагая, что аксиома выбора неверна, континуум-гипотезу невозможно ни доказать, ни опровергнуть! Это еще один пример "строгого, вполне удовлетворяющего нас решения, хотя и в другом направлении, чем то, которое сначала предполагалось".

4. Обобщенная континуум-гипотеза. В действительности Кантор формулировал континуум-гипотезу в форме $\mathfrak{c} = 2^{\aleph_0} = \aleph_1$. Вообще можно предпо-

---

[225]**Курт Гедель** (28.04.1906, Брно –) – один из крупнейших логиков XX века. Основные работы относятся к обоснованию арифметики и теории множеств. Теорема Геделя о полноте, теорема Геделя о неполноте. Система Геделя-Бернайса. Работал в Вене, но в 1940 году эмигрировал в США, с 1950 года работал в Institute for Advanced Studies.

[226]**Поль Коэн** (род. 02.04.1934, Longbranch, N.J.) – американский математик, самое известное достижение которого полное решение гипотезы континуума. За это замечательное достижение на Международном Конгрессе Математиков Москва–1966 Поль Коэн был удостоен высшей награды в математике – **филдсовской медали**. Интересно отметить, что по своей основной специальности Коэн не был математическим логиком, ему принадлежат существенные результаты в таких классических разделах математики, как анализ, теория топологических групп и теория дифференциальных уравнений. Это замечательный пример того, как специалист в одной области может добиться выдающегося результата в другой области. На русский язык переведена его замечательная книга 'Теория множеств и континуум-гипотеза', до сих пор являющаяся одним из лучших введений в аксиоматическую теорию множеств.

ложить, что всегда $2^{\aleph_n} = \aleph_{n+1}$. Это предположение известно под названием **обобщенной континуум-гипотезы GCH**. Обобщенная континуум-гипотеза и аксиома выбора уже не являются независимыми. В 1947 году Вацлав Серпиньский[227] доказал следующий результат.

Теорема Серпиньского. *Обобщенная гипотеза континуума влечет аксиому выбора.*

В 1963 году Р.Соловэй показал, что обобщенная континуум-гипотеза не вытекает из аксиомы выбора и континуум гипотезы.

[227]**Wacław Sierpiński** (14.03.1882, Варшава – 1969) – один из крупнейших польских математиков, создатель варшавской математической школы, автор более 700 работ, в том числе 15 монографий, значительная часть которых относится к теории множеств, топологии, теории функций и теории чисел. Ученик Г.Ф.Вороного. После учебы в Варшаве и Кракове преподавал во Львове и Варшаве. Серпиньский написал 13 научно-популярных книг, одна из которых, 'О теории множеств' переведена на русский язык. Последняя из его книг, 'Elementary theory of numbers', на которую мы часто ссылаемся в главе ?, была опубликована, когда ее автору было 82 года. В научно-популярной литературе часто упоминается 'ковер Серпиньского'.

Тема 5. Отношения

blabla

blabla[228].

§ 1. Отношения

В понятие отображения область определения X и область значений Y входят неравноправно. При этом каждому элементу $x \in X$ соответствует ровно один элемент множества Y, но элемент $y \in Y$ может не соответствовать никакому x, либо соответствовать более, чем одному x. Понятие (бинарного) отношения восстанавливает симметрию между X и Y.

1. Бинарные отношения. Пусть, как и в предыдущем параграфе, X и Y – два множества.

Определение. Бинарным отношением *между X и Y называется тройка (X, Y, R), где R подмножество $X \times Y$ декартова произведения множеств X и Y.*

В этом случае вместо **области** и **кообласти** X и Y обычно называются **левой** и **правой** областями отношения (X, Y, R), а множество R часто называется **графиком** этого отношения. Как и для отображений мы считаем, что два отношения равны, если равны их левые области, правые области и графики. Если X и Y определены контекстом, отношение полностью определяется своим графиком и в этом случае допуская вольность речи для краткости говорят просто об отношении R. В некоторых контекстах принято говорить о **соответствии** между элементами X и Y, задаваемым отношением R. Описанное выше чисто экстенсиональное понимание отношений возникло только в XX веке под влиянием Пеано. Бурбаки даже утверждают, что оно было впервые использовано итальянскими алгебраическими геометрами, в первую очередь Сегре, в работах об алгебраических соответствиях ([Bu], стр.307). Для записи отношений обычно используется **инфиксная** запись, так что вместо $(x, y) \in R$ пишут просто xRy и говорят, что

- 'x соответствует y относительно R'
- 'x находится в отношении R к y'.

Множество всех бинарных отношений между X и Y обозначается $\mathrm{Rel}(X, Y)$ (от английского relation). Если X и Y фиксированы, то отношение можно отождествить с его графиком, так что $\mathrm{Rel}(X, Y)$ становится просто другим именем для $2^{X \times Y}$. Следует, однако, иметь в виду, что если $R \subseteq U \times V \cap X \times Y$, то R рассматриваемое как элемент в $\mathrm{Rel}(U, V)$ не совпадает с R рассматриваемым как элемент в $\mathrm{Rel}(X, Y)$. В случае, когда левая и правая области отношения совпадают, т.е. $X = Y$, говорят о **бинарных отношениях на** X – отношения такого типа обычно называются **внутренними**: при этом $\mathrm{Rel}(X, X)$ часто обозначается просто $\mathrm{Rel}(X)$. Множество X называется **носителем** отношения $R \in \mathrm{Rel}(X)$.

Комментарий. В учебной литературе на русском языке принято различать соответствия и отношения, при этом отношениями называются внутренние бинарные соответствия (см., например, [Shi]). Однако, с моей точки зрения, эта

[228] blabla

практика приходит в противоречие с мематическим узусом: мы говорим 'отношение инцидентности' а не 'соответствие инцидентности'.

Среди всех отношений выделяются **тривиальное** или **пустое** отношение $\varnothing$ и само множество $X \times Y$, рассматриваемое как отношение между X и Y, называемое в этом случае **тотальным**, **универсальным** или **полным** отношением. В случае $X = Y$ совершенно особую роль играет еще **тождественное** отношение, графиком которого является множество пар $\{(x, x) \mid x \in X\}$, называемое обычно **диагональю** произведения $X \times X$ и обозначаемое Δ_X, или просто Δ, если ясно, о каком X идет речь.

Если $R \subseteq S$, то отношение R называется более **тонким**, чем отношение S, а отношение S – более **грубым**, чем R. Таким образом, $\varnothing$ – самое тонкое, а $X \times Y$ – самое грубое отношение между X и Y.

2. Реляционные системы. Пара (X, R), состоящая из множества X и заданного на нем внутреннего бинарного отношения, является простейшим примером того, что называется **реляционной системой** (точнее, это система сигнатуры (2) – система, состоящая из одного бинарного отношения). Две системы (X, R) и (Y, S) **изоморфны**, если существует такая биекция $\phi : X \longrightarrow Y$, что $\phi \times \phi(R) = S$. Следующая задача позволяет по достоинству оценить трудности, связанные такого рода комбинаторными задачами. Пусть r_n – количество неизоморфных реляционных систем сигнатуры (2) на n-элементном множестве.

Задача. Показать, что $r_2 = 10$. Перечислить все неизоморфные реляционные системы на множестве из двух элементов

Число r_n растет фантастически быстро. А именно, $r_3 = 104$, $r_4 = 3044$, а $r_5 = 291968$. По видимому, в этом месте читатель не должен испытывать особого желания классифицировать с точностью до изоморфизма все реляционные системы на шестиэлементном множестве.

3. Примеры бинарных отношений. Оставшаяся часть этого пункта будет посвящена примерам бинарных отношений. Первая группа примеров относится к теории множеств.

• **Отношение принадлежности** '$\in$': здесь $Y = 2^Z$ и $xRA \Longleftrightarrow x \in A$.

• **Отношение включения** '$\subseteq$': здесь $X = Y = 2^Z$ и $ARB \Longleftrightarrow A \subseteq B$.

• **Отношение равенства** '$=$': здесь $X = Y$ и $xRy \Longleftrightarrow x = y$.

• **Отношение дизъюнктности**: здесь $X = Y = 2^Z$ и $ARB \Longleftrightarrow A \cap B = \varnothing$.

Конечно, весьма важными частными видами отношений являются отображения и их обобщения:

• **Отображение** $f : X \longrightarrow Y$. Здесь $xRy \Longleftrightarrow f(x) = y$. В действительности, отображение как раз и есть не что иное, как такое бинарное отношение R, что $\forall x \in X\ \exists! y \in Y,\ xRy$.

• **'Многозначная функция'** $f : X \multimap Y$ – это бинарное отношение R удовлетворяющее более слабому условию $\forall x \in X\ \exists y \in Y,\ xRy$.

• **'Частичная функция'** $f : X \dashrightarrow Y$ – это бинарное отношение R удовлетворяющее другому ослаблению фигурирующего в 5) условия, а именно, $\forall x \in X\ xRy_1\ \&\ xRy_2 \Longrightarrow y_1 = y_2$.

С этой точки зрения произвольное бинарное отношение как раз и есть не что иное, как 'многозначная частичная функция', в то время как отображение есть по определению 'однозначная всюду определенная функция'.

Конечно, другие разделы школьной математики также дают нам множество примеров бинарных отношений. Обратимся, скажем, к элементарной геометрии. Там обычно говорят об отношениях, задаваемых различными типами

геометрических преобразований: скажем, отношении конгруэнтности, подобия и т.д. Вот еще несколько примеров.

• **Отношение параллельности**: пусть $X = Y$ есть множество прямых (или плоскостей) двумерного (или трехмерного) эвклидова пространства. Тогда $lRm \iff l \parallel m$.

• **Отношение ортогональности**: ibid., положим $lRm \iff l \perp m$.

• **Отношение инцидентности**: X - множество точек эвклидовой плоскости (или трехмерного пространства), Y – множество прямых, $xRl \iff x \in l$.

Еще одна группа примеров возникает в арифметике. Здесь мы предполагаем $X = Y = \mathbb{Z}$, анализ и обобщение этих примеров будет одной из наших основных целей в следующей главе.

• **Отношение порядка**: $mRn \iff m < n$ в обычном смысле.

• **Отношение делимости**. Будем писать $m|n$, если m делит n, т.е. существует такое $l \in \mathbb{Z}$, что $n = ml$ (то же самое часто записывается и как $n \vdots m$, 'n делится на m'). Тогда $mRn \iff m|n$.

• **Отношение ассоциированности**: $mRn \iff m|n \ \ \& \ \ n|m$.

• **Отношение сравнимости**. Фиксируем какое-то $m \in \mathbb{N}$ и будем говорить, что $l, n \in \mathbb{Z}$ сравнимы по модулю m и писать $l \cong n(\mod m)$, если $l - n$ делится на m. Тогда $lRn \iff l \cong n(\mod m)$.

§ 2. Композиция отношений

1. Объединение и пересечение бинарных отношений. Одно из важнейших преимуществ отношений по сравнению с отображениями состоит в том, что применяя к отношениям любую теоретико множественную операцию, мы снова получаем отношение. В частности, для отношений (X, Y, R) и (X, Y, S) можно говорить об их объединении $(X, Y, R \cup S)$ и пересечении $(X, Y, R \cap S)$, которые обладают всеми обычными свойствами: ассоциативностью, коммутативностью, дистрибутивностью, и т.д.

2. Произведение бинарных отношений. Понятие композиции отображений непосредственно обобщается на бинарные отношения. Эту операцию впервые рассматривал А.де Морган, а потом детально изучил Э.Шредер. Обратите внимание, что R пишется справа от первого аргумента, что отвечало бы записи $(x)f$ для функций, и поэтому компонируемые отношения пишутся слева направо.

Определение. *Пусть* $R \in \mathrm{Rel}(X, Y)$, $S \in \mathrm{Rel}(Y, Z)$. **Произведение** $R \cdot S$ *отношений* R *и* S *это отношение* $R \cdot S \in \mathrm{Rel}(X, Z)$ *определяемое следующим образом:*

$$R \cdot S = \{(x, z) \in X \times Z \mid \exists y \in Y, (x, y) \in R, (y, z) \in S\}$$

Ясно, что в случае, когда R и S являются отображениями, так введенное произведение отношений лишь порядком отличается от определенной в § 2 композиции отображений, а именно, $R \cdot S = S \circ R$. Произведение отношений полностью аналогично композиции отображений, с той разницей, что первое отношение пишется **слева**, а не справа. Это связано с тем, что в отличие от отображений,

для которых обычно используется **префиксная** запись, когда знак отображения стоит **слева** от аргумента, для отношений используется инфиксная запись, когда знак отношения стоит **справа** от первого аргумента. Легко видеть, что тождественное отображение является нейтральным элементом для произведения отношений. Точнее, если $R \in \mathrm{Rel}(X, Y)$, то $\Delta_X \cdot R = R = R \cdot \Delta_Y$.

Теорема. *Произведение отношений ассоциативно: если* $R \in \mathrm{Rel}(X, Y)$, $S \in \mathrm{Rel}(Y, Z)$, $T \in \mathrm{Rel}(Z, W)$, *то*

$$(R \cdot S) \cdot T = R \cdot (S \cdot T).$$

Композиция дистрибутивна по отношению к объединению:

$$R \cdot (S \cup T) = (R \cdot S) \cup (R \cdot T), \qquad (R \cup S) \cdot T = (R \cdot T) \cup (S \cdot T),$$

В то же время дистрибутивность по отношению к пересечению, вообще говоря, не имеет места. Можно утверждать лишь, что

$$R \cdot (S \cap T) \subseteq (R \cdot S) \cap (R \cdot T), \qquad (R \cap S) \cdot T \subseteq (R \cdot T) \cap (S \cdot T),$$

Задача. Постарайтесь понять почему нарушается дистрибутивность и постройте контр-примеры!

Указание. В самом деле, пусть $(x, z) \in (R \cdot S) \cap (R \cdot T)$. Это значит, что найдется такое $u \in Y$, что $(x, u) \in R$, $(u, z) \in S$ и такое $v \in Y$, что $(x, v) \in R$, $(v, z) \in T$. Однако отсюда совершенно не обязано следовать, что найдется такое $y \in Y$, что $(x, y) \in R$ и $(y, z) \in S \cap T$.

§ 3. Симметричное отношение

Определение. *Отношение* $\Delta = \Delta_X = \{(x, x) \mid x \in X\}$ *называется* **диагональю** *декартова квадрата* X *или* **тождественным отношением** *на* x . *Любое внутреннее бинарное отношение* R *на* X, *содержащее* Δ, *называется* **рефлексивным**.

Иными словами, R рефлексивно, если $\forall x \in X$, xRx. Как мы знаем, отображения $f : X \longrightarrow Y$ очень редко обладают обратными. Однако сопоставление каждому элементу $y \in Y$ его полного прообраза $f^{-1}(y)$ по-прежнему принадлежит $\mathrm{Rel}(Y, X)$. Это наводит на мысль определить для любого бинарного отношения R обратное отношение аналогичным образом – как транспонирование R относительно биссектрисы первого квадранта. Следующая операция над отношениями была также введена А.де Морганом.

Определение. *Если* $R \in \mathrm{Rel}(X, Y)$, *то* **симметричное отношение** $R' \in \mathrm{Rel}(Y, X)$ *определяется посредством* $yR'x \iff xRy$.

Иными словами, если R состоит из пар (x, y), то R' состоит из пар (y, x). Симметричное к R отношение часто (совершенно справедливо!) называется также **транспонированным** или (безо всяких к тому оснований!) **обратным** к R и обозначается R^{-1}. В действительности, этот последний термин оправдан лишь для **биективных** отображений, где симметричное к R отношение действительно совпадает с обратным к R отображением. Ясно, что $(R')' = R$,

но, разумеется, в этом случае $R \cdot R'$ и $R' \cdot R$ может быть *гораздо* больше, чем Δ.

Легко видеть, что переход к симметричному отношению является гомоморфизмом по отношению к объединению и пересечению:

$$(R \cap S)' = R' \cap S', \qquad (R \cup S)' = R' \cup S'.$$

В то же время, по отношению к композиции это антигомоморфизм:

$$(R \cdot S)' = S' \cdot R'.$$

Обратите внимание на изменение порядка сомножителей!

$R \subseteq S \Longrightarrow R' \subseteq S'$.

Примеры симметричных отношений. Знак симметричного отношения получается отражением знака исходного отношения относительно вертикальной оси:

- $\geq \leq$
- $\subseteq \supseteq$
- $\in \ni$
- $| \vdots$

§ 4. Дополнительное отношение

1. Дополнительное отношение.

Определение. *Если* $R \in \mathrm{Rel}(X, Y)$, *то* **симметричное отношение** $\overline{R} \in \mathrm{Rel}(X, Y)$ *определяется посредством* $x\overline{R}y \iff \neg xRy$.

Иными словами, $(x, y) \in \overline{R}$ в том и только том случае, когда $(x, y) \notin R$. Переход к дополнительному отношению связан с объединением и пересечением **тождествами де Моргана**:

$$(\overline{R \cap S}) = \overline{R} \cup \overline{S}, \qquad (\overline{R \cup S}) = \overline{R} \cap \overline{S}.$$

2. Примеры дополнительных отношений. Знак дополнительного отношения получается перечеркиванием знака исходного отношения:

- $= \neq$
- $\in \notin$
- $\subseteq \not\subseteq$
- $\geq \not\geq$
- $| \not|$

Закон Шредера. $R' \cdot (\overline{R \cdot S}) \subseteq \overline{S}$. Иными словами, утверждается, что $R' \cdot (\overline{R \cdot S}) \cap S = \varnothing$. В самом деле, предположим, что это перечение $\neq \varnothing$. Тогда найдется пара $(x, z) \in R' \cdot (\overline{R \cdot S}) \cap S$. Тем самым, существует y такое, что $(x, y) \in R'$, $(y, z) \in \overline{R \cdot S}$. Но тогда $(y, x) \in R$ и, значит, $(y, z) \in R \cdot S$, противоречие.

§ 5. Основные классы бинарных отношений

If $A = B$ and $B = C$, then $A = C$, except where void or prohibited by law.

Roy Santoro

В дальнейшем основную роль будут играть следующие два типа внутренних бинарных отношений.

Определение. *Отношение* $R \in \mathrm{Rel}(X)$ *называется* **симметричным**, *если* $R = R^{-1}$, *и* **антисимметричным**, *если* $R \cap R^{-1} \subseteq \Delta$.

Таким образом, R симметрично, если $\forall x, y \in X$, $xRy \Longrightarrow yRx$, и антисимметрично, если $\forall x, y \in X$, $xRy \ \& \ yRx \Longrightarrow x = y$.

Любые внутренние бинарные отношения на одном и том же множестве можно скомпонировать, особенно интересны степени рефлексивных отношений. Дело в том, что в этом случае каждая последующая степень содержит предыдущую: $\Delta = R^0 \subseteq R \subseteq R \cdot R \subseteq \ldots$ – особенно важны отношения, для которых эта цепочка включений стабилизируется уже на втором шаге.

Определение. *Отношение* $R \in \mathrm{Rel}(X)$ *называется* **транзитивным**, *если* $R \cdot R \subseteq R$. *По определению произведения бинарных отношений это означает, в точности, что* $\forall x, y, z \in R$ $xRy \ \& \ yRz \Longrightarrow xRz$.

Внутреннее бинарное отношение называется **эквивалентностью**, если оно рефлексивно, транзитивно и симметрично, и **порядком**, если оно рефлексивно, транзитивно и антисимметрично, эти два типа отношений будут изучены в следующих параграфах.

Отношение $|x - y| < 1$ на множестве $\mathbb{R}$ рефлексивно и симметрично, но не транзитивно.

Отступление. В программировании знак = часто используется не как знак отношения, а как *оператор*, называемый на программистском жаргоне `Set`. Пусть x обозначает *переменную*; с точки зрения программиста, 'переменная' это просто *имя* некоторого ящика, коробки, сундука, контейнера, ячейки, регистра, ларца, футляра или шкатулки. Содержимое этой шкатулки называется текущим значением x. Запись $x = y$ не утверждает, что содержимое шкатулки x равно содержимому шкатулки y. Она предлагает присвоить переменной x *текущее значение* переменной y, т.е. *изготовить копию* содержимого шкатулки y и положить в шкатулку x, уничтожив при этом старое содержимое шкатулки x. Ясно, что $x = y$ и $y = x$ это совсем не одно и то же. Некоторые языки программирования отличают оператор = непосредственного присваивания `Set`, придающий переменной x текущее значение переменной y на момент появления этого оператора, от оператора := отложенного присваивания `SetDelayed`, который заново присваивает переменной x текущее значение переменной y при каждом обращении к переменной x.

§ 6. Многоместные отношения

Многоместные отношения. Понятие отношения естественно обобщается на любое конечное семейство множеств $X_1, \ldots, X_n$.

Определение. Отношением *между* $X_1, \ldots, X_n$ *называется любое подмножество их декартова произведения* $R \subseteq X_1 \times \ldots \times X_n$. *Если требуется явно указать число* n, *то говорят об* n*-арных или* n**-местных** *отношениях* (n *называется* **арностью** *отношения* R).

В случае, когда $X_1 = \ldots = X_n$ отношение R называется внутренним. Об отношениях арности > 2 говорят обычно как о **многоместных**. При этом отношения арности 3 называются **тернарными**, а отношения арности 4 – **кватернарными**. К сожалению, большинство математиков затрудняется столь же ловко обозвать соответствующие отношения в случае $n = 8$ или $n = 9$ – впрочем и делать это приходится достаточно редко. Мы не собираемся обсуждать здесь теорию многоместных отношений, а ограничимся несколькими примерами.

• **Отношение коллинеарности**. Здесь X - множество точек на плоскости и $(x, y, z) \in R$, если x, y, z лежат на одной прямой.

• **Отношение сравнимости**. Рассмотрим отношение $l \cong n(\mod m)$ как тернарное отношение с аргументами $l, m, n \in \mathbb{Z}$.

• **Отношение 'лежать между' в геометрии**. Здесь X – множество точек прямой и $(x, y, z) \in R$, если $y \in [x, z]$, где через $[x, z]$ обозначен отрезок прямой с концами x и z.

• **Отношение 'лежать между' в теории множеств**. Говорят, что множество B лежит между A и C, если $A \subseteq B \subseteq C$.

• **Отношение 'лежать между' в психологии**. Для стимулов A, B, C говорят, что B лежит между A и C, если $A \cap \mathrm{C} \subseteq B \subseteq A \cup \mathrm{C}$, пишем $A|B|C$.

Приведем теперь примеры кватернарных отношений.

• **Отношение компланарности**. Здесь X - множество точек трехмерного евклидова пространства и $(x, y, z, u) \in R$, если x, y, z, u лежат в одной плоскости.

Примеры 1) и 6) являются частными случаями более общего n-арного отношения 'линейной зависимости', которое будет подробно обсуждаться в Главах 3 и 4.

Следующий пример играет ключевую роль в Главе ? при определении 'равенства дробей'.

• **Отношение пропорциональности**. Пусть $a, b, c, d \in \mathbb{Z}$. Тогда

$$(a, b, c, d) \in R \quad \Longleftrightarrow \quad a/b = \mathrm{c}/d \quad \Longleftrightarrow \quad ad = bc.$$

В действительности, при попытке обобщить конструкцию дробей на кольца с 'делителями нуля' приходится рассматривать следующее отношение арности 5.

§ 7. Отношение эквивалентности

> Вскоре Максим с такой силой овладел философией марксизма, что мог без труда изобретать новые непреложные законы развития человеческого общества. Так, глядя на своего друга Федора, да и просто так, допивая вторую бутылку портвейна, Максим часто говорил: "Одинаковое одинаковому — рознь!"
>
> Владимир Шинкарев, 'Максим и Федор'.

Другой важнейший тип отношений – отношения эквивалентности.

Отношения эквивалентности.

Определение. Эквивалентностью *на множестве X называется рефлексивное симметричное транзитивное бинарное отношение R.*

Мы будем обозначать эквивалентность следующим образом: $xRy \iff x \sim y$ (читается 'x эквивалентно y'), но часто потребляются и другие символы: $\cong$, $\equiv$, $=$, и так далее (названия эквивалентностей, которые будут нам встречаться и, соответственно, чтения этих символов будут определяться контекстом). По определению,

a) $x \sim x$ (рефлексивность),

b) $x \sim y \Longrightarrow y \in x$ (симметричность),

c) $x \sim y \ \ \& \ \ y \sim z \Longrightarrow x \sim z$ (транзитивность).

Для каждого элемента $x \in X$ через $\overline{x}$ обозначается соответствующий **класс эквивалентности**, определяемый как множество всех $y \in X$ эквивалентных x: $\overline{x} = \{y \in X \mid y \sim x\}$. При этом сам элемент x называется **представителем** класса $\overline{x}$. Так как по определени. $\overline{x} = \overline{y} \iff x \sim y$, то $\overline{x}$ однозначно определяется любым своим представителем. Условия a) – c) могут быть переформулированы теперь следующим образом:

a) $x \in \overline{x}$;

b) $y \in \overline{x} \Longrightarrow x \in \overline{y}$;

c) $y \in \overline{x} \ \ \& \ \ z \in \overline{y} \Longrightarrow z \in \overline{x}$.

На любом множестве есть два очевидных отношения эквивалентности: **тождественное**, когда $x \sim y \Longrightarrow x = y$ и **универсальное**, когда $x \sim y$ для всех x, y. Напомним теперь несколько других примеров, которые нам встречались:

• **Эквивалентность (изоморфизм) множеств**. Рассмотрим какое-то множество X множеств, например, 2^Z для некоторого фиксированного Z. Тогда $A \sim B \iff |A| = |B| \iff$ существует биекция между A и B.

• **Ассоциированность**. Пусть $X = \mathbb{Z}$ и $m \sim n \iff m|n \ \ \& \ \ n|m$.

• **Сравнимость по модулю** m. Пусть $X = \mathbb{Z}$ и m – некоторое фиксированное натуральное число. Положим $x \sim y \iff x \equiv y \pmod m$ (напомним, что это означает, что $x - y$ делится на m).

• **Сравнимость по модулю** $\mathbb{Z}$. Пусть теперь $X = \mathbb{R}$. Будем говорить, что два вещественных числа сравнимы по модулю $\mathbb{Z}$, и писать $x \equiv y \pmod{\mathbb{Z}}$, если их дробные части совпадают. Напомним, что дробная часть $\mathrm{Frac}(x) \in [0, 1)$ числа $x \in \mathbb{R}$ – это разность $x - \mathrm{Ent}(x)$, где $\mathrm{Ent}(x)$ обозначает целую часть x, т.е. наибольшее целое n такое, что $n \leq x$. По определению, $x = \mathrm{Ent}(x) + \mathrm{Frac}(x)$. Таким образом, $x \equiv y \pmod{\mathbb{Z}} \iff \mathrm{Frac}(x) = \mathrm{Frac}(y)$.

Множество примеров отношений эквивалентности содержалось в элементарной геометрии. Помимо уже упоминавшихся конгруэнтности, подобия, параллельности, и т.д. можно привести следующие примеры.

• **Равенство длин.** Пусть X множество векторов на плоскости или в трехмерном пространстве. Будем говорить, что $x \sim y$, если длины векторов x и y совпадают.

• **Равенство площадей**. Пусть X – 'множество фигур' на плоскости. Будем считать, две фигуры A и B эквивалентны, если они имеют одинаковую площадь (либо если ни для одной из них площадь не определена).

Будет ли произведение двух отношений эквивалентности снова отношением эквивалентности? Следующая задача показывает, что далеко не всегда.

Задача. Пусть R, S – два отношения эквивалентности на множестве X. Докажите, что для того, чтобы $R \cdot S$ было отношением эквивалентности, необходимо и достаточно, чтобы $R \cdot S = S \cdot R$.

Решение. $\Longrightarrow$ Если $R \cdot S$ симметрично, то $R \cdot S = (R \cdot S)' = S' \cdot R' = S \cdot R$.

$\Longleftarrow$ Обратно, пусть $R \cdot S = S \cdot R$. Так как $\Delta \subseteq R, S$, то $\Delta = \Delta \cdot \Delta \subseteq R \cdot S$, так что $R \cdot S$ рефлексивно. Кроме того, $(R \cdot S)' = S' \cdot R' = S \cdot R = S \cdot S$, так что $R \cdot S$ симметрично. Наконец, $(R \cdot S) \cdot (R \cdot S) = (R \cdot R) \cdot (S \cdot S) = R \cdot S$, так что $R \cdot S$ транзитивно.

§ 8. Разбиения и фактор-множества

> На древних страницах китайской энциклопедии "Небесная империя благодетельных знаний" написано, что животные делятся на а) принадлежащих императору, б) набальзамированных, в) прирученных, г) сосунков, д) сирен, е) сказочных, ж) отдельных собак, з) включенных в эту классификацию, и) бегающих как сумасшедшие, к) бесчисленных, л) нарисованных тончайшей кистью из верблюжьей шерсти, м) прочих, н) разбивших цветочную вазу, о) похожих издали на мух.
>
> Хорхе Луис Борхес, Аналитический язык Джона Уилкинса (Собр. Соч., т.2, с.85)

Напомним, что **разбиением** множества X называется его представление как дизъюнктного объединения какого-то семейства подмножеств: $X = \coprod X_i$, $i \in I$ (см. § 1). Понятие разбиения по сути совпадает с понятием эквивалентности. А именно, каждому разбиению можно сопоставить отношение эквивалентности, для которого $x \sim y$ тогда и только тогда, когда $x, y \in X_i$ для некоторого i.

Обратно, следующее предложение показывает, что каждая эквивалентность на X задает разбиение X на попарно различные классы. Для этого выберем из каждого класса X_i по одному представителю x_i, где i пробегает некоторое множество индексов I, и назовем $\{x_i, i \in I\}$ **системой представителей** (Vertretersystem, Repräsentantensystem) эквивалентности $\sim$ (или **трансверсалью** к этой эквивалентности).

Аксиома выбора. *Для каждого отношения эквивалентности существует трансверсаль.*

Предложение. *Множество классов эквивалентности является разбиением X. Иными словами, X представляется в виде дизъюнктного обьединения $X = \coprod X_i$, $i \in I$, различных классов.*

Доказательство. Прежде всего, заметим, что $X = \cup X_i$, $i \in I$. В самом деле, так как мы выбрали по одному x_i из каждого класса, то для любого $x \in X$ найдется x_i такой, что $x \sim x_i$, но тогда по свойству a) имеем $x \in \overline{x} = \overline{x}_i$.

Осталось заметить, что два различных класса не могут пересекаться. В самом деле, если $\overline{x} \cap \overline{y} \neq \varnothing$, то найдется $z \in \overline{x} \cap \overline{y}$, но тогда по свойству b) также $y \in \overline{z}$ и теперь по свойству c) мы можем заключить, что $y \in \overline{x}$, так что, окончательно, $\overline{y} = \overline{x}$, что и требовалось доказать.

Различные аватары следующей конструкции будут сопровождать нас на протяжении всего курса.

Определение. *Множество $X/\!\sim = \{\overline{x} \mid x \in X\}$ классов эквивалентности $\sim$ на множестве X называется* **фактор-множеством** *X по отношению $\sim$, а отображение* $\mathrm{pr} : X \longrightarrow X/\!\sim$, $x \mapsto \overline{x}$, *называется* **канонической проекцией** *X на $X/\!\sim$.*

Замечание. Это определение представляется полной тривиальностью, но на самом деле подлинный вопрос состоит в том, в какой степени $X/\!\sim$ наследует различные имеющиеся на X структуры? Например, если $\sim$ эквивалентность на чуме X, то на фактор-множестве

$X/\sim$ нельзя, вообще говоря, ввести структуру чума так, чтобы естественная проекция pr была изотонной. Первая естественная мысль состоит в том, чтобы для двух классов $\overline{x}$, $\overline{y}$ положить $\overline{x} > \overline{y}$ в том и только том случае, когда $x > y$ для некоторых представителей x, y этих классов. Однако это определение **некорректно**, в том смысле, что оно, вообще говоря, **зависит от выбора представителей** (т.е. для другой пары представителей возможно выполнение обратного неравенства $x < y$ или несравнимость x и y). Конечно, в данном случае легко сформулировать условие, которому должна удовлетворять эквивалентность $\sim$, чтобы такое определение стало корректным. Несложно гарантировать и перенос на $X/\sim$ основных *алгебраических* структур (см. понятие конгруэнции в § 1.3). Но для многих *геометрических* структур задание соответствующей структуры на фактор-множестве часто превращается в достаточно драматическую проблему.

§ 9. Факторизация отображений

– слои отображения

1. Факторизация отображений. Обычный способ задания разбиений множества X состоит в следующем. Пусть нам задано отображение $f : X \longrightarrow Y$ множества X в какое-то множество Y. Введем на X следующее отношение эквивалентности $\sim$: $x \sim y \Longleftrightarrow f(x) = f(y)$. Ядро отображения. Классы этой эквивалентности (полные прообразы точек из Y относительно отображения f) называются **слоями** отображения f и, как мы знаем, X представляется как дизъюнктное обьединение слоев $f^{-1}(y)$, $y \in \mathrm{Im}(f)$. Пусть, как обычно, $X/\sim$ обозначает множество слоев (фактор-множество X по отношению эквивалентности $\sim$. Тогда можно определить отображение $\overline{f} : X/\sim \longrightarrow Y$ полагая $\overline{f}(\overline{x}) = f(x)$. Это определение корректно, т.е. не зависит от выбора представителя x из данного класса, так как отображение постоянно на своих слоях. Отображение f включается в следующий **коммутативный треугольник**:

triangle

'Коммутативность' в этом контексте означает, x то $f = \overline{f} \circ \mathrm{pr}$ (см. § ? по поводу общего определения коммутативных диаграмм). Резюмируем получившийся результат.

Предложение. *Любое отображение представляется как композиция сюръективного и инъективного отображений.*

Доказательство. По самому построению фактор-множеств каноническая проекция сюръективна: $\mathrm{pr}(X) = Y$. Осталось проверить лишь, что f инъективно. В самом деле, если $f(x) = f(y)$ для некоторых классов $\overline{x}$ и $\overline{y}$, то по определению f тогда $f(x) = f(y)$ для представителей этих классов. Но это и означает, что x y, так что, окончательно, $\overline{x} = \overline{y}$.

§ 10. Схемы и диаграммы Юнга

Схемы и диаграммы Юнга. Особенно большую роль во многих разделах математики и физики играют отношения эквивалентности на конечных множествах и в этом пункте мы опишем классический прием визуализации таких отношений.

В этом пункте X будет обозначать n-элементное множество, в качестве которого обычно берут множество первых n натуральных чисел $I = \{1, \ldots, n\}$. Мы будем рассматривать отношения эквивалентности на I или, что то же самое, разбиения множества I. Пусть $I = \cup X_i$ – какое-то разбиение I на дизъюнктные подмножества $X_1, \ldots, X_t$. Ясно, что с точностью до изоморфизма (т.е. с точностью до перестановки элементов I, см. § ?) отношение эквивалентности полностью определяется порядками своих классов. В частности, можно считать, что

каждый из классов X состоит из последовательных натуральных чисел, и, таким образом, если $n_m = |X_m|$ обозначает порядок m-го класса, то $i \in X_m$ в том и только том случае, когда выполняются неравенства $n_1 + \ldots + n_{m-1} + 1 \leq i \leq n_1 + \ldots + n_m$.

В частности, n представляется в виде $n = n_1 + \ldots + n_t$. Любой набор натуральных чисел $\nu = (n_1, \ldots, n_t)$ называется разбиением числа n. В действительности, так как мы пока интересуемся лишь описанием отношений эквивалентности с точностью до изоморфизма, можно даже считать, что ν – неубывающее разбиение, т.е. что $n_1 \geq n_2 \geq \ldots \geq n_t$ (во многих книгах рассматриваются только разбиения удовлетворяющие этому дополнительному ограничению). Такие разбиения нагляднее всего представляются графически посредством схем или таблиц Юнга. Схема Юнга изображающая неубывающее разбиение ν представляет собой таблицу, содержащую n клеток, расположенных следующим образом: первая строка этой таблицы содержит n_1 клеток, вторая – n_2, и так далее вплоть до последней строки с номером t, которая содержит n_t клеток. В качестве примера изобразим схему Юнга представляющую разбиение $(6, 4, 4, 2, 1)$ числа 17:

$$bla - bla$$

Напомним, что строки этой таблицы кодируют информацию о порядках классов эквивалентности n. Например, схема Юнга универсального отношения (n) состоит из одной строки, а схема Юнга тождественного отношения $(1, \ldots, 1)$ – из n строк, в каждой из которых стоит по одной клетке, т.е. из одного столбца.

На схемах Юнга можно вводить различные отношения порядка, получая таким образом интересные примеры частично упорядоченных множеств. Проиллюстрируем, в частности, примеры 10 и 11, о которых шла речь в предыдущем параграфе. Обычный порядок на множестве схем Юнга с n клетками – это лексикографический порядок: из двух схем та больше, у которой больше клеток в первой строке, или, если в первой строке у них одинаковое количество клеток, та, у которой больше клеток во второй строке и так далее. Получающийся таким образом порядок линеен.

На множестве всех схем Юнга (т.е., по существу, всех неубывающих разбиений всевозможных натуральных чисел) часто рассматривается и другой порядок, частичный. При этом считают, что схема A меньше схемы B, если A можно вложить в B. Относительно этого порядка уже нельзя сказать, что $(n) > (1, \ldots, 1)$. Ниже приводится пример вложения схемы $(4, 4, 2, 1, 1)$ в схему $(5, 4, 4, 3, 2)$ (для наглядности клетки меньшей схемы заштрихованы):

$$bla - bla$$

Фактически отношение эквивалентности с данным типом разбиения на классы $\nu = (n_1, \ldots, n_t)$ получается расстановкой чисел от 1 до n в клетки схемы Юнга формы ν (в разных клетках стоят разные числа!). Схема Юнга, в заполненными таким образом клетками называется диаграммой Юнга. Имеется $n!$ различных диаграмм Юнга отвечающих каждой схеме Юнга с n клетками. Ниже приводится пример диаграммы Юнга типа $(4, 3, 2, 2)$:

$$bla - bla$$

Разумеется, одно и то же отношение эквивалентности может задаваться различными диаграммами Юнга. Например, без потери общности можно считать, что диаграмма стандартна по строкам, т.е. в каждой строке числа расположены в порядке возрастания. Кроме того, можно переставлять между собой строки (не меняя формы диаграммы).

В действительности диаграммы Юнга, различные их варианты и обобщения служат мощным инструментом в классификации представлений некоторых важнейших групп, описании симметрии тензоров и во многих других интересных комбинаторных задачах.

§ 11. Отношения порядка

Нам будут чрезвычайно часто встречаться отношения, обобщающие отношение неравенства '$\leq$' и отношение включения '$\subseteq$'.

1. Частично упорядоченные множества.

Определение. Порядком *на множестве X называется рефлексивное, антисимметричное транзитивное бинарное отношение R.*

Порядок обычно обозначается следующим образом: $xRy \iff x \leq y$ (читается 'меньше или равно', 'не больше', 'предшествует', 'минорирует'). По определению,

a) $x \leq x$ (рефлексивность),

b) $x \leq y \ \ \& \ \ y \leq x \Longrightarrow x = y$ (антисимметричность),

c) $x \leq y \ \ \& \ \ y \leq z \Longrightarrow x \leq z$ (транзитивность).

Отношение R^{-1}, обратное к R, обычно записывается $x \geq y$ (читается 'больше или равно', 'не меньше', 'следует', 'мажорирует'). Таким образом, $x \geq y \iff y \leq x$. Отношение $R \setminus \Delta$ записывается $x < y$ (читается 'меньше', 'строго меньше', 'строго предшествует', 'строго минорирует'). Иными словами, $x < y \iff x \leq y \ \ \& \ \ x \neq y$. Аналогичный смысл имеет $x > y$ ('больше', 'строго больше', 'строго следует', 'строго мажорирует').

2. Линейный порядок. Часто введенное выше понятие называется **частичным порядком**, чтобы подчеркнуть, что не любые два элемента множества X сравнимы относительно $<$. При этом два элемента X и Y называются **сравнимыми**, если $x < y \vee y < x$. В противном случае X и Y называют **несравнимыми**, и пишут $x \parallel y$. Само множество X, на котором задан частичный порядок называется **частично упорядоченным множеством** или, сокращенно, **чумом** (по аналогии с 'poset' от 'partially ordered set'). Следующее определение ввел Кантор в 1895 году[229].

Определение. *Порядок R на X называется* **линейным**, *если $R \cup R' = X \times X$, иными словами, если любые два элемента X сравнимы.*

Множество X, на котором задан линейный порядок, называется **линейно упорядоченным множеством** или **цепью**.

Теорема Шпильрайна. *Всякое упорядоченное множество вкладывается в линейно упорядоченное множество.*

Для конечного множества это очевидно. Достаточно упорядочить элементы по высоте, а потом произвольным образом внутри высоты. Для бесконечных множеств это аксиома выбора.

3. Первые примеры. Приведем теперь очевидные примеры порядка.

• Обычное отношение $<$ порядка на $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ задает там линейный порядок.

• Множество $X = 2^Y$ упорядочено по включению $\subseteq$. Если $|Z| \geq 2$, этот порядок не является линейным. Например, если $Z = \{a, b\}$, то множества $\{a\}$ и $\{b\}$ несравнимы.

• Множество $\mathbb{N}$ упорядочено относительно делимости $|$. В самом деле, a) $\forall n \in \mathbb{N}$, $n|n$; b) $\forall m, n \in \mathbb{N}$, $m|n \ \ \& \ \ n|m \Longrightarrow m = n$; c) $\forall l, m, n \in \mathbb{N}$, $l|m \ \ \& \ \ m|n \Longrightarrow l|n$.

• В то же время на множестве $\mathbb{Z}$ делимость не является порядком, так как здесь не имеет места антисимметричность: если для двух целых чисел m и n имеем $m|n$ и $n|m$, то можно умозаключить лишь, что $m = \pm n$.

[229] G.Cantor, Beiträge zer Begründung der transfiniten Mengenlehre. – Math. Ann., 1895, Bd.46, S.481–512.

Примеры 3) и 4) будут играть для нас ключевую роль в следующей главе. Пример 4) показывает, что, вообще говоря, отношение делимости задает на кольце лишь **предпорядок** (так называются рефлексивные транзитивные, но не обязательно антисимметричные отношения), а чтобы получить настоящий порядок, нужно перейти к классам ассоциированных элементов.

• Множество всех людей упорядочено относительно отношения $a < b \iff a$ потомок b.

• Большинство естественных алфавитов, например, русский {а,б,в,. . . ,я}, латинский {a,b,c,. . . ,z} или греческий $\{\alpha, \beta, \gamma, \ldots, \omega\}$, упорядочен обычным образом. Именно этот порядок позволяет искать слова в словаре. На самом деле алфавит содержит еще один важнейший знак – пробел ('space') , обозначаемый обычно в руководствах по программированию через ??. Как легко убедиться, рассматривая первую страницу любого словаря, пробел предшествует любой другой букве, но при этом слово не может начинаться с пробела.

• Для каждого порядка на X можно определить двойственный порядок, для которого x предшествует y в том и только том случае, когда x следует за y в исходном порядке. Мы будем обозначать множество X с таким порядком через X^*. При этом каждому утверждению, соответствует **двойственное** (alias **дуальное**) утверждение, в котором '$>$' заменено на '$<$'.

• Многие другие множества традиционно снабжаются некоторым фиксированным линейным порядком: множество нот {до, ре, ми, фа, соль, ля, си}, множество цветов радуги {красный, оранжевый, желтый, зеленый, голубой, синий, фиолетовый}, В действительности, как мы узнаем в § ?, на множестве из n элементов можно ввести $n!$ различных линейных порядков. Например, множество нот и множество цветов радуги могут быть линейно упорядочены $7! = 5040$ различными способами.

• чум X , в котором любые два различных элемента несравнимы, называется **антицепью**. Для антицепи $x \leq y \iff x = y$.

• Пусть X – частично упорядоченное мноджество, а Y – произвольное множество. Множество X^Y вещественных функций упорядочено отношением $f \leq g$ в том и только том случае, когда $f(x) \leq g(x)$ для всех $x \in X$

• Пусть Z – частично упорядоченное множество. Тогда его булеан 2^Z можно упорядочить следующим отношением $X \leq Y$ в том и только том случае, когда $\forall x \in X$, $\forall y \in Y$, $x \leq y$.

• усть Z – частично упорядоченное множество. Тогда его булеан 2^Z можно упорядочить также и следующим отношением $X \leq Y$ в том и только том случае, когда $\exists y \in Y$, $\forall x \in X$, $x \leq y$.

§ 12. Прямое произведение чумов

> "Три упорядочения" означают: упорядочение организации, упорядочение в идеологическом отношении и упорядочение стиля.
>
> Председатель Мао Цзе-дун, "Демократическое движение в армии" (30 января 1948 года)

Пусть теперь X и Y - два упорядоченных множества. Имеется два очевидных способа ввести порядок на $X \times Y$, которые, однако, приводят к различным результатам.

• **Лексикографический порядок**. Положим $(x_1, y_1) \leq (x_2, y_2) \iff x_1 \leq x_2 \vee (x_1 = x_2 \ \& \ y_1 \leq y_2)$. Получившийся порядок будет линеен, если порядок на X и Y линейны. Например, $(3, 4) < (4, 3)$. Заметим, что в этом определении мы неявно используем обычный порядок на множестве индексов $\{1, 2\}$.

• **Покомпонентный порядок**. Положим теперь $(x_1, y_1) \leq (x_2, y_2) \iff x_1 \leq x_2 \ \& \ y_1 \leq y_2$. При этом получившийся порядок не будет линейным даже если порядки на X и Y линейны. Например, если $X = Y = \mathbb{Z}$ с обычным порядком, то теперь в отличие от предыдущего примера $(3, 4)$ и $(4, 3)$ несравнимы. Множество $X \times Y$, снабженное таким порядком, называется **прямым произведением** чумов X и Y.

Комментарий. Эти примеры легко обобщаются на случай любого конечного числа сомножителей. Например, в определении обычного лексикографического порядка, используемого при составлении словарей, буквы, составляющие слово, нумеруются начиная с первой в возрастающем порядке: $1 < 2 < 3 < \ldots$. При рассмотрении нескольких чумов очень важно четко понимать, что именно мы дуализируем. Так, например, порядок в так называемых **обратных словарях** (используемых, например, поэтами и составителями кроссвордов), в которых слова располагаются в порядке возрастания их последних букв, отвечает обычному порядку алфавита, но инвертированному, по сравнению с определением ?), порядку индексов, которые теперь располагаются в порядке убывания: $-1 > -2 > -3 > \ldots$. (здесь -1 отвечает последней букве, -2 – предпоследней, и т.д.). Получающийся таким образом порядок на множестве слов вовсе не является двойственным к обычному лексикографическому порядку.

§ 13. Диаграмма Хассе

Множество X называется **плотным**, если между любыми двумя его различными сравнимыми элементами можно вставить еще один: $\forall x, y \in X, \ X < y \implies \exists z \in X, \ x < z < y$.

Упражнение. Если X – плотное частично упорядоченное множество, то для любых $x, y \in X$, $x < y$ существует бесконечно много таких $z \in X$, что $x < z < y$.

Упражнение. Множество X в том и только том случае плотно, когда ни у одного его элемента нет непосредственно предшествующего (или непосредственно следующего).

§ 13. Диаграмма Хассе

Диаграмма частично упорядоченного множества. Попробуем задать порядок '$\leq$' наиболее экономичным образом. Так как $x \leq x$, мы можем в дальнейшем обсуждать только строгое неравенство '$<$'. Говорят, что y лежит строго между x и z, если $x < y < z$. В силу транзитивности неравенство $x < z$ будет тогда вытекать из неравенств $x < y$ и $y < z$. Это мотивирует следующее определение.

Определение. *Говорят, что* y **непосредственно следует** *за* x *, если* $y > x$ *и не существует элементов, лежащих строго между* x *и* y.

Иными словами, это значит, что $y > x$ и $\forall z, \ y > z > x \implies z = y \vee z = x$. В этом случае говорят также, что y **покрывает** x, или двойственным образом, что x **непосредственно предшествует** y или что x **покрывается** y.

В общем случае элементы непосредственно следующие за каким-либо элементом не обязаны существовать. Например, для обычного порядка на $\mathbb{Q}$ ни

для одного рационального числа не существует ни непосредственно следующего ни непосредственно предшествующего (пусть $x < y$, тогда $(x + y)/2$ лежит строго между y и x). В то же время для многих важных случаев отношение '$<$' будет целиком определяться отношением непосредственного следования. Это так, например, для конечных множеств.

Диаграмма (или, точнее, **диаграмма Хассе**) конечного частично упорядоченного множества X изображается следующим образом. Ее вершины отвечают элементам множества x . Две вершины x и y соединяются стрелкой, направленной от x к y, если y покрывает x. Часто стрелка не ставится, а между x и y рисуется ребро, но y располагается выше x. Приведем в качестве примера диаграмму Хассе множества $2^{\{x,y,z\}}$:

§ 14. Мажорирование и минорирование

Мажорирование и минорирование. Пусть X – чум и $Y \subseteq X$. Говорят, что $x \in X$ **мажорирует** Y (или что x является **мажорантой** или **верхней гранью** Y), если $\forall y \in Y$, $x \geq y$. Понятие **минорирования** (и **миноранты** alias **нижней грани**) определяется двойственным образом. Для подмножества $Y \subseteq X$ верхняя и нижняя грани не обязаны существовать (см. курс анализа, где говорится об 'ограниченных' подмножествах в $\mathbb{R}$).

Элемент x называется **наибольшим** элементом множества X, если x – верхняя грань самого X, т.е., иными словами, $x \geq y$ для любого $y \in X$. Аналогично определяется понятие **наименьшего** элемента. Наибольший (наименьший) элемент может и не существовать, но если он существует, то непременно ровно один (в силу антисимметричности).

Понятие наибольшего элемента не следует путать с понятием максимального элемента. А именно, элемент $x \in X$ называется **максимальным**, если он не мажорируется никаким другим элементом, иными словами, если $\forall y \in X$, $y \geq x \Longrightarrow y = x$. Однако то, что x не мажорируется никаким другим элементом, отнюдь не означает, что сам x мажорирует все другие элементы – он может быть не сравним с ними. Двойственным образом определяется понятие **минимального** элемента. В X может существовать много максимальных (минимальных) элементов. Более того, даже если в X существует единственный максимальный (минимальный), это совершенно не означает, что X имеет наибольший (наименьший) элемент.

• Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ относительно обычного порядка не имеют ни наибольшего, ни наименьшего элемента. В тех случаях, когда это необходимо, положение исправляется следующим образом. К каждому из этих множеств X присоединяются два новых элемента, обозначаемых ∞ и $-\infty$, так что ∞ является наибольшим элементом множества $X \cup \{\pm\infty\}$, а $-\infty$ – наименьшим: $-\infty < x\infty$ для любого $x \in X$.

• Все элементы антицепи X являются одновременно как максимальными, так и минимальными элементами, но если $|X| \geq 2$, то ни наибольшего, ни наименьшего элемента там нет. Если присоединить к $\mathbb{Z}$ элемент $*$ не сравнимый ни с одним целым числом, то получившееся множество $X = \mathbb{Z} \cup \{*\}$ имеет единственный максимальный и единственный минимальный элемент $\{*\}$, но не содержит ни наибольшего, ни наименьшего элемента.

• Рассмотрим множество X непустых собственных подмножеств некоторого множества Z. Тогда минимальными элементами X будут одноэлементные

подмножества, а максимальными элементами – такие подмножества, дополнение которых одноэлементно, при этом наибольшего и наименьшего элемента в X нет. Разумеется, в множестве 2^Z есть как наибольший элемент Z, так и наименьший элемент $\varnothing$.

• В множестве $\mathbb{N}$ натуральных чисел относительно деления есть наименьший элемент 1, но не существует максимальных элементов. (Как мы увидим в следующей главе, в более глубоком смысле 1 является наибольшим элементом, и наоборот, число тем меньше, т.е. тем ближе к 0, чем у него больше делителей).

Пусть снова $Y \subseteq X$. Если множество всех мажорант Y имеет наименьший элемент, то он называется **точной верхней гранью** или **супремумом** множества Y и обозначается $\vee Y$ или $\sup(Y)$. Супремум не обязан существовать, а если он существует, то не обязан принадлежать Y, хотя может ему и принадлежать. Если $x = \sup(Y)$, то по определению $\forall y \in Y$, $x \geq y$, и если для некоторого z выполнено $\forall y \in Y$, $z \geq y$, то $z \geq x$. Аналогично, наибольший элемент множества всех минорант Y называется **точной нижней гранью** или **инфимумом** множества Y и обозначается $\wedge Y$ или $\inf(Y)$ и к нему относятся все замечания, высказанные в отношении супремума.

§ 15. Решетки

Особенно важны чумы, в которых существует супремум и инфимум любого двухэлементного подмножества $\{x, y\}$, обозначаемые в этом случае $x \vee y = \sup(x, y)$ и $x \wedge y = \inf(x, y)$, соответственно. Такие чумы обычно называются **структурами** или **решетками**. Операции взятия супремума и инфимума обладают следующими свойствами:

i) коммутативность $x \vee y = y \vee x$, $x \wedge y = y \wedge x$,

ii) ассоциативность: $(x \vee y) \vee z = x \vee (y \vee z)$, $(x \wedge y) \wedge z = x \wedge (y \wedge z)$,

iii) идемпотентность: $x \vee x = x$, $x \wedge x = x$.

Легко видеть, что в действительности в решетках существуют супремумы и инфимумы любых конечных множеств. Для этого достаточно заметить, что sup и inf можно индуктивно определить следующими формулами:

$$x_1 \vee \ldots \vee x_n = (x_1 \vee \ldots \vee x_{n-1}) \vee x_n, \qquad x_1 \wedge \ldots \wedge x_n = (x_1 \wedge \ldots \wedge x_{n-1}) \wedge x_n,$$

Приведем несколько очевидных примеров решеток.

• В любом чуме выполнено **условие поглощения** $x \leq y \iff x = x \wedge y \iff y = x \vee y$. Поэтому любая цепь является решеткой.

• Множество $X = 2^Z$ всех подмножеств множества Z является решеткой, в которой $x \vee y = x \cup y$ и $x \wedge y = x \cap y$ (теоретико-множественное объединение и пересечение). В действительности так как объединения и пересечения определены для любых – в том числе и бесконечных – семейств подмножеств, это **полная решетка** (так называются чумы, в которых любое подмножество имеет супремум и инфимум).

• Множество натуральных чисел $\mathbb{N}$ относительно делимости является решеткой, в которой $x \vee y = \mathrm{lcm}(x, y)$ (наименьшее общее кратное), а $x \wedge y = \gcd(x, y)$ (наибольший общий делитель).

Как показывает пример $X = \mathbb{Z}$, решетка не обязана содержать максимальные и минимальные элементы. Однако если максимальный элемент существует, то в силу условия поглощения он обязан быть наибольшим элементом, называемым также **единицей** решетки и обозначаемым 1. Аналогично, любой минимальный элемент является в действительности наименьшим, называемым также **нулем** решетки и обозначаемым 0. Согласно определению $x \vee 1 = 1$, $x \wedge 1 = x$ и, аналогично, $x \vee 0 = x$, $x \wedge 0 = 0$.

§ 16. Монотонные отображения

Морфизмы частично упорядоченных множеств. Число различных порядков, которые можно ввести на данном множестве растет невероятно быстро. Обозначим через $G^*(n)$ число различных способов, которыми можно ввести на n-элементом множестве частичный порядок. Тогда $G^*(1) = 1$, $G^*(2) = 3$, $G^*(3) = 19$, $G^*(4) = 219$, $G^*(5) = 4231$, $G^*(6) = 130023$, $G^*(7) = 6129859$.

Упражнение. Верно ли, что $G^*(n)$ всегда нечетно? (см. Г.Биркгоф, "Теория решеток", М., 1984, Гл.I, §§ 1–2)

Однако каково число 'существенно различных' способов упорядочить множество X? Для этого нам нужно определить, когда два чума можно считать 'одинаковыми'.

Определение. *Отображение $f : X \longrightarrow Y$ одного чума в другой называется* **изотонным**, *если для любых $x, y \in X$ неравенство $x \leq y$ влечет соответствующее неравенство для образов $f(x) \leq f(y)$. Изотонные отображения называются иначе* **сохраняющими порядок**, **возрастающими** *или* **морфизмами** *чумов.*

Заметим, что в этом определении не предполагается, что f инъективно. Иначе говоря, для двух элементов $x, y \in X$, связанных строгим неравенством $x < y$ их образы могут совпадать $f(x) = f(y)$. Инъективное изотонное отображение называется **строго изотонным** или **строго возрастающим**.

Биективное изотонное отображение называется **изоморфизмом** чумов, два чума называются **изоморфными**, если между ними существует изоморфизм. Например, любые два конечных линейно упорядоченных множества одного и того же порядка изоморфны, а множество $2^{\{0,1\}}$ изоморфно множеству натуральных делителей числа 6.

Обозначим через $G(n)$ число различных порядков, которые можно ввести на n-элементном множестве, рассматриваемых с точностью до изоморфизма. Тогда $G(1) = 1$, $G(2) = 2$, $G(3) = 5$, $G(4) = 16$, $G(5) = 63$, $G(6) = 318$. Эти значения гораздо меньше, чем соответствующие значения $G(n)$, но также довольно быстро растут.

Кроме отображений, сохраняющих порядок, часто рассматривают и отображения, **обращающие порядок**, называемые также **антиизотонными** или **убывающими**. А именно, для такого отображения а неравенство $x \leq y$ влечет обратное неравенство для образов $f(x) \geq f(y)$. В действительности, антиизотонные отображения из X в Y можно рассматривать просто как изотонные отображения двойственного множества X в Y (или как отображения X в двойственное Y). Ясно, какой смысл следует приписать словам **строго антиизотонное** или **строго убывающее** отображение. Изотонные и антиизотонные

отображения обьединяются под общим именем **монотонных**, а инъективное монотонное отображение называется **строго монотонным**.

Задача. Путь X, Y два частично упорядоченнных множества порядков m и n, соответственно. Доказать, что количество строго возрастающих отображений из X в Y равно $\binom{n}{m}$.

Глава 7. ПОРЯДКОВЫЕ ТИПЫ

Циньский царь Му-гун сказал Болэ:
— Вы уже в преклонных годах. Есть ли у вас в семье кто-нибудь, кого я мог бы послать на розыски коня?
— Хорошего коня можно опознать по его стати и взгляду, костям и мускулам, — ответил Болэ. — Но лучший конь Поднебесного мира как бы невиден, как бы неуловим, как бы не существует, как бы пропал. Такой конь не поднимает пыли и не оставляет следов. У сыновей вашего слуги способности небольшие. Они могут узнать хорошего коня, но не лучшего коня Поднебесной. Но я знаю человека, который разбирается в конях не хуже меня. Он носит овощи и собирает хворост для меня. Его зовут Цзюфан Гао. Прошу вас призвать его к себе.
Му-гун призвал этого человека к себе и послал его на розыски коня. Спустя три месяца он вернулся и снова предстал перед царем.
— Я нашел то, что нужно, в Песчаных Холмах.
— Что это за конь?
— Кобыла, каурая.
Царь велел привести кобылу, и она оказалась вороным жеребцом. Му-гун сильно опечалился и призвал к себе Болэ.
— Оказывается, тот, кого мы послали отбирать коней, ни на что не годен. Он не умеет даже отличить кобылу от жеребца и не разбирает масти! Что он может знать про лошадей!
Тут Болэ восхищенно вздохнул:
— Так вот, значит, чего он достиг! Как раз поэтому он стоит тысячи, десяти тысяч, всех в мире знатоков, подобных мне. Такие люди, как Гао, прозревают Небесный исток жизни, они схватывают суть и забывают о ненужном, пребывают во внутреннем и отрешаются от внешнего. Он видит то, на что хочет смотреть, и не замечает того, на что смотреть не нужно. Такие, как он, в лошадях видят нечто куда более важное, чем лошадь.

Ле-цзы, Гл. VIII. Рассказы о совпадениях

§ 16. Порядковые типы

Порядковые типы. Класс изоморфизма частично упорядоченных множеств называется порядковым типом.

Теорема Кантора. *каждое счетное линейно упорядоченное множество изоморфно подмножеству* $\mathbb{Q}$.

§ 16. Арифметика порядковых типов

Сложение порядковых типов. Пусть X – множество порядкового типа α, а Y – множество порядкового типа β. Упорядочим множество $X \sqcup Y$ следующим образом: ограничение порядка на X и на Y совпадает с исходным порядком на этих множествах и $x < y$ для любых $x \in X$, $y \in Y$. Тогда порядковый тип множества $X \sqcup Y$ зависит только α и β и обозначается $\alpha + \beta$.

Сложение порядковых типов ассоциативно: $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ Самое поразительное свойство сложения порядковых типов состоит в том, что сложение некоммутативно. Например, легко видеть, что для любого конечного n имеем $n + \omega = \omega \neq \omega + n$, так как в множестве типа $\omega + n$ есть наибольший элемент, а в множестве типа ω – нет. Поэтому слагаемые в $\alpha + \beta$ имеют разные названия, α называется angendus, а β – addendus.

Задача. Докажите, что $1+\omega^* \neq \omega^*+1=\omega^*$ и $\omega+\omega^* \neq \omega^*+\omega$. Постройте подмножества в $\mathbb{Q}$, упорядоченные по типу $\omega+\omega^*$ и по типу $\omega^*+\omega$.

Ответ. В качестве примера множества, упорядоченного по типу $\omega^*+\omega$ естественно взять $\mathbb{Z}$. С другой стороны, в качестве множества типа $\omega+\omega^*$ можно взять, например,

$$\{-1<-\frac{1}{2}<\ldots<-\frac{1}{n}<\ldots<\frac{1}{n}<\ldots<\frac{1}{2}<1\}.$$

В этом множестве есть как наибольший, так и наименьший элемент, в то время как в множестве $\mathbb{Z}$ нет.

Умножение порядковых типов. Пусть X – множество порядкового типа α, а Y – множество порядкового типа β. Упорядочим множество $X\times Y$ лексикографически. Тогда порядковый тип множества $X\times Y$ зависит только α и β и обозначается $\alpha\beta$. Умножение порядковых типов ассоциативно: $(\alpha\beta)\gamma=\alpha(\beta\gamma)$. Отсутствие коммутативности теперь уже не должно вызвать у нас никакого удивления. Например, ясно, что для любого конечного n имеем $n\omega=\omega\neq\omega n=\omega+\ldots+\omega$. Умножение дистрибутивно относительно сложения слева, $\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma$, но, вообще говоря, не справа, $(\alpha+\beta)\gamma\neq\alpha\gamma+\beta\gamma$. В самом деле, $\omega=2\omega=(1+1)\omega\neq 1\omega+1\omega=\omega+\omega$.

Задача. Докажите, что и $\omega\omega^*\neq\omega^*\omega$.

Указание. Посмотрите на нижние конусы элементов в этих множествах.

Теперь у нас все готово, чтобы начать снова учиться арифметике. Мы уже знаем, что $\omega(\omega+n)=\omega^2+\omega n$ для любого натурального n. Сейчас мы увидим нечто более витиеватое.

Задача. Убедитесь, что $(\omega+m)\omega=\omega^2$ и $(\omega+m)(\omega+n)=\omega^2+\omega n+m$ для любых натуральных m,n.

Удивительное рядом: Докажите, что сложение и умножение порядковых типов следующим образом ведут себя по отношению к двойственности:

$$(\alpha+\beta)^*=\beta^*+\alpha^*,\qquad (\alpha\beta)^*=\alpha^*\beta^*.$$

Потенцирование порядковых типов.

§ 16. Вполне упорядоченные множества

Линейно упорядоченное множество X называется **вполне упорядоченным**, если в любом непустом подмножестве $Y\subseteq X$ существует наименьший элемент.

- Конечное множество вполне упорядочено.
- ω, $\omega+1$, $\omega+\omega$, $\omega\cdot\omega$ вполне упорядочены.
- ω^*, η и λ не являются вполне упорядоченными.

Доказательство следующего результата основано на аксиоме выбора.

Теорема. *Линейно упорядоченное множество в том и только том случае вполне упорядочено, когда X не содержит ω^*.*

Доказательство. Очевидно, если X содержит ω^*, то оно не может быть вполне упорядоченным.

Обратно, пусть $Y\subseteq X$ – непустое подмножество, не содержащее минимального элемента. Тогда для каждого $y\in Y$ нижний конус $y^\nabla=\{z\in Y\mid z<y\}$ непуст. Пусть $f: Y\mapsto Y$ – функция такая, что $f(y)<y$ для любого $y\in Y$. Тогда множество $\{y>f(y)>f^2(y)>\ldots\}$ имеет порядковый тип ω^*.

§ 16. Принцип трансфинитной индукции

Следующий результат называется принципом трансфинитной индукции.

Теорема. *Пусть X – фундированное частично упорядоченное множество, $Y \subseteq X$. Предположим, что*

1) Все минимальные элементы множества X принадлежат Y.

2) Если для данного $x \in X$ все элементы $y \in X$, $y < x$ принадлежат Y, то $x \in Y$.

Тогда $Y = X$.

Доказательство. В самом деле, предположим, что $X \setminus Y$ непусто. Тогда в силу фундированности X множество $X \setminus Y$ имеет минимальный элемент z. Имеет место следующая альтернатива.

Элемент z является минимальным элементом множества X. Тогда он принадлежит Y по условию 1), противоречие.

Элемент z не является минимальным элементом множества X. Тогда для любого $w \in X$, такого, что $w < z$, в силу минимальности z имеем $w \in Y$. Значит $z \in Y$ по условию 2), так что мы снова получаем противоречие.

Тем самым $X \setminus Y = \varnothing$.

Тема 6. Аксиома выбора

> Почему же эта простая (если не самоочевидная) аксиома привела к столь многочисленным обсуждениям? Ни одна из аксиом после пятого постулата Эвклида о параллельных прямых не вызвала такого волнения в математических кругах и не возбудила так много споров по проблемам оснований математики.
>
> Томас Дж. Йех[230]

> Я знаю математиков, которые утверждают, что аксиома выбора имеет тот же характер интуитивной самоочевидности, который присущ самым элементарным законам логики, на которые опирается математика. Мне так никогда не казалось. Но как можно обсуждать вопросы интуиции?
>
> Алонзо Черч, "Поль Коэн и проблема континуума"

Сейчас мы обсудим одну из самых интересных аксиом теории множеств - аксиому выбора. При первом знакомстве она кажется очевидной, но из нее вытекают следствия – такие как "парадоксы" Хаусдорфа и Банаха-Тарского – представляющиеся многим нематематикам невероятными и даже абсурдными. С другой стороны, при дальнейшем знакомстве с математикой эти следствия становятся совершенно необходимыми и очевидными. Словом, отношение к этой аксиоме претерпевает – с обратным знаком – ту эволюцию которую Гамлет описал следующими словами: "то, что вчера было парадоксом, сегодня перестало им быть, но завтра снова им станет".

В самой простой формулировке аксиома выбора утверждает следующее:

Аксиома выбора. *Если X - объединение непересекающихся непустых множеств X_α, то существует по крайней мере одно подмножество Y, которое пересекается с каждым X_α ровно по одному элементу.*

Этой акиоме можно придать несколько эквивалентных форм, напрмер, следующую: если нам дано любой семейство непустых множеств X_α, $\alpha \in \Omega$, то существует отображение $f : \Omega \longrightarrow \bigcup X_\alpha$ такое, что для каждого $\alpha \in \Omega$ имеет место $f(\alpha) \in X_\alpha$. Иными словами, мы можем выбрать по одному элементу $x_\alpha = f(\alpha)$ из каждого множества X_α. Так как такая функция f может быть отождествлена с набором (x_α), $\alpha \in \Omega$, ее значений, представляющим элемент прямого произведения $\prod X_\alpha$, $\alpha \in \Omega$, то аксиому выбора можно сформулировать еще и таким образом: прямое произведение любого семейства непустых множеств непусто. В такой форме эта аксиома представляется особенно очевидной.

Лемма Куратовского-Цорна

Теорема Хаусдорфа

Теорема Банаха-Тарского

С другой стороны отсутствие аксиомы выбора приводит к гораздо более парадоксальным следствиям, которые в значительно большей степени противоречат нашей интуиции. Например, в отсутствие аксиомы выбора континуум может быть представлен в виде объединения счетного семейства счетных множеств. Этот парадоксальный вывод требует, конечно, значительно большего

[230]Т.Дж.Йех, Об аксиоме выбора. – Справочная книга по математической логике, т.II. Теория множеств. М., Наука, 1982, с.35–63.

пересмотра всего традиционного анализа, как в самых первых понятиях, связанных с вещественными числами, пределами и пр., так и, в особенности, в части, связанной с мерой и интегрированием. Такой пересмотр был бы гораздо более болезненен, чем тот отказ от представления, что все "фигуры" имеют "объем", который вытекает из принятия аксиомы выбора.

До сих пор в некоторых популярных изложениях можно встретить утверждение, что аксиома выбора в чем то отличается в смысле своего статуса от остальных аксиом теории множеств. В действительности в 1938-1940 годах Курт Гедель доказал, что если аксиоматическая теория множеств непротиворечива, то она остается непротиворечивой и после добавления аксиомы выбора. Метод доказательства состоял в построении **модели** для теории множеств с выполненной аксиомой выбора (и **обобщенной гипотезой континуума**, см. раздел ?) в рамках теории множеств, в которой аксиома выбора не предполагается. Ситуация здесь полностью параллельна построению модели неэвклидовой геометрии внутри эвклидовой геометрии, см. раздел ?. Спорить сегодня, спустя 60 лет после этого результата, о том, справедлива или нет "на самом деле" аксиома выбора, столь же наивно, как спорить о том, сколько прямых параллельных данной можно "на самом деле" провести через фиксированную точку. И та и другая возможность равным образом относятся к математике и – с абстрактной точки зрения – равным образом заслуживают рассмотрения. Однако математика, как физика или музыка, является человеческой деятельностью. Если мы и делаем какой-то выбор (а подавляющее большинство работающих математиков предпочитает иметь дело с теорией, в которой аксиома выбора выполняется), то он диктуется исключительно эстетическими соображениям: теория множеств с аксиомой выбора проще и эффективнее, чем теория без этой аксиомы.

§ 1. Покрытия и разбиения, аксиома выбора **ZF8**

1. Покрытия и разбиения. Следующее определение понадобится нам для того, чтобы привести простую формулировку аксиомы выбора **ZF8**. В дальнейшем мы приведем и много других формулировок этой аксиомы, на языке отображений, прямых произведений, мощностей, упорядоченных множеств и т.д., но самая простая формулировка использует понятие разбиения.

Определение. *Семейство подмножеств $X_i \subseteq X$, $i \in I$, называется* **покрытием** *X, если $X = \cup X_i$, $i \in I$, и* **разбиением** *X, если, кроме того, все X_i* **непусты** *и* **попарно дизъюнктны**, *иными словами, $X_i \cap X_j = \varnothing$ для любых $i \neq j$.*

Таким образом, если X_i, $i \in I$, – разбиение X, то $X = \coprod X_i$. При этом множества X_i называются обычно **классами** или **блоками** разбиения.

2. Разбиения и отношения эквивалентности. Задать разбиение множества X – это то же самое, что задать на X отношение эквивалентности. В самом деле, если $\sim$ отношение эквивалентности на X, а X_i, $i \in I$, – классы эквивалентности $\sim$, то два различных класса не пересекаются, поэтому X_i, $i \in I$, – разбиение X. Обратно, для любого разбиения X_i, $i \in I$, определим отношение эквивалентности $\sim$ на X, полагая $x \sim_X y$ в том и только том случае, если найдется такое i, что $x, y \in X_i$. Иными словами, как подмножество R в $X \times X$ это отношение эквивалентности определяется посредством $R = \coprod X_i \times X_i$, $i \in I$.

Определение. *Пусть X – разбиение множества A. Тогда подмножество $B \subseteq A$ называется* **трансверсалью** *к разбиению X (alias* **системой представителей** *отношения эквивалентности $\sim_X$), если для каждого $Y \in X$ множества B и Y пересекаются ровно по одному элементу.*

3. Аксиома выбора в форме Леви. Сейчас мы сформулируем аксиому, принятие которой резко упрощает строение множеств. В такой форме аксиома выбора была явно сформулирована Леви, хотя в действительности, Кантор использовал эту аксиому без явного упоминания.

ZF8 (аксиома выбора). *Для каждого разбиения существует хотя бы одна трансверсаль.*

Иными словами, утверждается, следующее: пусть $X = \coprod X_i$ – разбиение X на непустые множества X_i, то найдется такое множество Y, что каждое из пересечений $Y \cap X_i$ состоит ровно их одного элемента. Сформулированная аксиома часто обозначается еще **AC** (axiom of choice). Это единственная аксиома, которая формулируется во всех наивных изложениях теории множеств, причем часто формулируется совершенно ошибочно. А именно, говорят, что аксиома выбора утверждает, что можно *выбрать* по одному элементу в каждом из множеств X_i. Однако это утверждение очевидным образом верно *независимо от аксиомы выбора* – по крайней мере, если мы считаем, что всегда можно выбрать элемент из **одного** непустого множества.

4. Аксиома выбора в форме Цермело. Цермело формулировал аксиому чуть иначе, не требуя, чтобы множества X_i были непересекающимися.

ZF8 (аксиома выбора). *Для каждого семейства X_i, $i \in I$, непустых множеств X_i существует функция $f : I \longrightarrow \bigcup X_i$ такая, что $f(i) \in X_i$.*

Такая функция называется **функцией выбора**. Ясно, что аксиома выбора в форме Цермело влечет аксиому выбора в форме Леви. Покажем, что верно и обратное. В самом деле, рассмотрим произвольное семейство множеств X_i, $i \in I$. Нам нужно изготовить из него семейство попарно непересекающихся множеств. Стандартный прием состоит в следующем. Обозначим через Y_i множество упорядоченных пар (i, x), где $x \in X_i$. Ясно, что $Y_i \cap Y_j = \varnothing$. По аксиоме Леви найдется множество Z, которое пересекается с каждым Y_i ровно по одному элементу (i, x_i), где $x_i \in X_i$. Теперь мы можем определить функцию выбора, полагая $f(i) = x_i$.

5. Пафос аксиомы выбора. Пафос аксиомы выбора состоит в том, что этот выбор можно произвести **согласованным образом**, так, чтобы выбранные элементы **образовывали множество**. Из аксиомы подстановки будет тогда следовать, что *любой* выбор представителей является согласованным, т.е. образует множество. Вот как описывал аксиому выбора сам Цермело: “Man kann das Axiom auch so ausdrücken daß man sagt es sei immer möglich aus jedem Elemente $M, N, R, \ldots$ von T einzelne Elemente $m, n, r, \ldots$ auszuwählen **und alle diese Elemente zu einer Menge S_1 zu vereinigen**”. Френкель пишет, что невнимательное чтение этой фразы вызвало у многих современников непонимание сути аксиомы выбора: “Dieser letzte Satz hat vielfach die Meinung hergerufen der Kern des Axioms liege in der Forderung der Möglichkeit der “Auswahl eines ausgezeichneten Elementes” aus jeder Menge $M, N, \ldots$ oder in der Forderung der Möglichkeit der “gleichzeitingen Auswahl” aus ihnen allen”. Такое толкование

аксиомы не имеет, как мы увидим в следующем пункте, никакого отношения к ее действительному содержанию. Аксиома выбора не говорит ничего ни о возможности выбора представителей (который возможен **всегда**), ни о его фактическом осуществлении (которое не возможно даже для одного множества), напротив, она носит чисто **экзистенциальный** характер. То, что в действительности утверждается этой аксиомой – это не возможность выбора представителей, а возможность **соединить выбранные представители в множество**.

6. Невозможность выбора элемента из одного непустого множества. Заметим, что практически неосуществим именно конструктивный выбор представителя **одного** множества. Например, определим множество X следующим образом. Известно, что самой важной нерешенной (на осень 2003 года) проблемой математики – и не только математики, но и всей жизни, как заметил Гильберт – остается гипотеза Римана. Положим $X = \{1\}$, если гипотеза Римана **верна** (т.е. вытекает из аксиом **ZFC**), $X = \{0\}$, если гипотеза Римана **неверна** (т.е. ее отрицание вытекает из аксиом **ZFC**) и $X = \{1/2\}$, если гипотеза Римана **неразрешима** (т.е. не зависит от аксиом **ZFC**). Множество X непусто и поэтому мы можем сказать 'возьмем элемент множества X' и оперировать далее с этим элементом. В то же время, при нашем сегодняшнем состоянии знаний мы не можем конкретно указать ни одного элемента этого множества.

Если бы мы могли осуществить выбор элемента из произвольного непустого множества, то в силу свойств конъюнкции (или, как говорит Френкель, "поскольку математика не знает времени") мы могли бы осуществить такой выбор и из любого множества множеств. Но это совсем не означало бы, что аксиома выбора верна! Продолжим цитату из статьи Френкеля 1922 года: "Ist so die Auswahl für jede einzelne Menge möglich, so ist es **natürlich** auch gleichzeitig für alle Mengen von T, da die Auswahl wie jede mathematisvche Operation als etwas Zeitloses anzusehen ist".

7. Конечная аксиома выбора. Известно, что аксиома выбора независима от остальных теории множеств. Существуют модели теории множеств, в которых все аксиомы теории **ZF** выполняются, а аксиома выбора – нет. Впрочем, для одного случая аксиома выбора может быть доказана на основе остальных аксиом. А именно, разбиения на конечное число блоков аксиома выбора вытекает из аксиом пары и объединения (любая конечная совокупность объектов может быть соединена в множество). Видимо, даже Э.Борель и А.Лебег не оспаривали справедливость аксиомы выбора в этом случае.

8. Выбор из одноэлементных множеств. Есть еще один случай, когда аксиома выбора доказуема на основе остальных аксиом теории множеств – это выбор по одному представителю из **одноэлементных** множеств и объединение их в множество. В этом случае аксиома выбора утверждает, что если $\{\{x\}, \{y\}, \{z\}, \dots\}$ является множеством, то $\{x, y, z \dots\}$ тоже является множеством. Как отмечает Томас Йех, именно осуществимость выбора в этом случае побуждает некоторые государства (так называемые страны *народной* демократии) систематически проводить выборы с одним кандидатом на одно место.

9. Счетная аксиома выбора. Аксиома выбора для разбиения на счетное число блоков уже никоим образом не вытекает из остальных аксиом. Заметим, что для многих теорем анализа достаточно лишь следующей версии аксиомы

выбора.

CAC (счетная аксиома выбора). *Для каждого разбиения на счетное число блоков существует хотя бы одна трансверсаль.*

Разумеется, **CAC** является сокращением от Countable Axiom of Choice. Как мы сейчас увидим, счетная аксиома выбора не вытекает из аксиом теории **ZF** даже если все блоки *конечны*.

10. Невозможность выбора из двухэлементных множеств. Простейший случай, когда аксиома выбора проблематична – это выбор системы представителей для счетного числа двухэлементных блоков. Бертран Рассел поясняет этот случай следующим примером. Рассмотрим счетное множество пар ботинок. Поскольку ботинки выпускаются на левую и на правую ногу, в этом случае существует **функция выбора**, сопоставляющая каждой паре **левый** или **правый** ботинок, в зависимости от политических пристрастий (подробнее см. об этом Главу 4). Продолжая метафору Йеха, можно сказать, что если в стране существует ровно две партии, скажем, партия воров и партия вымогателей, и каждая из них выдвигает по одному кандидату на одно место, то самая простая стратегия для избирателя состоит в том, чтобы либо все время голосовать за вора, либо все время голосовать за вымогателя.

В то же время, продолжает Рассел, фабриканты носков придерживаются *достойного сожаления* (deplorable) обычая выпускать *неотличимые* носки на левую и на правую ногу. Так вот, если нам дано счетное множество пар носков, нет *никакого* естественного способа выбрать множество, содержащее ровно по одному носку из каждой пары и единственное основание, которое позволяет нам утверждать, что такое множество существует – это аксиома выбора. Иными словами, если на каждое место выдвигаются два кандидата, но не принадлежащих никакой партии, либо принадлежащих одной и той же партии, скажем, два вора, то нет никакого разумного способа осуществить выбор. С этим связано пристрастие некоторых государств (так называемые страны *западной* демократии) к жесткой двухпартийной системе (воры и вымогатели, или, эвфемически, демократы и республиканцы), позволяющей осуществить выборы с такой же легкостью, что и система, при которой на одно место выдвигается один кандидат.

§ ?. Лемма Куратовского-Цорна

Следствия аксиомы выбора. В этом пункте мы сформулируем несколько следствий (на самом деле переформулировок) аксиомы выбора в терминах частично упорядоченных множеств.

Наиболее важным из них для нас будет

Лемма Куратовского-Цорна. *Если любое линейно упорядоченное подмножество множества X имеет верхнюю грань, то в X существует максимальный элемент.*

Говорят, что множество X удовлетворяет **условию максимальности** (**минимальности**), если любое его непустое подмножество содержит максимальный (минимальный) элемент. Множества с условием максимальности называются еще **нетеровыми**, а множества с условием минимальности – **артиновыми**. Несложно убедиться, что условие максимальности эквивалентно следующему условию обрыва возрастающих цепей: если $x_1 \leq x_2 \leq \ldots \leq x_n \leq \ldots$, то

существует такое m, что $x_n = x_m$ для всех $n \geq m$. Аналогично, условие минимальности эквивалентно двойственному условию обрыва убывающих цепей. Лемма Куратовского-Цорна и условие максимальности будут для нас основой многих индуктивных доказательств.

Линейно упорядоченное множество, удовлетворяющее условию минимальности называется **вполне упорядоченным**. В силу линейной упорядоченности минимальный элемент обязан быть наименьшим, поэтому вполне упорядоченное множество может быть определено еще как множество, в котором любое непустое подмножество содержит наименьший элемент. Следующие утверждения являются еще двумя известными переформулировками аксиомы выбора (иногда называемыми **аксиомой полной упорядоченности** и **принципом максимальности Хаусдорфа**, соответственно).

Гл. ?. Переформулировки аксиомы выбора

> Вот Павел Сергеевич, ну известный наш академик, Александров, он никогда не летает на самолете. А вы знаете почему? Он не знает доказательства теоремы Жуковского и поэтому не понимает, как самолет держится в воздухе. А я знаю! И не боюсь летать!
>
> Борис Николаевич Делоне

В этой главе мы рассмотрим несколько замечательных переформулировок аксиомы выбора в терминах частично упорядоченных множеств.

§ ?. Лемма Куратовского-Цорна

Наиболее важным из них для нас будет следующее утверждение называемое обычно **леммой Куратовского-Цорна**, но иногда просто **леммой Цорна** или **dies irae**. Это утверждение является, вероятно, наиболее удобной и наиболее часто используемой в настоящее время формулировкой аксиомы выбора.

Лемма Куратовского-Цорна. *Если любое линейно упорядоченное подмножество множества X имеет верхнюю грань, то в X существует максимальный элемент.*

Доказательство.

Теорема Хаусдорфа влечет лемму Куратовского-Цорна. В самом деле, пусть Y – максимальная цепь в множестве Y, y – ее верхняя грань. Если y не является максимальным элементом множества X, то найдется $x \in X$, $x > y$. Тогда множество $Y \cup \{x\}$ является цепью, строго содержащей Y, что противоречит максимальности Y. Таким образом, y обязан быть максимальным элементом множества X.

Говорят, что множество X удовлетворяет **условию максимальности** (**минимальности**), если любое его непустое подмножество содержит максимальный (минимальный) элемент. Множества с условием максимальности называются еще **нетеровыми**, а множества с условием минимальности – **артиновыми**. Несложно убедиться, что условие максимальности эквивалентно следующему условию обрыва возрастающих цепей: если $x_1 \leq x_2 \leq \ldots \leq x_n \leq \ldots$, то существует такое m, что $x_n = x_m$ для всех $n \geq m$. Аналогично, условие минимальности эквивалентно двойственному условию обрыва убывающих цепей.

Лемма Куратовского-Цорна и условие максимальности будут для нас основой многих индуктивных доказательств.

Линейно упорядоченное множество, удовлетворяющее условию минимальности называется **вполне упорядоченным**. В силу линейной упорядоченности минимальный элемент обязан быть наименьшим, поэтому вполне упорядоченное множество может быть определено еще как множество, в котором любое непустое подмножество содержит наименьший элемент. Следующие утверждения являются еще двумя известными переформулировками аксиомы выбора (иногда называемыми **аксиомой полной упорядоченности** и **принципом максимальности Хаусдорфа**, соответственно).

Теорема Цермело. *Всякое множество можно вполне упорядочить.*

Доказательство. Проведем доказательство, основанное на лемме Куратовского-Цорна. Пусть X – произвольное множество и Z – множество, состоящее из всех пар $(A, \prec_A)$, где A – вполне упорядочиваемое подмножество множества X, а $\prec_A$ – какой-то полный порядок на A. Заметим, что Z непусто, так как $(\varnothing, \varnothing) \in Z$. Мы хотим показать, что $X \in \mathrm{pr}_1(Z)$. Для этого прежде всего введем частичный порядок на Z, полагая $(A, \prec_A) \leq (B, \prec_B)$, если выполняются следующие три условия: 1) $A \subseteq B$, 2) ограничение порядка $\prec_B$ на A совпадает с $\prec_A$ и 3) подмножество A является порядковым идеалом в B (иными словами, если $x \in A$, $y \in B$ и $y \prec_B x$, то $y \in A$).

Покажем, что любая цепь в Z имеет точную верхнюю грань. В самом деле, пусть $(A_i, \prec_i)$, $i \in I$, – какая-то цепь в Z. Рассмотрим объединение $A = \cup A_i$, $i \in I$, и покажем, что A можно вполне упорядочить так, чтобы выполнялись условия 2) и 3) выше. В самом деле, пусть $x, y \in A$, причем $x \in A_j$, а $y \in A_h$. Так как A_i, $i \in I$, – цепь, то одно из множеств A_j или A_h содержится в другом, поэтому без потери общности можно считать, что $x, y \in A_i$. В этом случае положим $x \prec y$ в том и только том случае, когда $x \prec_i y$. Это определяет неравенство $x \prec y$ корректно, так как если $h \in I$ другой индекс такой, что $x, y \in I_h$, то условие 2) гарантирует, что $x \prec_h y$ в том и только том случае, когда $x \prec_j y$. Нам осталось еще проверить, что так построенное отношение $\prec$ вполне упорядочивает множество A. Ясно, что A линейно упорядочено этим отношением и нам нужно лишь показать, что любое непустое подмножество B в A имеет наименьший элемент. В самом деле, так как B непусто, то найдется такой индекс $j \in I$, что $B \cap A_j$ непусто. Пусть $b \in B$ – наименьший элемент множества $B \cap A_j$. Покажем, что тогда b является наименьшим элементом множества B. В самом деле, по определению b не больше любого элемента $a \in A_j$. Предположим теперь, что существует элемент $a \in B \setminus A_j$ такой, что $a \prec b$. Возьмем любой индекс $h \in I$ такой, что $a \in A_h$. Тогда $A_j \subseteq A_h$, так что $a \prec_h b$ и теперь условие 3) гарантирует, что $a \in A_j$, противоречие. Тем самым, любое подмножество $B \subseteq A$ имеет наименьший элемент и, значит, A вполне упорядочено.

Таким образом по лемме Куратовского-Цорна множество Z содержит максимальный элемент, скажем, $(A, \prec_A)$. Предположим, вопреки ожиданиям, что $A \neq X$. Возьмем $z \in X \setminus A$ и рассмотрим множество $B = A \cup \{z\}$. Продолжим порядок $\prec$ с A на B, полагая $x \prec_B y$ для любых $x, y \in A$ в том и только том случае, когда $x \prec_A y$ и $x \prec_B z$ для всех $x \in A$. Тогда, очевидно, $(A, \prec_A) < (B, \prec_B)$, что противоречит максимальности $(A, \prec_A)$. Полученнное противоречие показывает, что $A = X$ так что множество X вполне упорядочиваемо.

Теорема Цермело влечет аксиому выбора. Пусть X – любое множество попарно дизъюнктных множеств. Согласно теореме Цермело все множества $A \in X$ можно вполне упорядочить. Рассмотрим теперь объединение $B = \cup A$, $A \in X$, и введем на нем частичный порядок, превращающий его в копроизведение упорядоченных множеств A. Тогда множество минимальных элементов является трансверсалью к разбиению X множества A.

Теорема Хаусдорфа. *Любая цепь в чуме X может быть включена в максимальную по включению цепь.*

§ ?. Аксиома выбора в форме Тарского

Теорема. *Если X – бесконечное множество, то $|X \times X| = |X|$.*

Доказательство. Рассмотрим множество Ω пар (Y, f), где Y – бесконечное подмножество X, а $f \in \mathrm{Inj}(Y, X \times X)$ – такое инъективное отображение, что $\mathrm{Im}(f) = Y \times Y$. В предположении аксиомы выбора множество Ω непусто (достаточно взять в качестве Y любое счетное подмножество в X). Введем на Ω частичный порядок полагая $(Y, f) \leq (Z, g)$, если $Y \subseteq Z$ и $f = g|_Z$. По лемме Цорна Ω содержит максимальный элемент (Z, g).

Обратно, как показал Альфред Тарский, это свойство эквивалентно аксиоме выбора.

Тема 1. БИНАРНЫЕ АЛГЕБРАИЧЕСКИЕ ОПЕРАЦИИ

Алгебраические операции, понимаемые в широком смысле, являются просто отображениями. Спецификой алгебраического подхода является акцент на **бинарных операциях** (законах композиции) и, в еще большей степени, на тех **тождествах** (функциональных уравнениях), которым они удовлетворяют и на **гомоморфизмах** между операциями, заданными на различных множествах.

§ 1. Бинарные операции

> Большинство людей довольно рано убеждается, что в таких арифметических действиях, как сложение, умножение, деление и т.д. всегда возникает много ошибок.
>
> Л.Морделл, "Размышления математика".

1. Внутренние бинарные операции. В самом широком понимании **n-арная алгебраическая операция** есть отображение $X_1 \times \ldots \times X_n \longrightarrow Y$, где $X_1, \ldots, X_n, Y$ суть непустые множества, a priori различные. В дальнейшем мы вернемся к рассмотрению некоторых типов **внешних** операций, однако начнем с наиболее важного случая **внутренних** операций, когда все эти множества равны между собой.

Определение. Внутренней n-арной операцией *на непустом множестве X называется отображение $f : X \times \ldots \times X \longrightarrow X$ его n-й декартовой степени X^n в само множество X.*

Эпитет 'внутренняя' часто опускается и обычно говорят просто об алгебраических операциях. При $n = 0$ такая операция называется **нульарной**, при $n = 1$ – **унарной**, при $n = 2$ – **бинарной**, при $n = 3$ – **тернарной**, и т.д. Вскоре мы скажем кое-что об операциях других **арностей** и о дальнейших обобщениях, но сразу отметим, что наиболее важен классический случай **бинарных операций**, часто называемых просто **операциями** или **законами композиции** (Verknüpfung), т.е. отображений

$$f : X \times X \longrightarrow X, \quad (x, y) \mapsto f(x, y).$$

При этом x и y называются **операндами**, а $f(x, y)$ – **результатом** операции. В старинных книжках алгебраические операции назывались еще **действиями**[231], однако мы используем термин 'действие' (action) в точном техническом смысле: "действие чего-то на чем-то", см. § ?.

2. Инфиксная запись бинарной операции. При записи бинарной операции вместо $f(x, y)$ иногда пишут xfy, но чаще всего заменяют f каким-либо знаком действия, например, '$*$', '$+$', '$\cdot$', и т.д. и вместо $f(x, y)$ пишут $x*y$, $x+y$, $x\cdot y$ (или просто xy) или что-нибудь в таком духе. Когда необходимо подчеркнуть, что множество X рассматривается вместе с заданной на нем операцией $*$, пишут $(X, *)$.

Такая запись, когда знак операции пишется **между** операндами, называется **инфиксной**, в отличие от **префиксной** записи $f(x, y)$, когда знак операции

[231] etwa "четыре действия арифметики: служение, почитание, угождение и давление." – "The different branches of Arithmetic – Ambition, Distraction, Uglification and Derision".

пишется **перед** операндами. Во втором случае можно обойтись без скобок и писать fxy, это так называемая **запись Лукасевича** (называемая в популярной литературе **польской записью**), обычная в логике и computer science, но алгебраисты редко ей пользуются. В некоторых микрокалькуляторах используется **постфиксная** запись, когда знак операции вводится **после** операндов. В популярной литературе такая запись обычно называется **обратной польской записью**. В настоящем курсе мы в соответствии с алгебраической традицией пользуемся почти исключительно инфиксной записью. В некоторых случаях традиционно используется **циркумфиксная** запись, которая охватывает операнды с двух сторон (сочетание совместно работающих префикса и постфикса), скажем, $[x, y]$, (x, y) и т.д.

Перечислим еще несколько обычных обозначений бинарных операций: $x \circ y$, $x \star y$, $x \times y$, $x \dot{+} y$, $x \wr y$, $x \uparrow y$, $x \downarrow y$, $x \wedge y$, $x \vee y$, $x \curlywedge y$, $x \curlyvee y$, $x \cap y$, $x \cup y$, $x \Cap y$, $x \Cup y$, $x \sqcap y$, $x \sqcup y$, $x \uplus y$, $x \top y$, $x \bot y$, $x \vdash y$, $x \dashv y$, $x \oplus y$, $x \otimes y$, $x \ominus y$, $x \oslash y$, $x \odot y$, $x \boxplus y$, $x \boxtimes y$, $x \boxminus y$, $x \boxdot y$, $x \Box y$, $x \Diamond y$, $[x, y]$, x^y, ${}^y x$, $x \hat{} y$ и т.д.). Соответственно этому операнды называются **слагаемыми**, **сомножителями**, **факторами** и т.д., а результат называется **суммой**, **произведением**, **суперпозицией** и т.д. – в § ? мы подробнее обсудим терминологию, относящуюся к некоторым наиболее употребительным нотациям.

3. Таблица Кэли. Любая бинарная алгебраическая операция $*$ на множестве X может быть задана посредством своей **таблицы Кэли**, строки и столбцы которой занумерованы элементами X, а на пересечении строки с номером x и столбца с номером y стоит элемент $x * y$. Такая таблица достаточно наглядна лишь для конечных множеств небольших порядков, но в этом случае мы будем иногда пользоваться таким представлением операции. В качестве примера, изобразим таблицы Кэли для полугруппы левых нулей и полугруппы правых нулей порядка 4, о которых пойдет речь в § ?:

$*$	a	b	c	d
a	a	a	a	a
b	b	b	b	b
c	c	c	c	c
d	d	d	d	d

$*$	a	b	c	d
a	a	b	c	d
b	a	b	c	d
c	a	b	c	d
d	a	b	c	d

Пусть $|X| = n$. Вообще говоря, для произвольной алгебраической операции на таблицу Кэли не накладывается никаких ограничений и, так как для каждого из n^2 произведений $x * y$ имеется n возможных значений, общее число бинарных операций на X – равно n^{n^2}. Однако обычно рассматриваются лишь операции, подчиненные достаточно жестким тождествам, и в следующих параграфах мы выясним, как это отражается на соответствующей таблице Кэли.

4. Размышлизм: почему бинарные операции? Ограничение функциями двух переменных может показаться начинающему искусственным. Однако в действительности для этого есть серьезное основание: минутное размышление убеждает в том, что *не существует* функций трех и более переменных – любая функция трех и более переменных представима в виде композиции функций двух переменных. Поэтому каждая операция более высокой арности может рассматриваться как производная операция. Более того, легко видеть, достаточно даже унарных операций и **одной** бинарной операции. В действительности, в связи с **тринадцатой проблемой Гильберта** А.Н.Колмогоров и В.И.Арнольд в 1957 показали, что это так даже в классе непрерывных функций: каждая непрерывная вещественная функция

от любого числа переменных представима в виде композиции непрерывных функций одной переменной и сложения! См. по этому поводу статью А.Г.Витушкина[232].

§ 2. Операции над числами

Напомним примеры внутренних бинарных операций, встречавшихся в школе и введем некоторые новые примеры. Рассмотрим прежде всего операции над числами.

• **Сложение и умножение чисел.** Пусть $X = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ и $f(x, y) = x + y$ – сумма чисел, или $f(x, y) = xy$ – произведение чисел. Эти операции дают названия двум наиболее употребительным системам записи алгебраических операций: аддитивной нотации и мультипликативной нотации. В **аддитивной** нотации операция обозначается '+' и называется **сложением**, операнды – **слагаемыми**, результат операции – **суммой**. В **мультипликативной** нотации операция обозначается '$\times$' или '$\cdot$' и называется **умножением**, операнды – **множителями, сомножителями** или **факторами**, результат операции – **произведением**. Мы вернемся к другим терминам, связанными с этими системами записи в § 4.

• **Вычитание и деление чисел.** Операция вычитания $f(x, y) = x - y$ не является всюду определенной операцией на множестве натуральных чисел. Мы должны либо расширить понятие операции (рассматривая **частичные операции** т.е. такие операции, которые не всюду определены, см. § ?), либо расширить понятие числа, введя в рассмотрение целые числа. Точно так же для выполнимости деления $f(x, y) = x/y$ вводятся 'обыкновенные дроби', т.е. множество $\mathbb{Q}_+$ положительных рациональных чисел. Однако требования выполнимости вычитания и деления оказываются **несовместимыми** (деление на 0 невозможно). Принятое в алгебре решение состоит в том, что вычитание и деление рассматриваются не как самостоятельные операции, а как **производные операции**, т.е. композиции сложения и умножения с некоторыми унарными операциями.

• **Арифметическое вычитание.** Еще один способ сделать вычитание натуральных чисел всюду определенным состоит в следующем. Назовем **арифметической разностью** $m \dot{-} n$ двух чисел $m, n \in \mathbb{N}_0$ их обычную разность $m - n$, если $m \geq n$ и 0, если $m < n$. Операция арифметической разности широко применяется в теории рекурсивных функций и некоторых азартных играх, где игрок обладает определенным количеством фишек и теряет их в определенных случаях, но при проигрыше, превышающем наличное количество фишек, долг не записывается.

• **Унитарное умножение.** На $\mathbb{N}_0$ можно рассмотреть операцию $\star$, называемую **унитарным умножением** и определяемую как $m \star n = mn$, если m и n взаимно просты и $m \star n = 0$ в противном случае.

• **Возведение в степень** (или, что то же самое, **'извлечение корня'**). На множестве натуральных чисел операция $f(x, y) = x^y$ всюду выполнима. В логике и большинстве языков программирования для операции возведения в степень используется специальный знак, например, $x \uparrow y$ или $x\hat{}y$. Использование других традиционных названий операции возведения в степень, таких

[232]А.Г.Витушкин, К тринадцатой проблеме Гильберта. – в книге: Проблемы Гильберта, М., Наука, 1969, с.163–170.

как **потенцирование** (Potenzierung) и **экспоненцирование** (exponentiation), запрещено Государственной Думой.

Размышлизм: зачем нужны вещественные числа? Как только мы расширяем понятие числа так, чтобы были выполнимы операции вычитания и деления, выясняется, что распространение этой операции на новые числа, скажем рациональные, снова требует дальнейшего расширения понятия числа. Детальное обсуждение этой темы слишком далеко от нашего курса. Заметим лишь, что иррациональность числа $\sqrt{2}$, которая обычно приводится в школьных учебниках как обоснование необходимости введения вещественных чисел, в действительности доказывает лишь необходимость введения **алгебраических** чисел, т.е. корней алгебраических уравнений с целыми коэффициентами. Однако как показывает полученное в 1934 году А.О.Гельфондом и Т.Шнайдером решение **седьмой проблемы Гильберта**, любая попытка распространить на *алгебраические* числа операцию возведения в степень с необходимостью приводит к **трансцендентным** числам[233,234].

§ 3. Операции над векторами

Перечислим теперь некоторые операции над векторами

• **Сложение векторов.** Пусть $u = (u_1, \dots, u_n)$ и $v = (v_1, \dots, v_n)$ – два вектора с компонентами из некоторого поля K (пока мы формально не знакомы с полями, можно считать, например, что $K = \mathbb{Q}, \mathbb{R}$ или $\mathbb{C}$ есть поле рациональных, вещественных или комплексных чисел). Тогда **сумма** векторов u и v, определяется покомпонентно. Иными словами, $u + v$ определяется как

$$(u_1, \dots, u_n) + (v_1, \dots, v_n) = (u_1 + v_1, \dots, u_n + v_n).$$

Для плоскости и трехмерного пространства это определение совпадает с обычным сложением векторов, как оно определялось в школе.

• **Покомпонентное умножение векторов.** Пусть $u = (u_1, \dots, u_n)$ и $v = (v_1, \dots, v_n)$ – два вектора с компонентами из некоторого поля K. Тогда можно определить их **покомпонентное произведение** векторов u и v, положив

$$(u_1, \dots, u_n)(v_1, \dots, v_n) = (u_1 v_1, \dots, u_n v_n)$$

Эти примеры являются частными случаями понятия прямой суммы/прямого произведения операций, которое будет определено в § ? и к которому мы будем многократно обращаться в дальнейшем.

• **Умножение векторов в K^2.** В действительности, векторы можно умножать и иначе, чем это делается в предыдущем примере. Скажем, векторы двумерного пространства $X = K^2$ над полем K можно умножать как **комплексные числа**

$$(a, b)(c, d) = (ac - bd, ad + bc),$$

как **дуальные числа**

$$(a, b)(c, d) = (ac, ad + bc)$$

или **как двойные числа**

$$(a, b)(c, d) = (ac + bd, ad + bc).$$

---

[233] А.О.Гельфонд, К седьмой проблеме Гильберта. – в книге: Проблемы Гильберта, М., Наука, 1969, с.121–127.

[234] Н.И.Фельдман, Седьмая проблема Гильберта, М., Изд-во Моск. ун-та, 1982, с.1–311.

• **Векторное умножение векторов в K^3.** Пусть $X = K^3$ – трехмерное векторное пространство над полем K. В этом пространстве можно ввести операцию сложения векторов $u+v$ и операцию **векторного умножения** $[u,y]$ (которое часто записывается еще как $x \times y$ и в этом случае называется **cross product**):

$$[u,v] = (u_2v_3 - u_3v_2, u_3v_1 - u_1v_3, u_1v_2 - u_2v_1).$$

• **Циклическая свертка векторов.** А вот совсем другой тип операции, который мы будем подробно изучать в следующей главе. Пусть $a = (a_1, \dots, a_n)$ и $b = (b_1, \dots, b_n)$ – два вектора из K^n. **Циклической сверткой** этих векторов называется вектор $c = a*b \in K^n$ такой, что $c_i = \sum a_j b_{i-j}$, где сумма берется по всем $j \in \underline{n}$, причем $i-j$ понимается по модулю n, так что, например, $a_0 = a_n$, $a_{-1} = a_{n-1}$ и т.д.

§ 4. Максимум и минимум

Следующие типы примеров в действительности можно трактовать совместно.

• **Максимум и минимум.** Пусть $X = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$. Тогда $\max(x,y)$ и $\min(x,y)$ можно рассматривать как алгебраические операции на X.

• **Булевы операции.** Еще один важнейший класс примеров связан с булевыми операциями над множествами. Пусть Z – произвольное множество и $X = 2^Z$. Тогда на X определены операции **объединения** $f(A,B) = A \cup B$, **пересечения** $f(A,B) = A \cap B$, **разности** $A \setminus B$ и **симметрической разности** $A \triangle B$.

• **Пропозициональные связки.** Бинарные пропозициональные связки $\&$, $\vee$, $\Longrightarrow$, $\Longleftrightarrow$ являются бинарными операциями на множестве высказываний.

• **НОД и НОК.** Пусть $X = \mathbb{N}$ – множество натуральных чисел, а $\operatorname{lcm}(x,y)$ и $\gcd(x,y)$ – наименьшее общее кратное и наибольший общий делитель элементов $x, y \in \mathbb{N}$.

• **Максимум и минимум функций.** Пусть $X = \mathbb{R}^{\mathbb{R}}$ – множество вещественнозначных функций вещественного аргумента. Определим функции $f \cup g$ и $f \cap g$, полагая

$$(f \cup g)(x) = \max(f(x), g(x)), \qquad (f \cap g)(x) = \min(f(x), g(x)).$$

Функции $f \cup g$ и $f \cap g$ часто называются еще **верхней огибающей** и **нижней огибающей** функций f и g.

Задача. Как вы думаете, почему $\cup$ и $\cap$ обычно не рассматриваются как самостоятельные операции над функциями?

Решение. Дело в том, что они выражаются через бинарную операцию $(f,g) \mapsto f+g$ и унарные операции $f \mapsto -f$ и $f \mapsto |f|$:

$$f \cup g = \frac{1}{2}(f+g+|f-g|), \qquad f \cap g = \frac{1}{2}(f+g-|f-g|).$$

Комментарий. А зря, так как существуют важные классы функций, замкнутые относительно этих операций, но не относительно сложения.

А вот и совместное обобщение пяти предыдущих примеров.

• **Супремум и инфимум в решетке.** Пусть X – какая-то решетка, а $f(x,y) = x \vee y$ или $f(x,y) = x \wedge y$ – точная верхняя и нижняя грани пары (x,y), соответственно (называемые по английски 'join' и 'meet' элементов x и y). В зависимости от контекста эти операции могут обозначаться также как $\max(x,y)$ и $\min(x,y)$, или как $\sup(x,y)$ и $\inf(x,y)$.

§ 5. Композиция

Еще одним важнейшим примером алгебраической операции – вероятно, *самым* фундаментальным примером – является композиция.

• **Композиция отображений.** Пусть вначале $X = \mathrm{Map}(Z,Z)$ – множество отображений Z в себя. Тогда, как мы знаем, для любых двух отображений $f, g \in X$ определена их композиция $f \circ g \in X$. Напомним, что значение композиции $f \circ g$ на элементе $z \in Z$ определяется как $(f \circ g)(z) = f(g(z))$.

• **Композиция отношений.** То же самое относится и к множеству $Y = \mathrm{Rel}(Z)$ внутренних бинарных отношений на Z. В § 3 мы определили композицию (произведение) двух отношений $R \bullet S$, которая всюду определена на Z. Напомним, что $R \bullet S = \{(x,y) \in Z \times Z \mid \exists z \in Z, (x,z) \in R, (z,y) \in S\}$.

Есть много классов отображений, **замкнутых относительно композиции**, и в дальнейшем нам часто придется рассматривать некоторые из этих классов. Например:

• композиция двух инъекций, сюръекций или биекций снова есть инъекция, сюръекция или биекция, соответственно.

• В случае, когда Z является частично упорядоченным множеством, композиция двух монотонных отображений есть монотонное отображение.

• В случае, когда Z является абелевой группой или векторным пространством, композиция двух линейных отображений есть линейное отображение.

• В случае, когда Z является топологическим пространством, композиция двух непрерывных отображений есть непрерывное отображение.

Нам встретится и много других подобных примеров.

§ 6. Операции над многочленами

Обозначим через $K[x]$ кольцо многочленов над полем K (как всегда, можно считать, например, что K – поле рациональных, вещественных или комплексных чисел). Тремя наиболее известными операциями над многочленами являются сложение, умножение и композиция:

• **Сложение многочленов**. Пусть $f = a_0 + a_1 x + \ldots + a_m x^m$ и $g = b_0 + b_1 x + \ldots + b_n x^n$ – два многочлена с коэффициентами из некоторого поля K. Тогда **сумма** $f + g$ многочленов f и g, определяется как $f = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_l + b_l)x^l$, где $l = \max(m,n)$.

• **Умножение многочленов**. Умножение одночленов определяется как $a_m x^m b_n x^n$ и продолжается на все многочлены по линейнойсти. Для тех же многочленов f, g, что и выше, их **произведение** равно $fg = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \ldots + a_m b_n x^{m+n}$.

Сложение и умножение известны из школьной программы и мы детально изучим их в следующих главах, поэтому сейчас мы опишем несколько менее известных операций, из которых чаще всего используется композиция.

• **Композиция многочленов** тесно связана с композицией функций и, в действительности, для перечисленных выше полей *является* частным случаем композиции функций (но имеет смысл и в более общей ситуации, когда многочлен не определяется задаваемой им полиноминальной функцией $c \mapsto f(c)$). А именно, **композиция** $f \circ g$ многочленов $f, g \in K[x]$ определяется как результат подстановки многочлена g в многочлен f. Например, если $g = x^2 - 2x + 1$, а $f = x^3 + 3x + 1$, то $f \circ g = (x^2 - 2x + 1)^3 + 3(x^2 - 2x + 1) + 1$.

Следующие операции менее известны, но они реально возникают в алгебраической геометрии, K-теории и теории характеристических классов[235,236,237]. Чтобы не обсуждать некоторые технические детали, мы определим эти операции только для **нормированных** многочленов, т.е. таких многочленов, старший коэффициент которых равен 1. Нормированный многочлен однозначно определяется набором своих корней.

• **Симметрической суммой** многочленов f и g называется многочлен $f \boxplus g$, корни которого являются попарными *суммами* корней многочленов f и g, с учетом кратности.

• **Тензорным произведением** многочленов f и g называется многочлен $f \otimes g$, корни которого являются попарными *произведениями* корней многочленов f и g, с учетом кратности.

Из формул Виета и теории симметрических многочленов вытекает, что в действительности коэффициенты многочленов $f \boxplus g$ и $f \otimes g$ выражаются через коэффициенты f и g.

§ 7. Операции над матрицами

Одной из основных целей нашего курса будет систематическое изучение операций над матрицами. Обозначим через $M(m, n, K)$ множество всех $m \times n$ **матриц** с коэффициентами из поля K, которые *изображаются* таблицами элементов K с m строками и n столбцами. Пара чисел (m, n) называется **размером** матрицы $x \in M(m, n, K)$. Матрица, для которой $m = n$ называется **квадратной**, Множество $M(n, n, K)$ квадратных матриц обозначается через $M(n, K)$. В этом случае n называется **порядком** или **степенью**. Например, 2×2-матрица с коэффициентами из поля K *изображается* таблицей

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad a, b, c, d \in K.$$

Вот некоторые наиболее часто используемые операции над матрицами.

• **Сумма матриц.** Матрицы из $M(m, n, K)$ можно *поэлементно* складывать, именно эта операция и называется **сложением матриц**

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}.$$

[235] Д.Мамфорд, Лекции о кривых на алгебраической поверхности, – М., Мир, 1968, с.1–236, лекция 26, в особенности стр. 220–221.

[236] Ф.Хирцебрух, Топологические методы в алгебраической геометрии, М., Мир, 1973, с.1–280, например, стр.88.

[237] Дж.Милнор, Дж.Сташеф, Характеристические классы, – М., Мир, 1979, с.1–371., стр.76–77

• **Произведение Адамара.** Матрицы из $M(m,n,K)$ можно поэлементно умножать, такое умножение обычно называется **умножением Адамара**:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} * \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae & bf \\ cg & dh \end{pmatrix}.$$

• **Произведение матриц.** Однако обычно, говоря об **умножении матриц**, имеют в виду следующую операцию на $M(n,K)$, явно определенную в начале 1840-х годов Артуром Кэли:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}.$$

Впрочем, в неявном виде эта операция появлялась еще у Эйлера, а Гаусс в связи с композицией квадратичных форм специально подробно рассматривал именно случай матриц размера 2×2.

В действительности имеется много других операций над матрицами, которые по отношению к матрицам фиксированных порядков являются внешними операциями, но становятся внутренними операциями на множестве *всех* матриц (всевозможных порядков!) с коэффициентами из K.

§ 8. Производные операции

Если на множестве задано несколько различных законов композиции, то комбинируя их можно строить новые законы композиции, среди которых встречаются и довольно интересные. В главе III мы рассмотрим *важнейшую* из таких производных операций – **свертку**, а пока приведем несколько элементарных примеров.

• **Присоединенное умножение.** Пусть, например, X – множество элементов какой-то природы, на котором заданы сложение '+'и умножение '$\times$'. Тогда можно рассмотреть операцию $x \bullet y = x+y+xy$, называемую **присоединенным умножением**.

• **Коммутирование и антикоммутирование.** Особенно важны следующие две производные операции, имеющие специальные наименования: **коммутирование** $[x,y] = xy - yx$ и **антикоммутирование** $x \circ y = (xy+yx)/2$. Конечно, на множестве чисел, где умножение коммутативно, эти операции не представляют никакого интереса, но вскоре мы введем объекты, которые можно складывать и умножать, так, что при этом умножение некоммутативно, т.е. $xy \neq yx$. Наиболее известным примером таких объектов являются, конечно, матрицы, но нам встретится и много других примеров. В этих случаях операции коммутирования и антикоммутирования приводят к важным новым алгебраическим структурам.

• **Лоренцево сложение.** Пусть $\mathbb{I} = [0,1]$ – единичный отрезок вещественной оси. На множестве $\mathbb{I}$ вводится довольно интересная операция, называемая **Лоренцевым сложением**, которая постоянно используется в специальной теории относительности:

$$u \boxplus v = \frac{u+v}{1+uv}, \qquad u,v \in \mathbb{I}.$$

Разумеется, это обычная релятивистская формула сложения скоростей, записанная в системе единиц, в которой скорость света c равна 1 (а чему еще может быть равна скорость света, если измерять время в метрах, а расстояние – в секундах?). Например, $1 \boxplus 1 = 1$, т.е. если пустить с космического корабля, движущегося со скоростью света, луч света в направлении его движения, то он все равно будет двигаться со скоростью света, а не с удвоенной скоростью света. Ясно, что Лоренцево сложение коммутативно.

• **Средние.** Сейчас мы сопоставим каждому вещественному числу $p \in \mathbb{R}$ некоторую внутреннюю бинарную операцию на множестве $\mathbb{R}_+$. При $p \neq 0$ **средним p-го порядка** двух положительных вещественных чисел x и y называется число

$$S_p(x,y) = \sqrt[p]{\frac{x^p + y^p}{2}}.$$

Заметим, что это один из случаев, когда для записи алгебраической операции используется префиксная, а не инфиксная запись. Например,

$$S_1(x,y) = \frac{x+y}{2}, \qquad S_2(x,y) = \sqrt{\frac{x^2+y^2}{2}}, \qquad S_{-1}(x,y) = \frac{2xy}{x+y}$$

известны как **среднее арифметическое**, **среднее квадратическое**, и **среднее гармоническое**, соответственно. Приведенная выше формула не определяет $S_0(x,y)$, но, изучая предел $S_p(x,y)$ при p стремящемся к 0, легко понять, что единственный разумный способ определить среднее 0-го порядка чисел x и y состоит в том, чтобы положить его равным их **среднему геометрическому** $S_0(x,y) = \sqrt{xy}$.

• **Параллельное сложение.** С гармоническим средним теснейшим образом связана другая операция, называемая **параллельным сложением**. А именно, для $x, y \in \mathbb{R}_+$ положим $x\|y = (x^{-1} + y^{-1})^{-1}$. Это название и обозначение обязаны своим происхождением тому, что параллельная сумма возникает в электротехнике как значение сопротивления двух резисторов с сопротивлениями x и y при параллельном соединении. В школьном курсе параллельное сложение возникает при изучении логарифмов:

$$\log_{xy}(z) = \log_x(z) \| \log_y(z).$$

Размышлизм: почему производные операции могут быть интересны? На первый взгляд изучение производных операций не дает ничего нового по сравнению с исходными операциями, через которые они выражаются. Однако в действительности это не совсем так. Это связано с тем, что хотя подмножество Y множества X, на котором определены наши операции, может быть не замкнуто относительно исходных операций, оно вполне может быть замкнуто относительно производных операций. Пусть, например, $X = M(n,K)$ – множество всех квадратных матриц степени n над полем K, а $Y = \mathfrak{sl}(n,K)$ – его подмножество, состоящее из всех матриц со следом 0, $\mathfrak{sl}(n,K) = \{x \in M(n,K) \mid \mathrm{tr}(x) = 0\}$. Если $\mathrm{tr}(x) = \mathrm{tr}(y) = 0$, то, вообще говоря, неверно, что $\mathrm{tr}(xy) = 0$. Тем не менее, $\mathrm{tr}(xy) = \mathrm{tr}(yx)$, поэтому $\mathrm{tr}([x,y]) = 0$. Тем самым, $\mathfrak{sl}(n,K)$ не замкнуто относительно умножения, но замкнуто относительно коммутирования – это один из самых важных примеров простых алгебр Ли.

§ 9. Операции, встречающиеся в анализе и геометрии

Все области математики **кишат** алгебраическими операциями, однако, поскольку аналисты и некоторые геометры относятся к алгебре с подозрением и все еще не выучили терминов 'идеал' и 'гомоморфизм', в этих областях не принято задумываться над тем, что во многих случаях использование даже простейших сведений из алгебры позволило бы радикально упростить традиционные изложения большинства разделов анализа, римановой геометрии и дифференциальных уравнений. Начинающий должен пропустить этот параграф, но преподавателю прочесть его полезно.

1. Свертки вещественных функций. Будем для определенности рассматривать вещественнозначные функции вещественного аргумента, хотя эта конструкция может обобщаться во многих различных направлениях. Для двух таких функций $f, g \in \mathrm{Map}(\mathbb{R}, \mathbb{R})$ определим их **свертку** $f * g$ равенством

$$(f * g)(x) = \int_{-\infty}^{+\infty} f(x-y)g(y)\,dy.$$

Мы предоставляем читателю самостоятельно уточнить, какому классу должны принадлежать функции f и g, чтобы интеграл в определении свертки сходился и получающаяся функция снова принадлежала этому же классу. В различных разделах анализа, математической физики и теории вероятностей рассматривается множество вариантов свертки (свертки мер, обобщенных функций и т.д.). Например, в операционом исчислении интеграл в этом определении обычно берется не от $-\infty$ до $+\infty$, а от 0 до x, чему есть свои глубокие причины. С точки зрения алгебры удобнее нормировать свертку, домножив интеграл справа на $(2\pi)^{-1}$.

2. Композиция Вольтерра. В теории интегральных уравнений рассматриваются так называемые **ядра**, являющиеся некоторыми функциями двух вещественных переменных с вещественными значениями. Вольтерра изучал композицию двух таких функций $K, L \in \mathrm{Map}(\mathbb{R}\times\mathbb{R}, \mathbb{R})$ определенную посредством

$$(K \circ L)(x, y) = \int K(x, z)L(z, y)\,dz.$$

Снова мы предоставляем читателю самостоятельно уточнить, какому классу должны принадлежать функции K и L, чтобы интеграл сходился и получающаяся функция снова принадлежала тому же классу. Заметим, что это определение пародирует определение умножения матриц, которое мы вскоре подробно изучим.

3. Скобки Пуассона. В теории дифференциальных уравнений и классической механике широко используется еще один замечательный закон композиции. Пусть $f(q, p)$ и $g(q, p)$ – две функции от $2n$ переменных $q = (q_1, \ldots, q_n)$ и $p = (p_1, \ldots, p_n)$. Тогда **скобкой Пуассона** функций f и g называется функция

$$\{f, g\} = \sum_{i=1}^{n} \left(\frac{\partial f}{\partial q_i}\frac{\partial g}{\partial p_i} - \frac{\partial f}{\partial p_i}\frac{\partial g}{\partial q_i} \right).$$

Обозначение q и p подсказано классической механикой, где в качестве q и p выступают **канонические переменные**[238], известные широким народным кругам под именами 'координат' и 'импульсов'.

4. Сложение и коммутирование векторных полей. Пусть M – дифференцируемое многообразие (можно для простоты ограничиться многообразиями класса C^∞). Обозначим через $\mathrm{Vect}(M)$ множество дифференцируемых векторных полей на M. Тогда на $\mathrm{Vect}(M)$ определены два бинарных закона композиции: сложение и коммутирование (скобка Ли) векторных полей. Напомним, что элементы $\mathrm{Vect}(M)$ можно мыслить как дифференциальные операторы первого порядка в кольце дифференцируемых функций на M. При этом, если $x_1, \ldots, x_n$ – локальные координаты, а f_i, g_i – дифференцируемые функции этих координат,

[238] В.И.Арнольд, Математические методы классической механики, 1979, § 40

то **скобка Ли** векторных полей $X = \sum f_i \dfrac{\partial}{\partial x_i}$ и $Y = \sum g_i \dfrac{\partial}{\partial x_i}$ описывается следующим образом[239]:

$$[X,Y] = \sum_{i=1}^{n} \sum_{j=1}^{n} \left(f_j \frac{\partial g_i}{\partial x_j} - g_j \frac{\partial f_i}{\partial x_j} \right),$$

5. Линейная связность ('ковариантная производная') и кручение. Предшествующий пример относится к дифференциальной топологии. Собственно дифференциальная геометрия начинается с введения еще одного закона композиции на $\mathrm{Vect}(M)$. Пусть, как и в предыдущем примере, M – дифференцируемое многообразие. **Линейной связностью** на M называется закон композиции

$$\nabla : \mathrm{Vect}(M) \times \mathrm{Vect}(M) \longrightarrow \mathrm{Vect}(M),$$

удовлетворяющий некоторым естественным предположениям[240]. При этом векторное поле $\nabla(X,Y)$ обычно обозначается $\nabla_X(Y)$ и называется **ковариантной производной** поля Y вдоль поля X. Именно операции $[X,Y]$ и $\nabla(X,Y)$ и связывающие их тождества придают основам римановой геометрии отчетливо алгебраический характер, затемняемый в традиционных изложениях координатными обозначениями. Громадную роль в геометрии играют различные производные операции, многие из которых имеют специальные названия. Например, закон композиции

$$T(X,Y) = \nabla(X,Y) - \nabla(Y,X) - [X,Y]$$

известен как **тензор кручения** (см. также § ?, где вводится тензор кривизны).

[239]Д.Громол, В.Клингенберг, В.Мейер Риманова геометрия в целом – 1971, § 1.9).

[240]ibid., § 2.1.

Тема 2: ВАЖНЕЙШИЕ ТОЖДЕСТВА

Истинное отличие алгебраических операции от всех прочих отображений состоит в том, что обычно предполагается, что они удовлетворяют чрезвычайно простым **функциональным уравнениям**, которые в алгебре обычно называются **тождествами**[241]. Особенно подробно рассмотрены тождества **ассоциативности** и **коммутативности**, и два наиболее важных тождества, в которые входят две операции – **дистрибутивность** и **тождество Якоби**.

§ 1. Ассоциативность

> Монтировал Сюропов динамично и бескомпромиссно. У него в это время начинал из всех (извините) интеллектуальных мест хлестать поток сознания. Он был бесспорным непризнанным ассом ассоциативного монтажа. Поэтому он повсюду ассоциировал.
>
> Александр Соловьев, 'Sun-техника'

Наиболее важным **во всей математике** несомненно является тождество ассоциативности.

1. Ассоциативность. Следующее тождество известно нам из начальной школы, где оно обычно называется **сочетательным законом**, термин 'ассоциативность' был введен Гамильтоном в 1843 году.

Определение. *Определенная на множестве X операция $*$ называется* **ассоциативной**, *если $(x * y) * z = x * (y * z)$ для любых $x, y, z \in X$*

В префиксной записи это тождество принимает вид следующего функционального уравнения

$$f(f(x, y), z) = f(x, f(y, z)),$$

или, в форме Лукасевича $ffxyz = fxfyz$.

Примеры ассоциативных операций:

- сложение и умножение чисел,
- сложение и умножение многочленов,
- сложение и умножение матриц,
- композиция функций или отношений,
- объединение и пересечение множеств,
- взятие супремума и инфимума,
- свертка.

В § ? мы обсудим некоторые простейшие следствия ассоциативности и приведем много дальнейших примеров ассоциативных операций.

---

[241] В этой главе обсуждаются лишь несколько простейших тождеств. Кроме них в алгебре используются *сотни* других тождеств. Часть этих тождеств, как, скажем, изучаемые в школе формулы сокращенного умножения, являются следствиями рассмотренных здесь основных тождеств. Например, бином Ньютона есть следствие ассоциативности и коммутативности сложения и умножения и дистрибутивности умножения относительно сложения. Другой тип тождеств – это тождества выделяюцие не новые типы алгебраических систем, а более узкие классы систем данного типа, как, скажем энгелево или бернсайдовы тождества в теории групп. Нужно иметь некий навык вычислений в теории групп, чтобы быть в состоянии оценить, как можно использовать тождества наподобие $xyx^{-1}y^{-1}z = zxyx^{-1}y^{-1}$.

Примеры неассоциативных операций:

- вычитание и деление чисел,
- возведение в степень,
- векторное умножение векторов,
- коммутирование.

В самом деле, $(x-y)-z$, вообще говоря, не равно $x-(y-z)$, а $(x/y)/y$, вообще говоря, не равно $x/(y/z)$. Это еще один очень серьезный аргумент в пользу того, чтобы не рассматривать вычитание и деление в качестве самостоятельных операций! Также и операция возведения в степень неассоциативна, $(z^y)^z \neq x^{(y^z)}$. Интересно, что в этом случае обычный порядок выполнения операции в отсутствие скобок - **правонормированный**, т.е. x^{yz} означает $x^{(y^z)}$, а вовсе не $(z^y)^z$, как было бы естественно ожидать, читая формулы слева направо! Операция векторного умножения удовлетворяет важнейшему аналогу ассоциативности – тождеству Якоби.

Задача. Пусть $*$ – ассоциативная операция на X, а $a \in X$. Докажите, что тогда операция $x \circ y = x * a * y$ ассоциативна.

Задача. Пусть $a = (a_i)$ и $b = (b_i)$ – две бесконечные последовательности, $i \in \mathbb{N}$. Определим **перемешивание** этих последовательностей как последовательность $a\sharp b = (a_1, b_1, a_2, b_2, \dots)$. Будет ли операция $\sharp$ ассоциативной?

Задача. Докажите, что Лоренцево сложение ассоциативно.

Решение. Легко видеть, что как $(u \boxplus v) \boxplus w$, так и $u \boxplus (v \boxplus w)$ равны

$$\frac{u+v+w+uvw}{1+uv+uw+vw.}$$

Задача. Докажите, что параллельное сложение ассоциативно.

Решение. Легко видеть, что как $(u\|v)\|w$, так и $u\|(v\|w)$ равны

$$\frac{uvw}{uv+uw+vw.}$$

2. Обобщенная ассоциативность. Предположим, что заданная на X операция ассоциативна. В этом случае мы можем определить произведение любых $n \geq 3$ элементов X по индукции. А именно, если $x_1, \dots, x_n \in X$, то положим $x_1 \cdots x_n = (x_1 \cdots x_{n-1})x_n$. Это определение равносильно **левонормированной** расстановке скобок в произведении, т.е., например, для $n = 5$ имеем $x_1x_2x_3x_4x_5 = (((x_1x_2)x_3)x_4)x_5$.

Задача. Глядя на определение Лоренцева сложения и параллельного сложения и на формулы для $u \boxplus v \boxplus w$ и $u\|v\|w$, полученные в предыдущих задачах, угадайте формулы для $u_1 \boxplus \dots \boxplus u_n$ и $u_1\| \dots \|u_n$.

Но ведь в произведении пяти множителей можно поставить скобки и иначе, скажем, так: $(x_1x_2)(x_3(x_4x_5))$. Получится ли при этом тот же результат, что и при левонормированнной расстановке скобок? Ассоциативность утверждает, что для произведения трех множителей это действительно так. Общий случай, называемый **обобщенной ассоциативностью**, легко получается отсюда по индукции.

Теорема (Allgemeine Klammerregel). *Предположим, что операция в X ассоциативна. Тогда результат умножения n элементов X не зависит от расстановки скобок.*

Доказательство. (см. Кострикин, Гл. 4, Теорема 1). Доказываем предложение по индукции. Для $n = 1, 2$ утверждение теоремы очевидно, а для $n = 3$ это в точности обычная ассоциативность. Предположим теперь, что для всех значений $m < n$ предложение уже доказано, так что при любой расстановке скобок произведение любых $m < n$ элементов равно их левонормированному произведению. Мы хотим доказать, что тогда и любое произведение w элементов $x_1, \dots, x_n$ равно их левонормированному произведению. Чтобы порядок действий был полностью определен, такое произведение должно содержать ровно $n - 2$ пары скобок. Посмотрим на те пары скобок, в которые попадает x_n, причем в первую очередь на самую внешнюю из них. Если x_n не охватывается ни одной парой скобок, то w имеет вид $w = ux_n$, где u – некоторое произведение $x_1, \dots, x_{n-1}$, и можно воспользоваться индукционным предположением. Если же внешняя пара скобок охватывает x_n, то w имеет вид $w = uv$, где u есть некоторое произведение $x_1, \dots, x_m$, $1 \leq m \leq n-2$, а v есть некоторое произведение $x_{m+1}, \dots, x_n$. Произведение v имеет длину $n - m < n$ и по индукционному предположению его можно переписать в виде $v = yx_n$, где y есть некоторое произведение $x_{m+1}, \dots, x_{n-1}$ (в действительности y можно считать левонормированным, но это не имеет никакого значения). Таким образом, $w = uv = u(yx_n) = (uy)x_n$ и мы снова попали в первый случай.

3. Проверка ассоциативности по таблице Кэли. Проверка ассоциативности операции по ее таблице Кэли занятие чрезвычайно неблагодарное. Фактически оно сводится к следующему. Обозначим операцию, ассоциативность которой мы хотим проверить, умножением. Фиксируем элемент z множества X и введем на X две производные операции: $x *_z y = (xz)y$ и $x \circ_z y = x(zy)$. Фактически проверка ассоциативности сводится к проверке совпадения таблиц $*_z$ и $\circ_z$ для всех элементов $z \in X$, а это чудовищно утомительное дело даже для случая, когда X содержит 4 или 5 элементов (см., например, А.Клиффорд, Г.Престон "Алгебраическая теория полугрупп", 1972, § 1.2). В действительности гораздо более интеллигентным[242] способом проверки ассоциативности является построение представлений, т.е. вложение рассматриваемой системы в какую-нибудь другую систему (отображения, отношения, матрицы), ассоциативность которой известна из общих соображений.

4. Ассоциативные тройки. Даже если операция на множестве X неассоциативна, могут найтись тройки $x, y, z \in X$ такие, что $(xy)z = x(yz)$. Такие тройки обычно называются **ассоциативными**, хотя было бы правильнее называть их **ассоциирующими**.

Задача. Найти все ассоциирующие тройки натуральных чисел относительно потенцирования: $(m^n)^p = m^{(n^p)}$.

Ответ. Вот все такие тройки: $(1, n, p)$, $(m, n, 1)$ и $(m, 2, 2)$.

А вот более экзотический и гораздо более трудный пример. Рассмотрим биномиальный коэффициент $\binom{n}{m}$ как бинарную операцию на $\mathbb{N}$. Для каких троек натуральных чисел имеет место равенство

$$\left(\binom{n}{m}\right) = \binom{n}{\binom{m}{l}}?$$

Этот курьезный вопрос рассматривал Соломон Голомб[243]. Он нашел пять типов таких троек

[242] Marked or characterised by intelligence.

[243] S.W.Golomb, Iterated binomial coefficients, – Amer. Math. Monthly, 1980, November, p.719–727.

(l, m, n), а именно,

(1) $(1, m, n)$, для всех m, n;
(2) $(\binom{n}{m}, m, n)$, при $l > m$;
(3) (l, m, n), при $m > l, n$;
(4) $(l, l, l + 1)$, для всех $l > 1$;
(5) (l, m, m), для всех $1 < l < m - 1$.

Скорее всего, не существует ни одной ассоциирующей тройки (l, m, n), для которой $1 < l < m < n$, но это не доказано.

§ 2. Числа Каталана и числа Родригеса

> There is nothing new under the Sun, but there are a lot of old things we do not know.
>
> Ambrose Bierce

Естественно возникает вопрос, сколько произведений можно составить из $n+1$ элементов, не предполагая, что закон композиции ассоциативен.

1. Числа Каталана. Расстановка $n - 1$ пар скобок, при которой произведение $x_1 \dots x_{n+1}$ становится однозначно определенным, называется **правильной**. Ясно, что для 2 множителей имеется единственная правильная расстановка скобок, а именно, x_1x_2, для 3 множителей таких расстановок две, а именно, $(x_1x_2)x_3$ и $x_1(x_2x_3)$, а для 4 множителей их уже пять, а именно, $((x_1x_2)x_3)x_4$, $(x_1(x_2x_3))x_4$, $(x_1x_2)(x_3x_4)$, $x_1((x_2x_3)x_4)$, $x_1(x_2(x_3x_4))$. Читатель без труда убедится, что имеется 14 различных правильных расстановок скобок для 5 множителей и 42 для 6 множителей. А каков ответ в общем случае? Следующий результат был доказан в 1838 году Каталаном[244].

Теорема. *Количество неассоциативных произведений, которые можно образовать из* $n + 1$ *сомножителя в фиксированном порядке, равно* n*-му* **числу Каталана**

$$C_n = \frac{1}{n+1}\binom{2n}{n} = \frac{1}{2n+1}\binom{2n+1}{n}.$$

Числа C_n называются **числами Каталана**, они возникают в *десятках* самых различных задач алгебры, теории чисел, комбинаторики и комбинаторной геометрии. Мы докажем эту теорему двумя способами, через рекуррентные соотношения и непосредственно.

В `Mathematica` числа Каталана определяются в пакете 'Комбинаторные функции', который подгружается командой

```
<<DiscreteMath‘CombinatorialFunctions‘.
```

После этого оценка выражения `CatalanNumber[n]` возвращает n-е число Каталана. Укажем несколько первых членов этой последовательности: $C_0 = 1$, $C_1 = 1$, $C_2 = 2$, $C_3 = 5$, $C_4 = 14$, $C_5 = 42$, $C_6 = 132$, $C_7 = 429$, $C_8 = 1430$, $C_9 = 4862$, $C_{10} = 16796$, $C_{11} = 58786$, $C_{12} = 208012$.

2. Индукционное доказательство. Для перехода к записи Лукасевича и проведения индукции по n нам будет удобно поставить для каждого произведения еще одну пару скобок, а именно, скобки вокруг всего произведения. Таким образом, мы считаем, что в правильной расстановке скобок в произведении $n + 1$ сомножителя n пар скобок. Например, для $n = 3$ мы теперь запишем произведения так: $(((x_1x_2)x_3)x_4)$, $((x_1(x_2x_3))x_4)$, $((x_1x_2)(x_3x_4))$, $(x_1((x_2x_3)x_4))$, $(x_1(x_2(x_3x_4)))$. Теперь, чтобы перейти к записи Лукасевича, достаточно убрать все *правые*, а, чтобы перейти к обратной записи Лукасевича, – все *левые* скобки и заменить оставшиеся скобки на знак операции. Кроме того, поскольку нас интересует только расстановка скобок, а не сами операнды, мы можем обозначить *все* операнды через x. Например, если обозначить операцию через f, то те же самые произведения запишутся как $fffxxxx$, $ffxfxxx$, $ffxxfxx$, $fxfffxxx$, $fxfxfxx$ для записи Лукасевича и как $xxfxfxf$, $xxxffxf$, $xxfxxff$, $xxxfxff$, $xxxxfff$ для обратной записи Лукасевича. В обратной записи

[244] Eugène–Charles Catalan (1814-1894) бельгийский математик

Лукасевича правильная расстановка скобок в произведении $n+1$ множителя соответствует такому слову длины $2n+1$ в алфавите x, f, что каждый начальный фрагмент этого слова содержит больше букв x, чем букв f. Такие слова будут называться **правильными** (well-formed).

Доказательство. Всего имеется $\binom{2n+1}{n}$ возможных слов, в которые буква x входит $n+1$ раз, а буква f входит n раз. Пусть w – любое такое слово. Мы утверждаем, что имеется ровно одна циклическая перестановка слова w являющаяся правильным словом. Таким образом, число различных расстановок скобок равно $\frac{1}{n+1}\binom{2n+1}{n}$, как и утверждалось.

Это доказывается индукцией по n. В самом деле, для $n=1$ это, очевидно, так: из слов xxf, xfx, fxx ровно одно, а именно xxf, является правильным. Пусть теперь w – слово длины $n>2$. Покажем, прежде всего, что существует правильная циклическая перестановка слова. В самом деле, само слово w или, если $w = f\dots fx\dots x$, то слово `RotateRight[`w`]` содержит фрагмент вида xf. Вычеркнем первое слева вхождение xf (в случае $w = f\dots fx\dots x$ вычеркнем самое левое f и самое правое x). Мы получаем слово z длины $2n-1$, в которое x входит n раз, а f входит $n-1$ раз. По индукционному предположению существует циклическая перестановка слова z, являющаяся правильным словом. Врисовывая в эту перестановку фрагмент xf на то место, откуда он был вычеркнут, мы получаем правильную циклическую перестановку исходного слова. Например, для $w = fxxffxx$, вычеркивание первого фрагмента xf дает нам слово $z = fx{-}fxx = fxfxx$. Правильной циклической перестановкой этого слова является $xxfxf = xxfx{-}f$. Снова врисовывая сюда xf мы получаем слово $xxfxxff$, являющееся правильной циклической перестановкой исходного слова w.

Для доказательства единственности заметим, что правильная циклическая перестановка слова w не может начинаться ни с буквы x, ни с буквы f вычеркнутой пары. Поэтому вычеркивание любого фрагмента xf из правильного слова снова дает правильное слово. Если бы у w было две правильных циклических перестановки, то вычеркивание одного и того же фрагмента xf из каждого из них приводило бы к двум правильным циклическим перестановкам слова z длины $2n-1$, что невозможно по индукционному предположению.

Комментарий. Это доказательство является парафразом доказательства из статьи Дэвида Сингмастера[245], который, в свою очередь, отмечает, что это специализация идеи Зильбергера. По существу то же самое, но чуть сложнее оформленное рассуждение чуть более общего факта приводится в[246] со ссылкой на работу Джорджа Рени 1960 года. В действительности, найти первоисточник затруднительно, так как это рассуждение должно быть хорошо известно специалистам в области математической статистики. Дело в том, что числа Каталана представляют собой ответ на частный случай проблемы Бертрана[247]. А именно, **проблема Бертрана** (Bertrand ballot problem) состоит в следующем. Предположим, что кандидаты получают m и n голосов, соответственно, причем $m>n$, а голоса считаются по одному. Какова вероятность того, что победитель оказывается впереди на каждом этапе голосования? Приведенное выше рассуждение решает эту проблему в частном случае $m = n+1$. Мы доказали, что вероятность в этом случае равна $1/(2n+1)$. Совершенно аналогичное рассуждение Хилтона и Педерсен[248], связанное с расстановкой скобок в произведениях высших арностей, показывает, что в общем случае вероятность равна $(m-n)/(m+n)$.

3. Рекуррентное соотношение для чисел Каталана. В самом деле, при любом $n \geq 2$ ровно одно умножение лежит вне всех скобок, пусть, скажем, это умножение между x_m и x_{m+1}, где $m = 1, \dots, n-1$. Тогда, так как существует C_{m-1} способов расставить скобки в произведении первых m множителей и C_{n-m} способ расставить скобки в произведении

---

[245] D.Singmaster, An elementary evaluation of the Catalan numbers, – Amer. Math. Monthly, ???, p.366–368.

[246] Р.Грехэм, Д.Кнут, О.Паташник, Конкретная математика, М., Мир, 1988, с.1–703, см. стр.393–395.

[247] В.Феллер, Введение в теорию вероятностей и ее приложения, т.I, М., Мир, 1967, с.1–498, т.I, Гл.3, §§ 1 – 2, числа Каталана, правда без названия, появляются в книге Феллера на страницах 86–88.

[248] P.Hilton, J.Pedersen, Catalan numbers, their generalization and their uses. – Mathematical Intelligencer, 1991, vol.13, N.2, p.64–75.

последних $n-m$ множителей, то

$$\mathrm{C}_n = \mathrm{C}_0\mathrm{C}_{n-1} + \mathrm{C}_1\mathrm{C}_{n-2} + \ldots + \mathrm{C}_{n-1}\mathrm{C}_0.$$

Как хорошо известно, этим рекуррентным соотношением определяется последовательность чисел Каталана, явную формулу для которых легко доказать, **например**, при помощи метода производящих функций, см.[249,250,251,252]. Обозначим через $f(x)$ производящую функцию для чисел Каталана $f = f(x) = C_0 + C_1x + C_2x^2 + \ldots$. Рекуррентное соотношение показывает, что $xf^2 = f - 1$. Решая квадратное уравнение $xf^2 - f + 1 = 0$, получаем

$$f(x) = \frac{1 \pm \sqrt{1-4x}}{2x}.$$

Однако выбор знака + перед корнем невозможен, так как он приводит к ряду Лорана, начинающемуся с $1/x$. Поэтому $f(x) = (1 - \sqrt{1-4x})/2x$. Раскладывая теперь $\sqrt{1-4x}$ по формуле бинома Ньютона, получаем искомую формулу.

Расстановка скобок в произведении $x_1, \ldots, x_n$ называется **вложенной** (nested), если все открывающие скобки стоят перед закрывающими, т.е. если после стирания всех x_i'х остается $(\ldots()\ldots)$. Например, расстановка скобок в произведении $(x_1x_2)(x_3x_4)$ не является вложенной, а все остальные правильные расстановки скобок в произведении четырех элементов вложенные.

Задача. Сколько расстановок скобок являются вложенными в условиях предыдущей задачи?

4. Числа Родригеса. В действительности, гораздо более простой подход к вычислению чисел Каталана был предложен в том же самом 1838 году О.Родригесом[253] в его статье "Sur le nombre des manières d'effectuer un produit de n facteurs".

Теорема. *Количество неассоциативных произведений, которые можно образовать из* $n+1$ *сомножителя в произвольном порядке, равно* n*-му* **числу Родригеса**

$$R_n = 2^n \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1).$$

Доказательство. Ясно, что существует ровно одно произведение одного множителя, так что $R_0 = 1$. Если уже имеется какое-то произведение n множителей, то $n+1$-й множитель можно дорисовать слева или справа от любого из n множителей, либо слева или справа от любого из $n-1$ частичных произведений. Например, дописывая z, из (xy) можно изготовить $((zx)y)$, $((xz)y)$, $(x(zy))$, $(x(yz))$, а также $(z(xy))$ и $((xy)z)$. Дописывая w к $((xy)z)$ получаем $(((wx)y)z)$, $(((xw)y)z)$, $((x(wy))z)$, $((x(yw))z)$, $((xy)(wz))$, $((xy)(zw))$, а также $(w((xy)z))$, $(((xy)z)w)$, $((w(xy))z)$ и $(((xy)w)z)$. Таким образом, количество произведений $n+1$ множителя, содержащих фиксированное произведение n множителей, всегда равно $2(2n-1)$. Это дает нам рекуррентное соотношение $R_n = 2(2n-1)R_{n-1}$.

Теперь мы можем вычислить $R_n =$ `rodrigues[n]` посредством

```
rodrigues[0] = 1; rodrigues[n_]:=2*(2n - 1)*rodrigues[n - 1].
```

Укажем несколько первых членов этой последовательности: $R_0 = 1$, $R_1 = 2$, $R_2 = 12$, $R_3 = 120$, $R_4 = 1680$, $R_5 = 30240$, $R_6 = 665280$, $R_7 = 17297280$, $R_8 = 518918400$, $R_9 = 17643225600$, $R_{10} = 670442572800$, $R_{11} = 28158588057600$, $R_{12} = 1295295050649600$.

Однако совершенно ясно, что числа Каталана и числа Родригеса связаны между собой следующим образом: $C_n = R_n/(n+1)!$. Таким образом, мы получили еще один, значительно более простой способ вычисления чисел Каталана.

---

[249] Р.Грехэм, Д.Кнут, О.Паташник, Конкретная математика, М., Мир, 1988, с.1–703, см. стр.391–393

[250] С.К.Ландо, Лекции о производящих функциях, М., МЦНМО, 2002, 143с.

[251] Р.Стэнли, Перечислительная комбинаторика, М., Мир, 1990

[252] Я.Гульден, Д.Джексон, Перечислительная комбинаторика, М., Наука, 1990

[253] Более известным в русской литературе по комбинаторике под французским псевдонимом Родриг ('формула Родрига') – ну да, конечно, Дон Кишот, traduit librement de l'espagnol!

§ 4. Коммутативность

And you know why four plus minus one
Plus ten is fourteen minus one?
'Cause addition is commutative, right?

Tom Lehrer

Следующим по значению тождеством является тождество коммутативности.

1. Коммутативность. Следующее тождество тоже известно нам из начальной школы, где оно обычно называется **переместительным законом**, термин 'коммутативность' был введен Сервуа в 1815 году.

Определение. *Операция $*$ на множестве X называется* **коммутативной**, *если $x * y = y * x$ для любых $x, y \in X$*

В префиксной записи это тождество принимает вид $f(x, y) = f(y, x)$.

Примеры коммутативных операций:

- сложение и умножение вещественных и комплексных чисел,
- сложение и умножение кардинальных чисел,
- сложение и умножение многочленов,
- сложение векторов и матриц,
- объединение и пересечение множеств,
- взятие супремума и инфимума.

Примеры некоммутативных операций:

- сложение ординальных чисел: $1 + \omega = \omega \neq \omega + 1$,
- возведение в степень: $x^y \neq y^x$,
- композиция функций или отношений,
- композиция многочленов,
- векторное умножение векторов,
- умножение кватернионов,
- умножение матриц.

Вообще, характерной чертой математики начиная с XIX века является неуклонный **отказ** от коммутативности. Скоро мы познакомимся со многими другими объектами, умножение которых некоммутативно: октавами, поливекторами и т.д. Конечно, самыми простыми примерами некоммутативных законов композиции являются вычитание и деление: $x - y \neq y - x$, $x/y \neq y/x$, но мы уже договорились не рассматривать их в качестве самостоятельных операций.

2. Обобщенная коммутативность. Оказывается, если операция ассоциативна и коммутативна, то как расстановка скобок, так и порядок сомножителей в произведении любого конечного числа элементов не имеют значения. В следующем результате S_n обозначает симметрическую группу, т.е. множество всех биекций $\underline{n} = \{1, \dots, n\}$ на себя относительно композиции, см. Главу II.

Теорема. *Предположим, что операция в X ассоциативна и коммутативна. Тогда для любых $x_1, \dots, x_n \in X$ и любой перестановки $\sigma \in S_n$ имеет место равенство*

$$x_{\sigma(1)} \dots x_{\sigma(n)} = x_1 \dots x_n.$$

Доказательство. Обобщенная ассоциативность + порождение S_n фундаментальными транспозициями.

3. Коммутирующие элементы. Даже если операция $*$ некоммутативна, могут найтись такие пары элементов, что $xy = yx$. Такие элементы x и y называются **коммутирующими** или **перестановочными**.

Фантазия. Найти все пары вещественных чисел $x, y \in \mathbb{R}_{>0}$ коммутирующих относительно экспоненцирования, т.е. таких, что $x^y = y^x$. Кроме **тривиальных** решений $x = y$ существуют и нетривиальные решения (например, $2^4 = 4^2$). Если $x^y \neq y^x$, то которое из них больше? Например, попробуйте ответить *без калькулятора*, которое из чисел e^π или π^e больше? Полный ответ на эти и подобные вопросы дает Эйлер в своем "Введении в анализ бесконечно малых".

Задача. Проверьте, что $x = x_s = s^{1/(s-1)}$ и $y = y_s = s^{s/(s-1)}$ коммутируют. Какой выбор t приводит к паре $x_t = y_s$, $y_t = y_s$?

Оказывается (loc. cit.), это **единственный** нетривиальный пример коммутирующих пар. Точки с рациональными координатами получаются здесь при $s = m/(m+1)$ и $s = (m+1)/m$, где $m \in \mathbb{N}$. Пример $x = 4$, $y = 2$ получается, когда мы берем здесь $m = 1$. Выбор $m = 2$ приводит к примеру $\left(\frac{27}{8}\right)^{\frac{9}{4}} = \left(\frac{9}{4}\right)^{\frac{27}{8}}$.

4. Проверка коммутативности по таблице Кэли. Коммутативность умножения xy означает, что оно совпадает с противоположным действием $*$, определяемым посредством $x * y = yx$. Таблица Кэли противоположного действия получается из исходной таблицы заменой строк на соответствующие столбцы и наоборот, т.е. **транспонированием**, или, что то же самое, отражением относительно главной диагонали. Например, таблица для полугруппы правых нулей получается транспонированием из таблицы для полугруппы левых нулей. Так вот, коммутативность эквивалентна симметричности таблицы Кэли, которая, таким образом, не должна меняться при транспонировании.

§ 5. Степени элемента

1. Степени элемента. В частности, если операция $*$ на X ассоциативна, то для любого элемента $x \in X$ и любого натурального числа $n \in \mathbb{N}$ мы можем определить **n-ю степень** x^n элемента x по индукции, полагая $x^1 = x$ и $x^n = x^{n-1} * x$. Однако согласно предложению x равняется произведению n экземпляров x при любой расстановке скобок. В моноиде мы доопределим $x^0 = 1$, а если x обратим, то $x^{-n} = (x^{-1})^n = (x^n)^{-1}$.

Тем самым выполнены обычные тождества $x^{m+n} = x^m * x^n$ и $(x^m)^n = x^{mn}$. Это наводит на мысль определить степень более интеллигентным способом, например, так:

$$x^n = \begin{cases} \left(x^{n/2}\right)^2, & \text{если } 2|n, \\ x^{n-1} * x, & \text{иначе.} \end{cases}$$

С точки зрения чистой математики отличие этого определения от предыдущего невелико и раньше математики редко задумывались о такого рода вещах. Однако с точки зрения компьютера разница **огромна**: традиционное определение требует $n-1$ умножения для вычисления x^n, в то время как даже самая поверхностная его модификация сразу снижает число умножений до не более,

чем $2\log_2 n$ (худший случай реализуется для $n = 2^m - 1$). Характерной чертой алгебры последних трех десятилетий является все возрастающее внимание к такого рода алгоритмическим вопросам, в связи со все более глубоким проникновением компьютеров в чисто теоретические исследования.

В случае, когда операция на X не только ассоциативна, но и коммутативна (точнее, если x и y коммутируют), очевидно еще одно тождество, а именно, $(xy)^n = x^n y^n$. Таким образом в этом случае отображение $\mathrm{pow}_n : x \mapsto x^n$ является **эндоморфизмом** X.

В аддитивной нотации степень x^m обозначается обычно через mx и называется **целочисленным кратным**[254] x. С учетом коммутативности обычные тождества для степеней перепишутся следующим образом: $1x = x$, $(m+n)x = mx + nx$, $(mn)x = m(nx)$, $m(x+y) = mx + my$. Мы снова увидим их в такой форме когда будем определять модули в векторные пространства!

2. Структура множества степеней. Пусть X – множество с ассоциативной операцией, $x \in X$. Ясно, что если множество степеней $x^{\mathbb{N}} = \{x^n, n \in \mathbb{N}\}$ бесконечно, то отображение $\mathbb{N} \longrightarrow x^{\mathbb{N}}$, $n \mapsto x^n$ является биекцией (проверьте!) Сейчас мы изучим структуру множества степеней $x^{\mathbb{N}}$ в том случае, когда оно конечно. Оказывается, что в этом случае множество $x^{\mathbb{N}}$ представляет собой *группу с хвостиком*. Напомним, что элемент $e \in X$ называется **идемпотентом**, если $e^2 = e$.

Теорема. *Предположим, что множество $x^{\mathbb{N}}$ степеней элемента $x \in X$ конечно. Тогда в нем существует единственный идемпотент x^l. При этом x^l представляет собой нейтральный элемент множества $G = \{x^m, m \leq l\}$, а все элементы множества G обратимы.*

Доказательство. Единственность идемпотента x^l очевидна. В самом деле, пусть x^l и x^m два идемпотента. Тогда $x^l = x^{lm} = x^{ml} = x^m$. Для доказательства существования заметим, что из конечности множества $x^{\mathbb{N}}$ вытекает существование таких $l \neq m$, что $x^l = x^m$. Рассмотрим лексикографически наименьшую пару $(h, h+k)$ такую, что $x^h = x^{h+k}$. Ясно, что тогда для любого $l \geq h$ имеем $x^l = x^{l+k} = x^{l+2k} = \ldots$. Возьмем наименьшее $l \geq h$ кратное k, пусть скажем, $l = ks$. Ясно, что $e = x^l = (x^k)^s$ идемпотент, в самом деле, $e^2 = x^{2l} = x^{l+ks} = x^l$. По той же причине x^l является нейтральным элементом в G, в самом деле, уже $x^k x^m = x^m = x^m x^k$, но x^k может не принадлежать G. Дополняя показатель степени m до ближайшего кратного k большего $m+l$, мы видим, что все x^m обратимы в G.

§ 5. Дистрибутивность

1. Дистрибутивность. В школьном курсе встречаются еще два важнейших тождества, в которых участвуют **две** алгебраических операции. Рассмотрим множество X с операциями $*$ и $\circ$.

Определение. *Определенная на множестве X операция $*$ называется* **дистрибутивной слева** *относительно $\circ$, если*

$$x * (y \circ z) = (x \circ y) * (x \circ z)$$

[254] не путать скалярные кратные с кратными в X!

и **дистрибутивной справа** *относительно* $\circ$*, если*

$$(x \circ y) * z = (x \circ z) * (y \circ z)$$

для любых $x, y, z \in X$*.*

Если $*$ дистрибутивно относительно $\circ$ как слева, так и справа, говорят о **двусторонней дистрибутивности** или просто о **дистрибутивности** $*$ относительно $\circ$ (в школе здесь говорилось о 'распределительном законе').

Если операция $*$ коммутативна, то для проверки дистрибутивности $*$ относительно $\circ$ достаточно проверить одностороннюю дистрибутивность. Приведем некоторые примеры, дальнейшие примеры встретятся нам в Главе III.

Примеры двусторонне дистрибутивных операций:

• Умножение чисел дистрибутивно относительно сложения: $x(y+z) = xy+xz$ и $(x+y)z = xz+yz$.

• Умножение дистрибутивно относительно вычитания: $x(y-z) = xy-xz$ и $(x-y)z = xz-yz$.

• Объединение и пересечение дистрибутивны друг относительно друга: $A \cup (B \cap \mathrm{C}) = (A \cap B) \cup (A \cap \mathrm{C})$ и $A \cap (B \cup C) = (A \cup B) \cap (A \cup \mathrm{C})$

• На $\mathbb{R}$ сложение дистрибутивно относительно max и min:

$$x + \max(y,z) = \max(x+y, z+z), \qquad x + \min(y,z) = \min(x+y, z+z).$$

• На $\mathbb{R}_+$ умножение дистрибутивно относительно max и min:

$$x \cdot \max(y,z) = \max(xy, xz), \qquad x \cdot \min(y,z) = \min(xy, xz).$$

• На $\mathbb{R}$ операции max и min дистрибутивны друг относительно друга:

$$\max(x, \min(y,z)) = \min(\max(x,y), \max(x,z)),$$
$$\min(x, \max(y,z)) = \max(\min(x,y), \min(x,z)).$$

Примеры односторонне дистрибутивных операций:

• Деление дистрибутивно относительно сложения справа, но не слева: $(x+y)/z = x/z + y/z$, но $x/(y+z) \neq x/y + x/z$.

• На $\mathbb{N}$ возведение в степень дистрибутивно относительно умножения слева, но не справа: $(xy)^z = x^z y/z$, но $x^{yz} \neq x^y x^z$.

• Пусть X – множество с бинарной операцией $*$. Рассмотрим две операции на множестве отображений X^X: композицию $\circ$ и поточечную операцию $(f * g)(x) = f(x) * g(x)$. Тогда композиция дистрибутивна относительно $*$ слева $(f * g) \circ h = (f \circ h) * (g \circ h)$, но не справа $f \circ (g * h) \neq (f \circ g) * (f \circ h)$,

Примеры недистрибутивных операций:

• Сложение не дистрибутивно относительно умножения: $x + yz \neq (x+y)(x+z)$.

• Взятие супремума и инфимума в решетке X, вообще говоря, не дистрибутивны друг относительно друга. Решетка, в которой выполнены тождества

$x \vee (y \ \& \ z) = (x \ \& \ y) \vee (x \ \& \ z)$ и $x \ \& \ (y \vee z) = (x \vee y) \ \& \ (x \vee z)$, называется **дистрибутивной**[255].

Задача. Пусть K – произвольное поле, а f и g – две функции $K \longrightarrow K$. Напомним, что их суммой и произведением называются функции $f+g$ и fg, полученные применением сложения и умножения к их значениям, т.е. $(f+g)(x) = f(x)+g(x)$ и $(fg)(x) = f(x)g(x)$, соответственно, см. ниже. Верно ли, что композиция функций $f, g \mapsto f \circ g$ дистрибутивна относительно сложения функций? А относительно умножения?

Задача. Показать, что операция взятия суммы множеств по Минковскому дистрибутивна относительно объединения, но, вообще говоря, не пересечения.

Задача. Покажите, что $A + (B \cap C) \subseteq (A+B) \cap (A+\mathrm{C})$ и $(A \cap B) + C \subseteq (A+C) \cap (B+C)$.

Задача. Верно ли, что операция взятия разности по Минковскому дистрибутивна относительно пересечения? А относительно объединения?

Задача. В теории интеграла Даниэля–Стоуна часто используется операция $\curlywedge$, определяемая как

$$f \curlywedge g = \mathrm{sign}(fg)(|f| \cap |g|).$$

Проверьте, будет ли она ассоциативной? Дистрибутивной относительно сложения и вычитания?

§ 6. Нарушение ассоциативности и дистрибутивности в машинной арифметике

> При сложении чисел в столбик сначала снизу вверх, а потом наоборот, вы всегда получите разные суммы.
>
> мадам М.П.Ла Туш, цитируется по[256]

Следующие команды переводят нас режим эмуляции арифметики чисел с плавающей запятой с точностью до 8 значащих цифр, обычной для многих микрокалькуляторов:

```
<< NumericalMath‘ComputerArithmetic‘; SetArithmetic[8]
```

Впрочем, читатель может повторить эти вычисления и на обычном микрокалькуляторе. Оказывается, сложение и умножение компьютерных чисел коммутативны. Отклонение от выполнения других тождеств в программистской практике принято измерять в ульпах. **Ульпом???** (ulp – unit in the last place) называется наименьшее компьютерное число ε такое, что в используемом формате $1+\varepsilon \neq 1$. Например, для точности 8 значащих цифр 1 ульп равен 0.0000001. Несложная оценка ошибки округления[257] показывает, что умножение ассоциативно *с точностью* до двух ульпов относительной погрешности.

А вот с ассоциативностью сложения ситуация подлинно трагическая. Вот несложный пример, в котором ошибка составляет миллионы ульпов. Рассмотрим следующие три компьютерных числа:

```
x=ComputerNumber[10000001], y=-x, z=ComputerNumber[0.51100000]
```

---

[255]Например, классическая теорема Оре (O.Ore, Structures and group theory. II. – Duke Math. J., 1938, vol.4, p.247–269) утверждает, что решетка $X = L(G)$ подгрупп группы G в том и только том случае дистрибутивна, когда G **локально циклическая** (любое конечное множество элементов группы G порождает циклическую подгруппу). В частности, решетка подгрупп конечной группы в том и только том случае дистрибутивна, когда G циклическая.

[256]Д.Э.Кнут, Искусство программирования. Том 2. Получисленные алгоритмы, 3е изд., Вильямс, М.–СПб–Киев, 2000, с.1–828. стр.225

[257]ibid., с.268–269

Теперь вычисление показывает, что $(x \oplus y) \oplus z = 0.51100000$, но $x \oplus (y \oplus z) = 1.0000000$.

Аналогичные примеры легко привести и для дистрибутивности умножения.

В связи с этим многие специалисты предлагают *полностью* отказаться от методов вычислений, численного анализа и использовать только вычисления с целыми числами, (infinite precision arithmetic, error-free calculations). По крайней мере

§ 6. Тождество Якоби

1. Тождество Якоби[258]**.** Пусть теперь на X заданы две операции $*$ и $+$. Говорят, что в X выполняется **тождество Якоби**, если для любых $x, y, z \in X$ имеет место равенство

$$(x * y) * z + (y * z) * x + (z * x) * y = 0.$$

Известный из школьного курса геометрии пример выполнения этого тождества относится к случаю, когда $+$ есть сложение векторов трехмерного пространства, а $*$ есть векторное произведение, обозначаемое обычно $[x, y]$, когда тождество принимает вид

$$[[x, y], z] + [[y, z], x] + [[z, x], y] = 0.$$

Это основное тождество, входящее в определение **алгебр Ли**. Приведем дальнейшие примеры операций удовлетворяющих тождеству Якоби:

- коммутирование в ассоциативной алгебре,
- коммутирование дифференцирований,
- скобка Ли векторных полей,
- скобка Пуассона.

Комментарий. Это замечательное тождество является вариантом **правила Лейбница** дифференцирования произведения, если считать, что дифференциальные операторы и функции, на которых они действуют, живут в одном и том же кольце – а именно в этом и состоит точка зрения алгебр Ли. В теории алгебр Ли это тождество всегда используется вместе с **антикоммутативностью**: $[y, x] = -[x, y]$. В последние 10–15 лет во многих работах тождество Якоби используется **без** предположения антикоммутативности операции $[x, y]$, т.е. непосредственно в форме **тождества Лейбница**

$$[x, [y, z]] = [[x, y], z] + [y, [x, z]].$$

С тождествами Якоби и Лейбница тесно связано **тождество Пуассона**, в котором фигурируют *три* операции, а именно, одно из коммутирований заменено на ассоциативное умножение:

$$[x, yz] = [x, y]z + y[x, z].$$

[258]**Карл Густав Якоб Якоби** (10.12.1804, Потсдам — 18. 02.1851) — один из классиков XIX века, которому принадлежат замечтаельные работы по многим областям математики. С 1826 по 1842 годы работал в Кенигсберге, потом в Берлине. Основные работы Якоби относятся к алгебре, теории чисел, теории эллиптических функций, теории дифференциальных уравнений с чатсными производными и механике. Кроме тождества Якоби с его именем связаны многочлены Якоби, тэта-функции, символ Якоби, Якобиевы матрицы, функциональный определитель (якобиан) и множество упоминаемых в нашем курсе теорем. В 1833 году Якоби был избран иностранным членом Петербургской Академии наук и к концу жизни планировал переехать в Петербург, но, к сожалению, ранняя смерть помешала осуществиться этим планам.

Это замечательное тождество характеризует класс **алгебр Пуассона**. Оно выполняется, например, для обычной скобки Пуассона, сложения и умножения функций.

Аналоги тождества Якоби, известные как **тождество Риччи**, **тождество Бьянки** и т.д. выполняются для операций в римановой геометрии.

§ 7. Другие важные тождества с одной операцией

1. Идемпотентность. Элемент $x \in X$ называется **идемпотентом**, если $x * x = x$. Говорят, что бинарная операция $*$ удовлетворяет тождеству

идемпотентности: $x * x = x$; для любого $x \in X$.

В префиксной записи это означает, что $f(x, x) = x$.

Примеры идемпотентных операций:

- конъюнкция и дизъюнкция,
- операции объединения и пересечения множеств,
- взятия максимума и максимума,
- наибольшего общего делителя и наименьшего общего кратного.

2. Ослабленная ассоциативность. В некоторых случаях ассоциативность не имеет места для произвольных троек, но выполняются какая-то ее ослабленная версия. Кроме тождества Якоби, которое является скорее аналогом ассоциативности, чем ее вариантом, наибольшее значение имеют следующие тождества,

левая альтернативность: $(xx)y = x(xy)$;

эластичность: $(xy)x = x(yx)$;

правая альтернативность: $(xy)y = x(yy)$.

Как обычно, о тождестве говорят, если соответствующее равенство выполняется для всех $x, y, z \in X$. Мы вернемся к анализу этих тождеств в Главе V при рассмотрении умножения в алгебрах октав и октонионов.

При анализе исключительных геометрий Рут Муфанг открыла следующие замечательные ослабления ассоциативности:

левое тождество Муфанг: $((xy)x)z = x(y(xz))$;

правое тождество Муфанг: $x(y(zy)) = ((xy)z)y$;

центральное тождество Муфанг: $(xy)(zx) = x(yz)x$.

Эти тождества кажутся экзотикой, но на самом деле они *естественно* возникают в самых различных разделах математики, например, в алгебраической геометрии[259]. Так как эти тождества как правило используются в сочетании с эластичностью (либо какими-то дополнительными условиями, при которых они влекут эластичность), при их записи скобки в произведениях вида xyx и yzy обычно не ставятся. На самом деле, в отсутствие эластичности выписанные выше тождества Муфанг *отличаются* от следующих тождеств:

левое тождество Бола: $(x(yx))z = x(y(xz))$;

правое тождество Бола: $x((yz)y) = ((xy)z)y$.

3. Йорданово тождество. Встречаются еще более причудливые на первый взгляд ослабления ассоциативности, такие как

йорданово тождество: $(x^2 * y) * x = x^2 * (y * x)$,

где под x^2 как обычно понимается $x * x$.

Комментарий. Это тождество появилось в 1934 году в работе Паскуаля Йордана, Юджина Вигнера и Джона фон Неймана, посвященной математическим основаниям квантовой механики. Представляется невероятным, чтобы подобное тождество могло быть интересным,

[259]Ю.И.Манин "Кубические формы", М., 1972, Гл.1.

однако в действительности существуют совершенно замечательные 27-мерные алгебры над $\mathbb{R}$ и над $\mathbb{C}$, удовлетворяющие этому тождеству. Именно с этими алгебрами связаны все наиболее замечательные исключительные объекты алгебры и геометрии (исключительные простые алгебры Ли и группы Ли, симметрические римановы пространства и т.д.)

4. Медиальность и автодистрибутивность. Вот еще три важных тождества, в которые входит одна операция:

левая автодистрибутивность: $x(yz) = (xy)(xz)$;

правая автодистрибутивность: $(xy)z = (xz)(yz)$.

медиальность: $(xy)(zw) = (xz)(yw)$;

Медиальность *похожа* на коммутативность, но это совсем не коммутативность. Вычитание некоммутативно, но легко видеть, что оно медиально,

$$(x - y) - (z - w) = (x - z) - (y - w).$$

Задача. Зафиксируем $a, b \in \mathbb{R}$ и введем на $\mathbb{R}$ бинарную операцию, полагая $x * y = ax + by$. Проверьте, что для любого выбора a и b операция $*$ медиальна. Когда она будет ассоциативной? Коммутативной?

Задача. Покажите, что медиальная операция, для которой существует (двусторонний) нейтральный элемент, в действительности коммутативна и ассоциативна.

Задача. Пусть A – абелева группа, $\phi, \psi \in \mathrm{Aut}(G)$, $\phi\psi = \psi\phi$ – два коммутирующих автоморфизма группы A, $c \in A$. Определим на A **операцию Брака-Тойоды** $xy = \phi(x) + \psi(y) + c$. Покажите, что эта операция медиальна. Будет ли она коммутативной?

§ 8. Другие важные тождества с двумя операциями

1. Антикоммутативность. Предположим, что на множестве X задано две операции – умножение и сложение, причем умножение дистрибутивно относительно сложения. Умножение называется **антикоммутативным**, если $x^2 = 0$ для всех $x \in X$. Вычисляя $(x+y)^2 = x^2 + xy + yx + y^2$ так что $xy + yx = 0$ или, если X образует абелеву группу по сложению, то $xy = -yx$. Наиболее известным примером антикоммутативной операции является векторное умножение векторов.

Комментарий. Фактически тождество антикоммутативности возникло еще в первой половине XIX века у Грассмана и Якоби, и в дальнейшем его значение в математике постоянно росло. Это тождество встречается как само по себе – наряду с тождеством Якоби оно выполняется в **алгебрах Ли** – так и в более рафинированном виде в сочетании с коммутативностью. Именно, в так называемых **супералгебрах** элементы разбиваются на однородные компоненты определенных степеней, причем сами эти однородные элементы либо коммутируют, либо антикоммутируют. В последние годы все большее распространение получают другие виды контролируемой некоммутативности, например, q-коммутативность $xy = qyx$.

2. Тождество взаимной дистрибутивности. Следующее тождество естественно возникает в алгебраической топологии при изучении гомотопических групп и H-пространств (см. [Spa]). Говорят, что две операции $\circ$ и $*$ на множестве X **взаимно дистрибутивны**, если для любых $x, y, u, v \in X$ имеет место равенство

$$(x \circ y) * (u \circ v) = (x * u) \circ (y * v).$$

Задача. Докажите, что если два закона композиции $\circ$ и $*$ на множестве X взаимно дистрибутивны и имеют общий двусторонний нейтральный элемент, то они совпадают между собой, т.е. $x * y = x \circ y$ для любых $x, y \in X$.

Заметим, что из Задачи ? вытекает, что в этом случае закон $*$ ассоциативен и коммутативен.

Коан. Известно, что умножение матриц и тензорное произведение связаны тождеством $(x \otimes y)(z \otimes w) = xz \otimes yw$. Почему же они не совпадают между собой?

3. Тождество модулярности. Говорят, что операции $\circ$ и $*$ связаны **тождеством модулярности**, если для любых $x, y, z \in X$ имеет место равенство

$$x \circ (y * z) = x \circ ((y \circ (x * z)) * z).$$

Комментарий. Это тождество, по-видимому, впервые использовал Рихард Дедекинд около 1900 года. Оно характеризует **модулярные** решетки. Однако чаще условие модулярности решетки формулируется в виде более простого тождества $x \circ (y * z) = (x \circ y) * z$, которое, однако выполняется уже не для всех $x, y, z \in X$ а только для тех троек, для которых $x \geq z$.

4. Стандартное тождество. Следующее тождество является обобщением коммутативности:

$$\sum_{\pi \in S_n} \operatorname{sgn}(\pi) x_{\pi(1)} \dots x_{\pi(n)} = 0.$$

Запишем для примера стандартное тождество степени 3:

$$xyz + yzx + zxy = yxz + zyx + xzy.$$

§ 9. Ассоциативность и коммутативность в языке

1. Отсутствие ассоциативности. В русском, как и в других флективных языках, возможности строить фразы, допускающие различную расстановку скобок, весьма ограничены. Сакраментальный пример, когда расстановка скобок необходима, ‘казнить нельзя помиловать’. В этом случае запятая нужна именно для того, чтобы зафиксировать расстановку скобок ‘(казнить нельзя) помиловать’ или ‘казнить (нельзя помиловать)’.

Возможности изолирующих языков (таких, как китайский или английский) в этом смысле гораздо больше, особенно в связи с тем, что в этих языках почти любое слово может быть любой частью речи. Проблема расстановки скобок реально возникает при переводе, в частности, компьютерном. Вот классический пример Ноама Хомского: `they are flying planes`. Большинство носителей языка в обычной ситуации проинтерпретируют эту фразу как `they (are flying) planes`, однако интерпретация `they are (flying planes)` не только грамматически правильна, но и в принципе возможна. Вот параллельный пример из фильма ужасов: `they are eating apples`[260]. А вот совсем реальный пример: переводчики фильмов на НТВ по умолчанию переводят фразу `biting dogs can be dangerous` как `опасно кусать собак` (отсутствие указания на число в сочетании с неассоцивностью и некоммутативностью!). Англофон живет в неассоциативном мире и *вынужден* автоматически интерпретировать `fresh fruit market` как `(fresh fruit) market`, а `new fruit market` как `new (fruit market)`. Но вот убрать неоднозначность в выражении `some more convincing evidence`[261] не прочтя его вслух в принципе невозможно: `(some more) convincing evidence` значит совсем не то же самое, что `some (more convincing) evidence`. А что может значить `beautiful girl's dress` или `square dance record`? Читатель может без труда придумать сотни английских фраз, в которых перестановка скобок приводит к удивительным переливам смысла.

Предостережение. В действительности, дело обстоит еще сложнее: отстутствие скобок значит совсем не то же самое, что любая из двух возможных расстановок скобок! Джон Лайонс[262] приводит такой пример: `Tom and Dick and Harry` имеет *три* различных интерпретации: `(Tom and Dick) and Harry`, `Tom and (Dick and Harry)` и, наконец, `Tom and Dick and Harry`.

---

[260]Джон Лайонс, Введение в теоретическую лингвистику, М., Прогресс, 1978, с.1–543, см. § 6.6.2. ‘Трансформационная неоднозначность’: `eating apples cost more than cooking apples`, стр. 265 и далее. Дополнительная неоднозначность в этом примере убирается использованием множественного числа, сравни с `eating apples costs more than cooking apples`.

[261]ibid., § 6.1.3. ‘Грамматическая неоднозначность’, стр. 225 и далее.

[262]ibid., § 6.2.7, ‘Рекурсивные координированные структуры’, стр.236.

Отсутствие ассоциативности представляет вполне реальную проблему при переводе. Рассмотрим следующие две фразы: `algebraic group theory` и `geometric group theory`. Может ли переводчик владеющий языком, но не предметом, понять, что `algebraic group theory` интерпретируется как `(algebraic group) theory` и переводится как **теория алгебраических групп**, в то время как абсолютно параллельную по форме фразу `geometric group theory` следует интерпретировать как `geometric (group theory)` и ее переводить как **геометрическая теория групп**. В письменном немецком языке с целью группировки используется довольно тонкое средство, а именно слитное и раздельное написание существительных. Например, `geometric group theory` будет переведено как `geometrische Gruppentheorie`, в то время как `algebraic group theory` можно было бы перевести как `algebraische Gruppen Theorie`, хотя, конечно, большинство носителей языка предпочтут в такой ситуации обратиться к иносказанию `Theorie von algebraischen Gruppen`.

Упражнение. Расставьте скобки в следующих выражениях: `abelian group theory`, `arithmetic group theory`, `combinatorial group theory`, `topological group theory`, `differential group theory`, `abstract group theory`, `finite group theory`, `concrete group theory`.

Часто перед переводчиком, не понимающим, о чем идет речь, возникает совершенно реальная проблема! Как, например, следует интерпретировать фразу `general Burnside problem`: как `(general Burnside) problem` – **проблема генерала Бернсайда** или же как `general (Burnside problem)` – **общая проблема Бернсайда**? Ответ на этот вопрос дается *только* констекстом. Например, я своими глазами видел перевод фразы `class field theory` как **классовая теория поля** (правильно **теория полей классов**). На этом свойстве английского языка построено громадное число шуток, загадок, лимериков, детских стишков и т.д. Вот небольшой тест на понимание живого английского языка: `time flies like (an) arrow, fruit flies like banana`. Специфические проблемы, связанные с расстановкой скобок, возникают при анализе составных немецких слов. Именно с этим связаны трудности, которые возникают у начинающих при понимании таких совсем простых слов, как `Gegenuhrzeigersinn`.

2. Отсутствие коммутативности. `кровь с молоком` versus `молоко с кровью`.

Координация в китайском языке. Например, `shanshui` (буквально, горы–реки) значит 'пейзаж', например, в живописи, в то время как `shuishan` (реки–горы) ничего такого не значит. ... горячо–холодно,

`Более-менее` (`more or less`, `mehr oder weniger`, `più o meno`) – только в голландском наоборот! Из этого, вероятно, можно делать глубокие психологические заключения.

Латынь является флективным языком и поэтому там нет больших проблем с ассоциативностью. Кроме того, свободный порядок слов позволяет (с небольшой натяжкой!) считать латынь близкой к коммутативности. Шесть фраз[263]

`Catullus Clodiam amabat,`	`Catullus amabat Clodiam,`
`Clodiam Catullus amabat,`	`Clodiam amabat Catullus,`
`amabat Catullus Clodiam,`	`amabat Clodiam Catullus,`

не только все грамматически правильны и стилистически приемлемы, но и передают примерно одну и ту же мысль: **Катулл любил Клодию**, **Катулл Клодию любил**, **Клодию Катулл любил**, **Клодию любил Катулл**, **любил Катулл Клодию**, **любил Клодию Катулл**. Конечно, эти фразы слегка отличаются эмфазисом, коннотациями и, как замечает Лайонс, 'контекстуальными пресуппозициями'. Выпускники классических гимназий могут поупражняться в составлении всех 24 перестановок фраз, состоящих из 4 слов, всех 120 перестановок фраз, состоящих из 5 слов и т.д.

[263]ibid., § 6.2.8, 'Прерывные составляющие', стр. 237.

Тема 3. ГОМОМОРФИЗМЫ

Весь цимес алгебраического подхода состоит в том, что алгебраические структуры рассматриваются вместе с классами отображений, сохраняющими эти структуры.

§ 1. Гомоморфизм

Самым важным и самым характерным понятием алгебры XIX–XX веков было понятие гомоморфизма. Пусть $(X, *)$ и $(Y, \circ)$ – два множества с алгебраическими операциями. Отображение $f : X \longrightarrow Y$ называется **гомоморфизмом**, если

$$f(x * y) = f(x) \circ f(y)$$

для всех $x, y \in X$.

Условие, что f является гомоморфизмом эквивалентно коммутативности следующей диаграммы:

$$\begin{array}{ccc} X \times X & \xrightarrow{\ *\ } & X \\ {\scriptstyle f\times f}\downarrow & & \downarrow{\scriptstyle f} \\ Y \times Y & \xrightarrow[\ \circ\ ]{} & Y \end{array}$$

В дальнейшем мы будем обычно обозначать операцию в множествах X и Y одним и тем же символом $*$, имея в виду, что в конкретных ситуациях эта $*$ может специализироваться в различные операции, такие как сложение, умножение, пересечение, обхединение, композиция и т.д. Символ $\circ$ теперь будет использоваться для композиции отображений.

Класс гомоморфизмов замкнут относительно композиции. Иными словами, композиция двух гомоморфизмов снова является гомоморфизмом: если $f : X \longrightarrow Y$, $g : Y \longrightarrow Z$ – два гомоморфизма, то $g \circ f : X \longrightarrow Z$ – тоже гомоморфизм. В самом деле,

$$(g\circ f)(x*y) = g(f(x*y)) = g(f(x)*f(y)) = g(f(x))*g(f(y)) = (g\circ f)(x)*(g\circ f)(y).$$

Сформулируем два важных дополнения к этому правилу:

• Тождественное отображение id_X является гомоморфизмом X на себя.

• Если $f : X \longrightarrow Y$ – биективный гомоморфизм, то $f^{-1} : Y \longrightarrow X$ – тоже гомоморфизм.

§ 2. Аддитивные гомоморфизмы

В настоящем параграфе мы приводим примеры отображений $f : X \longrightarrow Y$, которые являются **гомоморфизмами по сложению**, $f(x + y) = f(x) + f(y)$. Классически такие отображения называются **аддитивными**. В случае, когда X и Y являются абелевыми группами, такие отображения называются **групповыми гомоморфизмами**. Много дальнейших примеров приводится в главе II. В приводимых в этом параграфе примерах на рассматриваемых множествах есть и операция умножения, но эту операцию f не сохраняет.

• **Вещественная и мнимая часть.**

$$\mathrm{re}(z + w) = \mathrm{re}(z) + \mathrm{re}(w), \qquad \mathrm{im}(z + w) = \mathrm{im}(z) + \mathrm{im}(w).$$

В то же время, вообще говоря, $\mathrm{re}(zw) = \mathrm{re}(z)\,\mathrm{re}(w)$, $\mathrm{im}(zw) = \mathrm{im}(z)\,\mathrm{im}(w)$.

• **След матрицы.** Квадратной матрице $x \in M(n, K)$ с коэффициентами из поля K можно сопоставить ее **след** $\mathrm{tr}(x) = x_{11} + \ldots + x_{nn}$. След аддитивен, $\mathrm{tr}(x + y) = \mathrm{tr}(x) + \mathrm{tr}(y)$, но не мультипликативен.

• **Дистрибутивность.** Дистрибутивность умножения относительно сложения означает в точности, что умножение на любое $x \in R$ аддитивно: $x(y+z) = xy + xz$.

• **Дифференцирование и интегрирование.**

$$(f + g)' = f' + g', \qquad \int (f + g)\,dx = \int f\,dx + \int g\,dx$$

• **Определенный интеграл.**

$$\int\limits_a^b (f + g)\,dx = \int\limits_a^b f\,dx + \int\limits_a^b g\,dx$$

• **Частная производная.** Пусть f – функция n переменных $x_1, \ldots, x_n$. Отображение $f \mapsto \dfrac{\partial f}{\partial x_i}$ линейно,

$$\frac{\partial(f + g)}{\partial x_i} = \frac{\partial f}{\partial x_i} + \frac{\partial g}{\partial x_i}.$$

§ 3. Мультипликативные гомоморфизмы

В настоящем параграфе мы приводим примеры отображений $f : X \longrightarrow Y$, которые являются **гомоморфизмами по умножению**, $f(xy) = f(x)f(y)$. Классически такие отображения называются **мультипликативными**. В случае, когда X и Y являются полугруппами/группами, такие отображения называются **полугрупповыми/групповыми гомоморфизмами**. Много дальнейших примеров приводится в § ? и главе II. В приводимых в этом параграфе примерах на рассматриваемых множествах есть и операция сложения, но эту операцию f не сохраняет.

• **Возведение в степень.** Пусть K – поле, а $n \in \mathbb{N}$. Тогда отображение $x \mapsto x^n$ мультипликативно $(xy)^n = x^n y^n$, но, вообще говоря, не аддитивно, т.е. $(x + y)^n \neq x^n + y^n$.

Комментарий. Тем не менее, если $n = p \in \mathbb{P}$ – простое число, а характеристика поля K равна p (например, $K = \mathbb{F}_p$ – поле из p элементов), то $(x + y)^p = x^p + y^p$, так что в этом случае отображение $\mathrm{Fr} : x \mapsto x^p$ оказывается гомоморфизмом как по умножению, так и по сложению. Этот гомоморфизм, известный как **автоморфизм Фробениуса**, играет громадную роль в теории Галуа, теории чисел и алгебраической геометрии.

• **Абсолютная величина/модуль.** $|xy| = |x| \cdot |y|$.

• **Знак.** $\mathrm{sign}(xy) = \mathrm{sign}(x)\,\mathrm{sign}(y)$

• **Знак отображения.** Пусть $\pi \in \mathrm{Map}(\underline{n}, \underline{n})$ – отображение конечного множества $\underline{n}$ на себя. Если π не является биекцией, то положим $\mathrm{sgn}(\pi) = 0$, а если

π является биекцией, то определим $\operatorname{sgn}(\pi)$ как знак перестановки π. Как будет доказано в Главе II, $\operatorname{sgn}(\pi\sigma) = \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma)$.

• **Определитель.** Предположим, что R – коммутативное кольцо, например, $R = K$ – поле. В конце XVII века Секи Кова и фон Лейбниц связали с каждой матрицей $x \in M(n, R)$ элемент $\det(x)$ кольца R, называемый **определителем** (alias, **детерминантом**) матрицы x. *Смысл* введения определителя, его raison d'être, состоит в том, что определитель мультипликативен, $\det(xy) = \det(x)\det(y)$. Однако равенство $\det(x+y) = \det(x) + \det(y)$, вообще говоря, совершенно неверно!

• **Внешняя степень матрицы.** Сопоставим матрице $x \in M(n, K)$ ее m-ю **внешнюю степень** $\bigwedge^m(x)$, состоящую из всех миноров m-го порядка матрицы x, расположенных лексикографически (это в точности тот порядок, в котором они генерируются функцией `Minors`). В линейной алгебре[264] матрица $\bigwedge^m(x)$ часто называется m-й **ассоциированной матрицей**. Классическая **теорема Бине-Коши** утверждает, что отображение $\bigwedge^m : M(n, K) \longrightarrow M(\binom{m}{n}, K)$ является мультипликативным гомоморфизмом, $\bigwedge^m(xy) = \bigwedge^m(x)\bigwedge^m(y)$.

• **Симметрическая степень.** Кроме определителя с каждой квадратной матрицей $x \in M(n, K)$ можно связать перманент $\operatorname{per}(x) \in K$, в который входят те же слагаемые, что в определитель, но теперь все они берутся со знаком $+$. Тем самым, мы можем связать с матрицей $x \in M(n, K)$ ее m-ю **симметрическую степень** $S^m(x)$, состоящую из всех подперманентов m-го порядка матрицы x, расположенных лексикографически. Отметим, что в отличие от миноров, строки и столбцы которых не могут повторяться, в подперманент одна и та же строка или один и тот же столбец могут входить несколько раз. Тем самым, количество подперманентов m-го порядка в матрице порядка n равно квадрату количества выборок из n по m *с повторениями*. **Теорема Бине-Коши для перманентов** утверждает, что отображение $S^n : M(n, K) \longrightarrow M(\binom{m}{n+m}, K)$, $x \mapsto S^m(x)$, является гомоморфизмом, $S^m(xy) = S^m(x)S^m(y)$.

• **Старший коэффициент многочлена.** $\operatorname{lc}(fg) = \operatorname{lc}(f)\operatorname{lc}(g)$ (но равенство $\operatorname{lc}(f+g) = \operatorname{lc}(f) + \operatorname{lc}(g)$, вообще говоря, не имеет места!)

• **Содержание и примитивная часть многочлена.** Гаусс связал с многочленом $f \in \mathbb{Z}[x]$ его **содержание** $\operatorname{cont}(f)$, которое определяется как наибольший общий делитель коэффициентов многочлена f, а с каждым ненулевым многочленом $f \neq 0$ – его **примитивную часть** $\operatorname{pp}(f) = \operatorname{cont}(f)^{-1}f$. **Лемма Гаусса** утверждает, что $\operatorname{cont}(fg) = \operatorname{cont}(f)\operatorname{cont}(g)$ и, тем самым, $\operatorname{pp}(fg) = \operatorname{pp}(f)\operatorname{pp}(g)$. Конечно, ни о какой аддитивности в этих случаях не может быть речи.

§ 4. Гомоморфизмы между различными операциями

В настоящем параграфе мы приводим первые примеры отображений $f : X \longrightarrow Y$, которые являются гомоморфизмами между различными операциями, например, между сложением и умножением, для которых выполняется одно из следующих равенств $f(x+y) = f(x)f(y)$ и $f(xy) = f(x) + f(y)$. В случае, когда множества X и Y являются группами, относительно этих операций, такие отображения будут **групповыми гомоморфизмами**. Приводимые здесь примеры и много дальнейших примеров подробно обсуждаются в главе II.

[264] Р.Хорн, Ч.Джонсон, Матричный анализ. – М.Мир, 1989, с.1–655. стр.32.

• **Экспонента и логарифм.**

$$\exp(x+y)=\exp(x)\exp(y),\qquad \ln(xy)=\ln(x)+\ln(y).$$

• **Формула де Муавра.** $\phi\mapsto\cos(\phi)+i\sin(\phi)$

$$\cos(\phi+\psi)+i\sin(\phi+\psi)=(\cos(\phi)+i\sin(\phi))(\cos(\psi)+i\sin(\psi)).$$

•

$$x\mapsto\begin{pmatrix}1&x\\0&1\end{pmatrix},\qquad\begin{pmatrix}1&x+y\\0&1\end{pmatrix}=\begin{pmatrix}1&x\\0&1\end{pmatrix}\begin{pmatrix}1&y\\0&1\end{pmatrix}.$$

• **Степень.** $x^{m+n}=x^mx^n$.

• **Аргумент.** $\arg(xy)=\arg(x)+\arg(y)$.

• **Определитель.** Пусть как и в конце § ? $X=\bigcup M(n,K)$, $n\in\mathbb{N}_0$, – множество квадратных матриц над K всевозможных конечных порядков, рассматриваемое относительно операций прямой суммы и тензорного (кронекеровского) произведения. Тогда $\det(x\oplus y)=\det(x)\det(y)$ ('теорема об определителе ступенчатой матрицы'). В то же время формула для определителя тензорного произведения несколько сложнее

$$\det(x\otimes y)=\det(x)^{\deg(y)}\det(y)^{\deg(x)}.$$

• **Преобразование Фурье.** $F(f*g)=F(f)F(g)$.

• **Преобразование Лапласа.** $L(f*g)=L(f)L(g)$.

• **Многочлены Чебышева.** $T_{mn}=T_m\circ T_n$.

• **Степень многочлена.** Если $f,g\in K[x]$, то $\deg(fg)=\deg(f)+\deg(g)$ и $\deg(f\circ g)=\deg(f)\deg(g)$.

• **Характеристический многочлен.** Пусть, X множество квадратных матриц над K всевозможных конечных порядков с операциями прямой суммы и тензорного произведения. Квадратной матрице $x\in X$ сопоставляется ее характеристический многочлен $\chi_x\in K[x]$, являющийся нормированным многочленом степени $\deg(x)$. Тогда

$$\chi_{x\oplus y}=\chi_x\chi_y,\qquad\chi_{x\otimes y}=\chi_x\otimes\chi_y,\qquad\chi_{x\boxplus y}=\chi_x\boxplus\chi_y.$$

§ 5. Аддитивные и мультипликативные гомоморфизмы

В настоящем параграфе мы приводим первые примеры отображений $f:X\longrightarrow Y$, которые одновременно являются гомоморфизмами по сложению и умножению, для которых выполняются оба равенства $f(x+y)=f(x)+f(y)$ и $f(xy)=f(x)f(y)$. В случае, когда множества X и Y являются кольцами относительно этих операций, такие отображения называются **кольцевыми гомоморфизмами**. Все приводимые здесь примеры и много дальнейших более трудных примеров подробно обсуждаются в главе III.

• **Проекция на компоненту.**

$$\mathrm{pr}_i(x+y)=\mathrm{pr}_i(x)+\mathrm{pr}_i(y),\qquad\mathrm{pr}_i(xy)=\mathrm{pr}_i(x)\,\mathrm{pr}_i(y).$$

• **Комплексное сопряжение.** $^- : \mathbb{C} \longrightarrow \mathbb{C}$, $z = x + iy \mapsto \overline{z} = x - iy$. Известно, что комплексное сопряжение обладает следующими свойствами $\overline{z+w} = \overline{z} + \overline{w}$, $\overline{zw} = \overline{z} \cdot \overline{w}$.

• **Комплексно сопряженная матрица.** Пусть $X = M(n, \mathbb{C})$ – множество всех *комплексных* квадратных матриц степени n. Тогда **комплексное сопряжение** $X \longrightarrow X$, $x \mapsto y^*$, сопоставляющее матрице $x = (x_{ij})$ матрицу $\overline{x} = (\overline{x_{ij}})$, является автоморфизмом по сложению и умножению $\overline{x+y} = \overline{x} + \overline{y}$ и $\overline{xy} = \overline{x} \cdot \overline{y}$.

• **Предел.**

$$\lim_x(f+g) = \lim_x(f) + \lim_x(g), \qquad \lim_x(fg) = \lim_x(f)\lim_x(g).$$

?. Замена переменной. Пусть A – абелева группа. Любое отображение $\phi : X \longrightarrow Y$ определяет гомоморфизм $\widetilde{\phi} : A^Y \longrightarrow A^X$, называемый **заменой переменной**, по формуле $(\widetilde{\phi}(f))(x) = f(\phi(x))$ при этом $\widetilde{\phi}$ является гомоморфизмом по сложению. Если $A = K$ является кольцом, то замена переменной является, кроме того, и гомоморфизмом и по умножению:

$$\widetilde{\phi}(f+g) = \widetilde{\phi}(f) + \widetilde{\phi}(g), \qquad \widetilde{\phi}(fg) = \widetilde{\phi}(f)\widetilde{\phi}(g).$$

Вот несколько простых примеров замены переменных:

• **Сдвиг.** Замена переменной, отвечающая **трансляции** аргумента $T_y : x \mapsto x+y$, называется **сдвигом** функций $\mathrm{shift}_y = \widetilde{T_y}$. Таким образом, $\mathrm{shift}_y(f)(x) = f(x+y)$. Ясно, что

$$\mathrm{shift}_y(f+g) = \mathrm{shift}_y(f) + \mathrm{shift}_y(g), \quad \mathrm{shift}_y(fg) = \mathrm{shift}_y(f)\,\mathrm{shift}_y(g).$$

• **Масштабирование.** Замена переменной, отвечающая **растяжению** аргумента $D_c : x \mapsto cx$, называется **масштабированием** функций $\mathrm{stretch}_c = \widetilde{D_c}$. Таким образом, $\mathrm{stretch}_c(f)(x) = f(cx)$. Ясно, что

$$\mathrm{stretch}_c(f+g) = \mathrm{stretch}_c(f) + \mathrm{stretch}_c(g), \quad \mathrm{stretch}_c(fg) = \mathrm{stretch}_c(f)\,\mathrm{stretch}_c(g).$$

• **Ограничение.** Пусть $X \subseteq Y$, а $\phi : X \longrightarrow Y$ – каноническое вложение. В этом случае замена переменной $\widetilde{\phi}$ называется **ограничением** и обозначается через res^Y_X, а результат ее применения к функции $f \in R^X$ часто обозначается просто $f|_X = \mathrm{res}^Y_X(f)$. При этом

$$(f+g)|_X = f|_X + g|_X, \qquad (fg)|_X = f|_X g|_X.$$

• **Значение в точке.** Этот пример по существу является частным случаем предыдущего. Определим отображение $\mathrm{ev}_c(f) = f(c)$, сопоставляющее функции f ее значение в точке $c \in X$. На научном языке отображение ev_c называется **эвалюацией** в точке c, откуда обозначение ev – evaluation. Как всегда,

$$\mathrm{ev}_c(f+g) = \mathrm{ev}_c(f) + \mathrm{ev}_c(g), \qquad \mathrm{ev}_c(fg) = \mathrm{ev}_c(f)\,\mathrm{ev}_c(g).$$

• **Степень матрицы.** Пусть $X = \bigcup M(n, K)$, $n \in \mathbb{N}_0$, – множество квадратных матриц над K всевозможных конечных порядков, рассматриваемое относительно операций прямой суммы и тензорного (кронекеровского) произведения.

Обозначим через $\deg(x)$ степень (порядок) матрицы x, т.е. то (единственное!) n, для которого $x \in M(n, K)$. Тогда

$$\deg(x \oplus y) = \deg(x) + \deg(y), \qquad \deg(x \otimes y) = \deg(x)\deg(y).$$

• **След матрицы.** Пусть, по-прежнему, X множество квадратных матриц над K всевозможных конечных порядков с теми же операциями. Тогда

$$\mathrm{tr}(x \oplus y) = \mathrm{tr}(x) + \mathrm{tr}(y), \qquad \mathrm{tr}(x \otimes y) = \mathrm{tr}(x)\,\mathrm{tr}(y).$$

• **Обратная матрица.** Пусть $G = \bigcup \mathrm{GL}(n, K)$, $n \in \mathbb{N}_0$, – множество всех квадратных обратимых матриц над K всевозможных конечных порядков, также рассматриваемое относительно операций прямой суммы и тензорного (кронекеровского) произведения. Тогда отображение $G \longrightarrow G$, $g \mapsto g^{-1}$, сопоставляющее матрице g ее обратную, является гомоморфизмом,

$$(h \oplus g)^{-1} = h^{-1} \oplus g^{-1}, \qquad (h \otimes g)^{-1} = h^{-1} \otimes g^{-1}.$$

Предостережение. Этот пример носит *заведомо* провокационный характер! Он (как и ряд других примеров) служит тому, чтобы читатель начал обращать внимание на то, *где и относительно каких операций* данное отображение является гомоморфизмом. Дело в том, что обычно рассматривается множество $\mathrm{GL}(n, K)$ обратимых матриц *фиксированного* порядка n относительно *обычного* умножения матриц, в этом случае отображение $g \mapsto g^{-1}$ является **антиавтоморфизмом**, но не автоморфизмом!

§ 6. Гомоморфизмы булевых операций

• **Прообраз.** Любое отображение $f : X \longrightarrow Y$ определяет гомоморфизм $f^{-1} : 2^Y \mapsto 2^X$ относительно $\cup$, $\cap$ и $\setminus$ $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$, $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$, $f^{-1}(A \setminus B) = f^{-1}(A) \setminus f^{-1}(B)$, – обратный образ

• **Образ объединения.** Любое отображение $f : X \longrightarrow Y$ определяет гомоморфизм $f : 2^X \mapsto 2^Y$ относительно $\cup$, $f(A \cup B) = f(A) \cup f(B)$, в то же время, это отображение, вообще говоря не является гомоморфизмом $2^X \mapsto 2^Y$ относительно $\cap$ и $\setminus$, см. § ?.

• **Характеристические функции.** Рассмотрим отображение $2^Z \longrightarrow \{0, 1\}^Z$, сопоставляющее подмножеству $X \subseteq Z$ его характеристическую функцию χ_A, значение которой $z \in Z$ равно 1, если $z \in X$ и 0, если $z \notin X$.

$$\chi_{A \cap B} = \chi_A \chi_B, \qquad \chi_{A \triangle B} = \chi_A + \chi_B.$$

• **Характеристические функции, cont. индикаторные функции**, **индикаторы** – характеристические функции, рассматриваемые как функции со значениями в $\mathbb{Z}$ или в $\mathbb{R}$.

$$\chi_{A \cap B} = \chi_A \cap \chi_B, \qquad \chi_{A \cup B} = \chi_A \cup \chi_B.$$

• **Формулы де Моргана.** Дополнение является инволютивным изоморфизмом $(2^Z, \cup)$ и $(2^Z, \cap)$:

$$\overline{A \cup B} = \overline{A} \cap \overline{B}, \qquad \overline{A \cap B} = \overline{A} \cup \overline{B}.$$

• **Формулы де Моргана, cont.** Пусть $\cup$ и $\cap$ – обозначают соответственно образование верхней огибающей и нижней огибающей вещественных функций. Тогда

$$-(f \cup g) = -f \cap -g, \qquad -(f \cap g) = -f \cup -g.$$

• **Замыкание и внутренность.** Замыкание является эндоморфизмом множества $(2^Z, \cup)$, а внутренность – эндоморфизмом $(2^Z, \cap)$.

$$\mathrm{Clos}(A \cup B) = \mathrm{Clos}(A) \cup \mathrm{Clos}(B), \qquad \mathrm{Int}(A \cap B) = \mathrm{Int}(A) \cap \mathrm{Int}(B).$$

• **Производное множество.** В анализе с подмножеством $A \subseteq X$ топологического пространства X часто связывается множество его **точек накопления** A^d, называемое также производным множеством. Напомним, что точка $x \in X$ называется **точкой накопления** множества A, если $x \in \mathrm{Clos}(A \setminus \{x\}$. Проверьте, что $(A \cup B)^d = A^d \cup B^d$.

• **Оценка истинности.**

• **Функционал Минковского.** Пусть V – вещественное векторное пространство. Подмножество $X \subseteq V$ называется **поглощающим**, если для любого $v \in V$ существует $\lambda \in \mathbb{R}_+$ такое, что $v \in \lambda X = \{\lambda x, x \in X\}$, **выпуклым**, если для любых $x, y \in X$, и любых $\lambda, \mu \in \mathbb{R}_+$, $\lambda + \mu = 1$, имеем $\lambda x + \mu y \in X$, и **уравновешенным**, если для любого $x \in X$ и любого $\lambda \in \mathbb{R}$, $|\lambda| < 1$, имеем $\lambda x \in X$. Каждому поглощающему выпуклому уравновешенному множеству $X \subseteq X$ можно сопоставить его **функционал Минковского** $p_X : V \longrightarrow \mathbb{R}_+$, определяемый как $p_X(v) = \inf\{\lambda \in \mathbb{R}_+ \mid v \in \lambda X\}$. Проверьте, что если $X, Y \subseteq V$ два поглощающих выпуклых уравновешенных множества, то их пересечение $X \cap Y$ также является поглощающим выпуклым и уравновешенным, причем $p_{X \cap Y} = p_X \cup p_Y$.

• **Ортогональное дополнение.** Пусть V – эвклидово пространство над $\mathbb{R}$ со скалярным произведением $B : V \times V \longrightarrow \mathbb{R}$. Тогда каждому $X \leq V$ можно сопоставить его **ортогональное дополнение** $X^\perp = \{v \in V \mid B(X, v) = 0\} \leq V$. Легко проверить, что

$$(X + Y)^\perp = X^\perp \cap Y^\perp, \qquad (X \cap Y)^\perp = X^\perp + Y^\perp.$$

§ 7. Арифметические функции

В этом параграфе рассматриваются **арифметические функции**, т.е. отображения $f : \mathbb{N} \longrightarrow \mathbb{C}$. Впрочем, иногда термин арифметическая функция употребляют и в применении к отображениям $f : \mathbb{Z} \longrightarrow \mathbb{C}$. Специалисты по теории чисел называют арифметическую функцию f **мультипликативной**, если $f(mn) = f(m)f(n)$ для *взаимно простых* $m, n \in \mathbb{N}$. Функции же мультипликативные в нашем смысле, т.е. такие, что $f(mn) = f(m)f(n)$ для *любых* $m, n \in \mathbb{N}$, в теории чисел принято называть **вполне мультипликативными**. Аналогично, арифметическая функция f называется **аддитивной**, если $f(mn) = f(m) + f(n)$ для *взаимно простых* $m, n \in \mathbb{N}$, и **вполне аддитивной**, если $f(mn) = f(m) + f(n)$ для *любых* $m, n \in \mathbb{N}$.

• **Функция $\Omega(n)$.** Пусть $n = p_1^{m_1} \dots p_s^{m_s}$ – каноническое разложение натурального n на простые. Обозначим через $\Omega(n) = m_1 + \dots + m_s$ количество всех (не обязательно различных!) простых делителей числа n. Тогда

$\Omega(mn) = \Omega(m) + \Omega(n)$. В то же время функция $\omega(n) = s$, равная количеству *различных* простых делителей числа n, аддитивна, но не вполне аддитивна.

• **Функция Лиувилля.** Пусть, как и выше, $n = p_1^{m_1} \dots p_s^{m_s}$ – каноническое разложение натурального n на простые. **Функция Лиувилля** определяется как $\lambda(n) = (-1)^{\Omega(n)} = (-1)^{m_1+\dots+m_s}$. Легко видеть, что $\lambda(xy) = \lambda(x)\lambda(y)$.

• **Характер Дирихле.** Арифметическая функция $\chi : \mathbb{Z} \longrightarrow \mathbb{C}$ называется **характером Дирихле** по модулю m, если 1) она вполне мультипликативна, т.е. $\chi(kl) = \chi(k)\chi(l)$, для всех целых k, l, 2) значение $\chi(l)$ зависит только от класса l по модулю m, т.е. $\chi(l+m) = \chi(l)$, и 3) $\chi(l) = 0$ в том и только том случае, когда l не взаимно просто с m.

• **Символ Лежандра.** Пусть $a \in \mathbb{Z}$, а $p \in \mathbb{P}$ – нечетное простое. Тогда **символ Лежандра** $\left(\frac{a}{p}\right)$ определяется как $+1$, если a взаимно просто с p и является квадратом по модулю p; -1, если a взаимно просто с p и не является квадратом по модулю p; и, наконец, 0, если a делится на p. Символ Лежандра мультипликативен по первому аргументу: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

• **Символ Якоби.** Пусть $a \in \mathbb{Z}$, а $n \in \mathbb{N}$ нечетное натуральное число > 1. Тогда определен **символ Якоби** $\left(\frac{a}{n}\right)$. А именно, если $n = p_1 \dots p_s$ – разложение n на (не обязательно различные!) простые, то

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_s}\right).$$

Символ Якоби мультипликативен как по первому, так и по второму аргументу:

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right), \qquad \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right),$$

где $a, b \in \mathbb{Z}$, а $m, n \in \mathbb{N}$ – нечетные натуральные > 1.

• **Числа Фибоначчи.** $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.

• **Числа Мерсенна.** Для любого $a > 1$ отображение $n \mapsto a^n - 1$ является гомоморфизмом относительно gcd. Иными словами, для любых $m, n \in \mathbb{N}$, имеем $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$.

§ 8. Компоненты гомоморфизмов

• **Дифференцирования.**

Теоремы сложения. Теоремы сложения означают, что функция f является либо гомоморфизмом, либо компонентой гомоморфизма.

• **Тригонометрические функции.**

$$\sin(x+y) = \sin(x)\cos(y) + \cos(x)\sin(y), \quad \cos(x+y) = \cos(x)\cos(y)\sin(x)\sin(y).$$

В действительности, с точностью до аффинной замены переменной функции $f = \sin$, $g = \cos$ являются единственными *непрерывными* решениями функционального уравнения $f(x+y) = f(x)g(y) + g(x)f(y)$.

$$\operatorname{tg}(x+y) = \frac{\operatorname{tg}(x) + \operatorname{tg}(y)}{1 - \operatorname{tg}(x)\operatorname{tg}(y)}.$$

• **Гиперболические функции.**

§ 9. Композиция гомоморфизмов

• **Логарифм абсолютной величины.** $\ln(|fg|) = \ln(|f|) + \ln(|g|)$.

• **Логарифмическая производная.** Функция $\frac{d}{dx}(\ln(f)) = \frac{f'}{f}$ называется **логарифмической производной** функции f. Логарифм переводит произведение в сумму, а производная аддитивна, поэтому сопоставление функции ее логарифмической производной является гомоморфизмом мультипликативной структуры в аддитивную: $\frac{(fg)'}{fg} = \frac{f'}{f} + \frac{g'}{g}$.

§ 10. Антигомоморфизмы

Пусть $(X, *)$ и $(Y, \circ)$ – два множества с алгебраическими операциями. Отображение $f : X \longrightarrow Y$ называется **антигомоморфизмом**, если

$$f(x * y) = f(y) \circ f(x)$$

для всех $x, y \in X$. Таким образом, антигомоморфизм отличается от гомоморфизма тем, что он *обращает* порядок операндов. Антигомоморфизм $(X, *)$ в $(X, *)$ называется антиэндоморфизмом,

Антигомоморфизмы относительно композиции. В школьном курсе и в элементарном курсе анализа антигомоморфизмы (не являющиеся одновременно гомоморфизмами!) встречаются редко, так как единственной некоммутативной операцией там является композиция отображений.

• **Обратное отображение.** Рассмотрим множество $S_X = \mathrm{Bij}(X, X)$ биекций множества X на себя. Тогда отображение $\phi \mapsto \phi^{-1}$ сопоставляющее обратимому ϕ является антиавтоморфизмом S_X, а именно, $(\phi\circ\psi)^{-1} = \psi^{-1}\circ\phi^{-1}$

• **Замена переменной.** Рассмотрим множество $S_X = \mathrm{Map}(X, X)$ всех отображений множества X на себя. Тогда отображение $\psi \mapsto \widetilde{\phi}$ является антигомоморфизмом $\mathrm{Map}(X, X) \longrightarrow \mathrm{Map}(K^X, K^X)$, а именно, $\widetilde{\phi \circ \psi} = \widetilde{\psi} \circ \widetilde{\phi}$

Однако как только мы вводим некоммутативные операции, антигомоморфизмы встречаются на каждом шагу.

Матричные антигомоморфизмы.

• **Обратная матрица.** Пусть R – любое кольцо, $G = \mathrm{GL}(n, R)$ – множество квадратных обратимых матриц степени n над R. Тогда обращение $G \longrightarrow G$, $g \mapsto g^{-1}$, является антигомоморфизмом по умножению $(gh)^{-1} = h^{-1}g^{-1}$

• **Транспонированная матрица.** Пусть R – *коммутативное* кольцо, $X = M(n, R)$ – множество всех квадратных матриц степени n над R. Тогда **транспонирование** $X \longrightarrow X$, $x \mapsto x^t$, заменяющее строки матрицы на ее столбцы $(x_{ij})^t = (x_{ji})$, является антиавтоморфизмом по умножению $(xy)^t = y^t x^t$. Кроме того, это автоморфизм по сложению $(x + y)^t = x^t + y^t$.

Предостережение. Без предположения о коммутативности кольца R определенное так транспонирование (называемое в алгебре **формальным** транспонированием), не является антиавтоморфизмом! Как мы узнаем в главе III, *настоящее* транспонирование это отображение $M(n, R) \longrightarrow M(n, R^o)$, где R^o – кольцо, противоположное к R.

• **Присоединенная матрица.** Пусть R, по-прежнему, *коммутативное* кольцо, $X = M(n, R)$ – множество всех квадратных матриц степени n над R. Обозначим через $\widehat{x}$ **присоединенную** к x матрицу, элемент которой $\widehat{x}_{ij}$ в позиции (i, j) представляет собой **алгебраическое дополнение** к элементу x_{ji} матрицы x, т.е. определитель матрицы, получающейся из x вычеркиванием j-й строки и i-го столбца, со знаком $(-1)^{i+j}$. Эта матрица иногда называется также **взаимной** к матрице x. Тогда отображение $X \longrightarrow X$, $x \mapsto \widehat{x}$, является антигомоморфизмом по умножению $\widehat{xy} = \widehat{y}\widehat{x}$.

• **Эрмитовски сопряженная матрица.** Пусть $X = M(n, \mathbb{C})$ – множество всех *комплексных* квадратных матриц степени n. Тогда **эрмитово сопряжение** $X \longrightarrow X$, $x \mapsto y^*$, сопоставляющее матрице $x = (x_{ij})$ матрицу $x^* = (\overline{x_{ji}})$, является антиавтоморфизмом по умножению $(xy)^* = y^*x^*$. Кроме того, это автоморфизм по сложению $(x + y)^* = x^* + y^*$.

• **Кватернионное сопряжение.** Напомним, что сопряжение на теле кватернионов $\mathbb{H} \longrightarrow \mathbb{H}$, $z \mapsto \overline{z}$ определяется посредством

$$\overline{a + bi + cj + dk} = a - bi - cj - dk.$$

Легко проверить, что $\overline{zw} = \overline{w} \cdot \overline{z}$. В действительности $z \mapsto \overline{z}$ **инволюция** тела $\mathbb{H}$, т.е., кроме того, это автоморфизм по сложению, $\overline{z + w} = \overline{z} + \overline{w}$, причем инволютивный, т.е. $\overline{\overline{z}} = z$.

§ 11. Полугомоморфизмы

На мифологическом уровне основное отличие анализа от алгебры состоит вовсе не в том, что в анализе рассматриваются бесконечноместные операции, как это часто говорят. В действительности и в алгебре есть разделы, в которых систематически рассматриваются бесконечноместные операции, хотя, конечно, делается это там иначе, чем в анализе, без упора на вопросы сходимости. С другой стороны, в конечномерном выпуклом анализе никаких бесконечноместных операций нет, и тем не менее, по общему признанию это все-таки анализ. *Подлинное* отличие анализа от алгебры состоит в том, что там рассматриваются не тождества, а *неравенства*; не гомоморфизмы, а *полугомоморфизмы*.

1. Субгомоморфизмы и супергомоморфизмы. Дело в том, что в анализе рассматриваются *упорядоченные* алгебраические структуры. Отображение $f : X \longrightarrow Y$ множества с операцией $(X, *)$ в множество с операцией $(Y, \circ)$ называется **полугомоморфизмом**, если оно удовлетворяет одному из следующих неравенств:

$$f(x * y) \leq f(x) \circ f(y), \qquad f(x * y) \geq f(x) \circ f(y)$$

В первом случае отображение f часто называется **субгомоморфизмом**, а во втором случае – **супергомоморфизмом**. Приведем несколько классических примеров

• **Неравенство треугольника.** Модуль вещественного/комплексного числа обладает свойством **субаддитивности**, которое в этом случае называется **неравенством треугольника**: $|x + y| \leq |x| + |y|$.

• **Ранг матрицы.** Каждой матрице $x \in M(m, n, K)$ сопоставляется численный инвариант $\mathrm{rk}(K) \in \mathbb{N}_0$, называемый **рангом**. Легко видеть, что $\mathrm{rk}(x+y) \leq \mathrm{rk}(x) + \mathrm{rk}(y)$.

• **Размерность.** Пусть V – конечномерное векторное пространство, L – множество всех его подпространств. Рассмотрим отображение $\dim : L \longrightarrow \mathbb{Z}$, сопоставляющее каждому пространству $X \in L$ его размерность. Это отображение субаддитивно $\dim(X+Y) \leq \dim(X) + \dim(Y)$ для любых $X, Y \in L$. В действительности это неравенство является следствием более точного утверждения, известного как **теорема о размерности суммы и пересечения** $\dim(X+Y) = \dim(X) + \dim(Y) - \dim(X \cap Y)$.

• **Выпуклые и вогнутые функции.**

$$f\left(\frac{x+y}{2}\right) \leq \frac{f(x)+f(y)}{2}. \qquad f\left(\frac{x+y}{2}\right) \geq \frac{f(x)+f(y)}{2}.$$

• **Логарифмически выпуклые функции.**

$$f\left(\frac{x+y}{2}\right) \leq \sqrt{f(x)f(y)}.$$

• **Образ пересечения и разности.** $f(A \cap B) \subseteq f(A) \cap f(B)$, $f(A \setminus B) \supseteq f(A) \setminus f(B)$. Заметим, что при дополнительном предположении $B \subseteq A$ имеет место равенство $f(A \setminus B) = f(A) \setminus f(B)$. Отметим, что в важном частном случае, когда $f \in \mathrm{Bij}(X, Y)$, имеем $f(A \cap B) = f(A) \cap f(B)$.

• **Замыкание пересечения и внутренность объединения.**

$$\mathrm{Clos}(A \cap B) \subseteq \mathrm{Clos}(A) \cap \mathrm{Clos}(B), \qquad \mathrm{Clos}(A \setminus B) \supseteq \mathrm{Clos}(A) \setminus \mathrm{Clos}(B)$$

.

$$\mathrm{Fr}(A \cup B) \subseteq \mathrm{Fr}(A) \cup \mathrm{Fr}(B).$$

$$\mathrm{Int}(A \cup B) ? \, \mathrm{Int}(A) \cup \mathrm{Int}(B).$$

• **Супремум и инфимум.** Супремум субаддитивен, а инфимум супераддитивен

$$\sup(f+g) \leq \sup(f) + \sup(g), \qquad \inf(f+g) \geq \inf(f) + \inf(g).$$

• **Верхний и нижний предел.** Верхний предел субаддитивен, а нижний предел супераддитивен

$$\overline{\lim}_x(f+g) \leq \overline{\lim}_x(f) + \overline{\lim}_x(g), \qquad \underline{\lim}_x(f+g) \geq \underline{\lim}_x(f) + \underline{\lim}_x(g).$$

• Пусть $BV^*[a,b]$ – множество функций ограниченной вариации на $[a,b]$ с закрепленным концом (т.е. таких, что $f(a) = 0$). Обозначим через $V(f)$ вариацию функции f. Тогда $V(fg) \leq f(f)V(g)$.

§ 12. Неравенство треугольника

Векторные нормы. Пусть V – векторное пространство над $K = \mathbb{C}$ или $\mathbb{R}$. Функция $\|\cdot\| : V \longrightarrow \mathbb{R}$ называется **полунормой**, если она **неотрицательна**, т.е. $\|x\| \geq 0$ для всех $x \in V$; **абсолютно однородна**, т.е. $\|\lambda x\| = |\lambda|\|x\|$ для всех $\lambda \in K$, $x \in V$ и удовлетворяет **неравенству треугольника** $\|x+y\| \leq \|x\| + \|y\|$. Полунорма $\|\cdot\|$ называется **нормой**, если она **положительна**, т.е. $\|x\| = 0 \Longleftrightarrow x = 0$ (или, иными словами, $\|x\| > 0$ для всех

$x \neq 0$). Иногда вместо $\|x\|$ пишут $N(x)$, так что неравенство треугольника принимает вид $N(x+y) \leq N(x) + N(y)$.

В дальнейшем мы рассматриваем n-мерное векторное пространство $V = K^n$, а через x_i обозначается i-я координата x по отношению к стандартному базису, $x = (x_1, \ldots, x_n)$. Если B – положительно определенное скалярное произведение на V, то $\|x\| = B(x,x)$, сопоставляющее каждому вектору (положительный) квадратный корень из его скалярного квадрата, является нормой. Именно такой вид имеет

• ℓ_2**-норма**, более известная под алиасом **эвклидова норма**, которая определяется как $\|x\|_2 = \sqrt{\sum\limits_{i=1}^{n} |x_i|^2}$. Неравенство треугольника для этого случая называется **неравенством Коши**.

Другими наиболее известными примерами норм являются

• ℓ_1**-норма** $\|x\| = |x_1| + \ldots + |x_n|$ и

• ℓ_∞**-норма** $\|x\| = \max\limits_{1 \leq i \leq n} |x_i|$, известная как **норма равномерной сходимости** или **норма Чебышева**.

Для этих норм неравенство треугольника сразу вытекает из неравенства треугольника для абсолютной величины. В анализе широко рассматривается совместное обобщение всех этих примеров, а именно,

• ℓ_p**-норма**, $\|x\|_p = \sqrt[p]{\sum\limits_{i=1}^{n} |x_i|^p}$. известная как **норма Гельдера**, неравенство треугольника в этом случае называется **неравенством Минковского**.

Матричные нормы. Норма на векторном пространстве $M(n,K)$ называется **матричной нормой**, если, в дополнение к обычным свойствам векторной нормы, она выпукла по отношению к умножению, $\|xy\| \leq \|x\|\,\|y\|$. Например, из неравенства треугольника сразу вытекает, что

• ℓ_1**-норма**, определенная как $\|x\|_1 = \sum\limits_{i,j=1}^{n} |x_{ij}|$, является матричной нормой.

• Неравенство Коши означает в точности, что ℓ_2**-норма**, определенная как

$$\|x\|_2 = \sqrt{\sum_{i,j=1}^{n} |x_{ij}|^2},$$

является матричной нормой. В случае векторных пространств эта норма называется **эвклидовой**, но в применении к матрицам ее часто называют также **нормой Гильберта-Шмидта**, **нормой Фробениуса** или **нормой Шура**[265].

В то же время ℓ_∞**-норма** $\|x\|_\infty = \max\limits_{1 \leq i,j \leq n} |x_{ij}|$ не является матричной нормой.

Матричная норма, **индуцированная** векторной нормой, определяется как

$$\|x\| = \max_{\|u\|=1} \|xu\|.$$

Наиболее известны следующие три нормы такого типа:

• **столбцовая норма** $\|x\|_c = \max\limits_{1 \leq j \leq n} \sum\limits_{i=1}^{n} |a_{ij}|$, которая индуцирована векторной нормой $\|u\|_1$ на K^n,

• **строчная норма** $\|x\|_r = \max\limits_{1 \leq i \leq n} \sum\limits_{j=1}^{n} |a_{ij}|$, индуцированная векторной нормой $\|u\|_\infty$,

• **спектральная норма** $\|x\|_s$, индуцированная векторной нормой $\|u\|_2$.

• **Неравенство Минковского.** Положим

$$N_p(f) = \left(\int |f|^p \, dx \right)^{\frac{1}{p}}$$

$N_p(f+g) \leq N_p(f) + N_p(g)$ для $1 \leq p < \infty$

[265]Р.Хорн, Ч.Джонсон, с.351–354.

§ 13. Мера и вероятность

1. Мера. Пусть R – подмножество в 2^X замкнутое относительно булевых операций, в анализе такое семейство R обычно называется **кольцом множеств**. Отображение $\mu : R \longrightarrow \mathbb{R}$ называется **функцией множества**. Чаще всего рассматриваются неотрицательные функции $\mu(A) \geq 0$ удовлетворяющие неравенству $\mu(A \cup B) \leq \mu(A) + \mu(B)$. Это свойство меры иногда называется **полуаддитивностью**. В действительности, равенство $\mu(A \cup B) = \mu(A) + \mu(B)$ имеет место только при дополнительных предположениях типа $A \cap B = \varnothing$.

Предостережение. В анализе функцию множества μ принято называть **аддитивной**, если $\mu(A \cup B) = \mu(A) + \mu(B)$ для любых множеств A и B таких, что $A \cap B = \varnothing$. Для аддитивной в этом смысле функции имеет место равенство

$$\mu(A \cup B) = \mu(A) + \mu(B) - \mu(A \cap B).$$

Обычно рассматриваются меры, определенные на **σ-алгебрах**, замкнутых относительно произвольных счетных объединений. Такая мера называется **счетно аддитивной**, если $\mu(\bigcup\limits_{i=1}^{\infty} A_i) = \sum\limits_{i=1}^{\infty} \mu(A_i)$ для семейства множеств A_i такого, что $A_i \cap A_j = \varnothing$ при $i \neq j$. Свойство меры, выражаемое неравенством $\mu(\bigcup\limits_{i=1}^{\infty} A_i) \leq \sum\limits_{i=1}^{\infty} \mu(A_i)$, называется **счетной полуаддитивностью**.

2. Почему независимость? С общей точки зрения теория вероятностей представляет собой просто раздел теории меры. В то же время, даже поверхностное знакомство с предметом создает впечатление, что это весьма специфический раздел теории меры, в котором *центральную* роль играют понятия такие, как понятие **независимости**, которые вообще не обсуждаются в общей теории. Это связано с тем, что там, где в общей теории меры работают с полугомоморфизмами, в теории вероятностей[266] предпочитают использовать квазигомоморфизмы.

• **Функция распределения.** С каждой случайной величиной x можно связать ее **функцию распределения** $F_x : \mathbb{R} \longrightarrow [0, 1]$, значение которой в точке $t \in \mathbb{R}$ определяется как $F_x(t) = P\{\omega, x(\omega) \leq t\}$. Случайные величины x и y называются **независимыми**, если их **совместная функция распределения**

$$F_{x,y} : \mathbb{R} \times \mathbb{R} \longrightarrow [0, 1], \qquad F_{x,y}(s, t) = P\{\omega, x(\omega) \leq s, y(\omega) \leq t\},$$

является тензорным произведением их функций распределения: $F_{x,y} = F_x \otimes F_y$. Одно из основных свойств функции распределения, открытое Чебышевым, состоит в том, что функция распределения суммы **независимых** случайных величин x и y является сверткой функций распределения слагаемых[267], $F_{x+y} = F_x * F_y$.

• **Математическое ожидание.** Одним из наиболее важных инвариантов случайной величины x является ее **математическое ожидание** $M(x)$, выражающее среднее значение x. Математическое ожидание идемпотентно, т.е. $M(M(x)) = M(x)$ (специалист по теории вероятностей написал бы $M(x - M(x)) = 0$). Кроме того, оно аддитивно, т.е. $M(x + y) = M(x) + M(y)$ для *любых* двух случайных величин x и y, не обязательно независимых. В то же время мультипликативность математического ожидания $M(xy) = M(x)M(y)$ имеет место, вообще говоря, только в случае, когда x и y **независимые** случайные величины.

• **Дисперсия.** Другим важнейшим инвариантом случайной величины x является ее **дисперсия** $D(x) = M(x - M(x))^2$, выражающая ее средне-квадратичное отклонение от среднего значения. Пользуясь перечисленными в предыдущем примере свойствами математического ожидания, легко проверить, что для **независимых** случайных величин дисперсия аддитивна, $D(x + y) = D(x) + D(y)$.

---

[266] A.N.Kolmogorov, Grundbegriffe der Wahrscheinlichkeitsrechnung. – Berlin, 1933.

[267] А.Н.Ширяев, Вероятность. – М., Наука, 1980, с.1–575, см. стр.47.

Тема 3. ОСНОВНЫЕ КОНСТРУКЦИИ НАД ОПЕРАЦИЯМИ

> A composition on a set begets a variety of other compositions on closely related sets, each mirroring to some degree the properties of its parent.
>
> Seth Warner[268]

Сейчас мы опишем несколько основных способов построения новых алгебраических операций по уже имеющимся. Пусть X – множество с бинарной операцией $*$. Так как теперь нам будет важно указывать, где именно определена операция, мы будем иногда писать $(X,*)$, чтобы обозначить множество X с операцией $*$, и $*_X$, чтобы уточнить, что $*$ рассматривается как операция именно на X. Сейчас мы опишем пять основных способов строить новые операции из $*$, а именно, подоперации, фактор-операции, прямые суммы, операции на функциях и на подмножествах. Эти конструкции будут играть центральную роль в следующих главах[269].

§ 1. Подоперация

Прежде всего выясним, когда операция на X определяет операцию на подмножестве X

Определение. *Непустое подмножество $Y \subseteq X$ называется* **замкнутым** *относительно $*$, если для любых $x,y \in Y$ имеем $x*y \in Y$.*

В этом случае определено сужение $* = *_Y$ операции $* = *_X$ на Y, задаваемое посредством $(x,y) \mapsto x*y$, для всех $x,y \in Y$. Тогда $*_Y$ называется подоперацией операции $*$ и обычно обозначается тем же символом $*$, что и исходная операция.

В дальнейшем мы конкретизируем эту идею в понятиях подмоноида, подгруппы, подкольца, подмодуля, подпространства и т.д., поэтому ограничимся сейчас только небольшим колическтвом примеров.

• $\mathbb{N} \subseteq \mathbb{Z}$ замкнуто относительно сложения и умножения, но не относительно вычитания.

• Множество $2\mathbb{Z} \subseteq \mathbb{Z}$ четных чисел замкнуто относительно сложения, вычитания и умножения, а множество $2\mathbb{Z}+1 \subseteq \mathbb{Z}$ нечетных чисел замкнуто относительно умножения, но не относительно сложения и вычитания. Произведение двух нечетных чисел нечетно, но сумма и разность двух нечетных чисел четны.

• $\mathbb{Z} \subseteq \mathbb{Q}$ замкнуто относительно сложения, вычитания и умножения.

• множество $\Lambda(X) \subseteq 2^X$ всех конечных подмножеств множества X замкнуто относительно булевых операций объединения[270], пересечения, разности и симметрической разности.

• $\mathrm{Surj}(X,X), \mathrm{Inj}(X,X), \mathrm{Bij}(X,X) \subseteq X^X$ замкнуто относительно композиции.

---

[268] S.Warner, Modern algebra. v.I. – Prentice Hall, 1965, p.1–457.

[269] Разумеется, в математике встречаться *десятки* конструкций, позволяющих строить новые алгебраические операции из уже известных (свертка, симметризация, сплетение, экспоненцирование, различные виды произведений, такие как полупрямое произведение, свободное произведение, амальгамированное произведение, тензорное произведение, ограниченное произведение, ультрапроизведение, и т.д.), и многие из этих конструкции будут описаны в дальнейшем. Однако все эти конструкции либо определяются заметно сложнее, либо требуют для своего определения наличия *нескольких* операций на исходных множествах.

[270] Речь здесь идет о **конечных** объединениях.

• Множество $\{f \in K[x] \mid f(0) = 0\} \subseteq K[x]$ многочленов без свободного члена замкнуто относительно сложения и умножения.

• Множество $K[x]_n \subseteq K[x]$ многочленов степени $\leq n$ замкнуто относительно сложения, но при $N > 0$ не относительно умножения.

• Множество $\left\{ \begin{pmatrix} a & b \\ b & c \end{pmatrix} \;\middle|\; a, b, c \in K \right\} \subseteq M(2, K)$ симметрических матриц замкнуто относительно сложения, но не относительно умножения:

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

§ 2. Фактор-операция

> Многие из трудностей теории меры и вся имеющаяся здесь патология возникают в связи с существованием множеств меры нуль. Алгебраическая трактовка обходит все эти неприятности путем отказа от рассмотрения отдельных множеств вообще; вместо этого рассматриваются классы множеств, сравнимых по модулю множеств меры нуль.
>
> Поль Халмош[271]

Пусть теперь на множестве X задано отношение эквивалентности $\sim$. Напомним, что классом элемента $x \in X$ относительно эквивалентности $\sim$ называется множество $\overline{x} = \{y \in X \mid y \sim x\}$. Рассмотрим фактор-множество $Y = X/\sim = \{\overline{x} \mid x \in X\}$ и попробуем ввести на нем операцию $*_Y$ так, чтобы каноническая проекция $\mathrm{pr} : X \longrightarrow Y$ стала гомоморфизмом, т.е. чтобы $\overline{x} *_Y \overline{y} = \overline{x * y}$. Единственный способ сделать это – определить умножение в Y так, чтобы выполнялась эта формула, т.е. **определить** для двух классов эквивалентности $\overline{x}$ и $\overline{y}$ их композицию $\overline{x} * \overline{y}$ как $\overline{x * y}$. Однако, вообще говоря, это определение **некорректно**, так как класс $x * y$ может **зависеть** от выбора представителей x и y в классах $\overline{x}$ и $\overline{y}$. Таким образом мы приходим к следующему определению.

Определение. *Эквивалентность $\sim$ на множестве $(X, *)$ называется* **конгруэнцией** *по отношению к $*$, если $x_1 \sim x_2$ и $y_1 \sim y_2 \Longrightarrow x_1 * y_1 \sim x_2 * y_2$.*

В этом случае говорят также, что эквивалентность $\sim$ **согласована** с операцией $*$. Для конгруэнции действительно класс эквивалентности произведения $x * y$ не зависит от выбора представителей x и y из двух данных классов эквивалентности, так что теперь равенство $\overline{x} * \overline{y} = \overline{x * y}$ **корректно** определяет алгебраическую операцию на H.

Определение. *Операция $* = *_Y$ на фактор-множестве $Y = X/\sim$ по отношению к конгруэнции $\sim$, определенная как $\overline{x} * \overline{y} = \overline{x * y}$, называется* **фактор-операцией** *операции $* = *_X$.*

Так же и эта конструкция будет в дальнейшем конкретизирована в понятиях фактор-группы, фактор-кольца, фактор-модуля и т.д., тем не менее приведем сразу же **важнейший** пример, являющийся одним из основных объектов, рассматривающихся в нашем курсе.

---

[271] П.Халмош, Лекции по эргодической теории. – РХД, М.–Ижевск, 2001, с.1–131, стр.55.

§ 3. Кольцо классов вычетов

Только то и держится на гвозде,
что не делится без остатка на два.

Иосиф Бродский, 'Урания, Римские Элегии'.

Пусть $X = \mathbb{Z}$ и $m \in \mathbb{N}$. Введем на $\mathbb{Z}$ следующее отношение эквивалентности. Скажем, что $x \sim y$ в том и только том случае, когда $x \equiv y \pmod m$. Фактор-множество $\mathbb{Z}$ по этому отношению эквивалентности обычно обозначается $\mathbb{Z}/m\mathbb{Z}$. Оно состоит из m классов эквивалентности с представителями $\overline{0}, \overline{1}, \dots, \overline{m-1}$.

Лемма. *Отношение сравнимости по модулю m является конгруэнцией на $\mathbb{Z}$ как по сложению, так и по умножению.*

Доказательство. Пусть $x \equiv y \pmod m$ и $z \equiv w \pmod m$. Проверим вначале, что $x + z \equiv y + w \pmod m$. В самом деле, $(x + z) - (y + w) = (x - y) + (z - w)$, причем по условию оба слагаемых в правой части делятся на m. Требуемое сравнение по умножению проверяется аналогично. Мы хотим показать, что $xz \equiv yw \pmod m$. В самом деле, $xz - yw = (xz - yz) + (yz - yw) = (x - y)z + y(z - w)$, причем снова по условию оба слагаемых в правой части делятся на m.

Таким образом, $\overline{x} + \overline{y} = \overline{x + y}$ и $\overline{x} \cdot \overline{y} = \overline{xy}$ корректно определяют операции на $\mathbb{Z}/m\mathbb{Z}$, которые превращают это множество в кольцо, называемое **кольцом классов вычетов по модулю** m. В следующей главе мы дадим широкое обобщение этой конструкции.

§ 4. Прямое произведение/прямая сумма

Рассмотрим два множества X и Y с операциями $*_X$ и $*_Y$, которые мы обычно будем обозначать одним и тем же символом $*$. Тогда на прямом произведении $X \times Y$ этих множеств можно ввести операцию $* = *_{X\times Y}$ определив ее **покомпонентно**, т.е. положив

$$(x_1, y_1) * (x_2, y_2) = (x_1 * x_2, y_1 * y_2)$$

для любых $x_1, x_2 \in X$ и $y_1, y_2 \in Y$. Так определенная операция называется **прямым произведением** операций на X и на Y.

Иногда, особенно в случае, когда $* = +$, эта конструкция называется также прямой суммой и обозначается $\oplus$. Иными словами, $X \oplus Y$ как множество совпадает с $X \times Y$, а сложение в $X \oplus Y$ определяется как $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$. Наиболее известным примером этой конструкции являются, конечно, покомпонентные операции на векторах, по отношению к координатам этих векторов.

§ 5. Операции на функциях

Предположим теперь, что Y – множество с операцией $* = *_Y$, а X – произвольное множество и рассмотрим множество отображений $Z = \mathrm{Map}(X, Y)$. Тогда на Z можно ввести операцию $* = *_Z$ следующим образом. Мы должны для двух любых $f, g \in Z$ определить новое отображение $f * g \in Z$. Определить отображение значит определить для каждого $x \in X$ его образ под действием этого

отображения и мы сделаем это следующей формулой: $(f*g)(x) = f(x)*g(x)$. Такой способ переноса операции на функции называется **поточечным**. Заметим, что именно так обычно определяются **сумма функций** $(f+g)(x) = f(x)+g(x)$ и **произведение функций** $(fg)(x) = f(x)g(x)$ в анализе и геометрии. При этом, конечно, fg – это совсем не то же самое, что композиция $f \circ g$ функций f и g, которая вообще не определена если X и Y различны. На самом деле в различных разделах математики определяется много других законов композиции на функциях: свертки, скобки Пуассона, и т.д. (заметим, кстати, что в анализе символ $f * g$ обычно используется именно для обозначения свертки).

§ 6. Операции на подмножествах

Пусть X – множество с операцией $*$ и $Y = 2^X$. Тогда можно ввести операцию $*$ на элементах Y следующим образом: $A *_Y B = \{a*b \mid a \in A, b \in B\}$. В случае, когда $* = +$ так определенная операция

$$A + B = \{a + b \mid a \in A, b \in B\}$$

это в точности **сумма по Минковскому**. В действительности, существуют другие способы перенести операцию $*$ на подмножества различных типов. Например, под произведением идеалов A и B обычно понимается **идеал**, порожденный произведениями ab, $a \in A$, $b \in B$, а вовсе не **множество** таких произведений. Чтобы уточнить, что операция $*$ определяется на подмножествах именно таким образом, обычно говорят о переносе операции $*$ **по Минковскому**. Например, **произведение по Минковскому** множеств A и B определяется как $AB = \{ab \mid a \in A, b \in B\}$.

Эту операцию обычно обозначают тем же символом $*$, но часто это приводит к двусмысленностям. Например, если $*$ это операция обьединения или пересечения, то невозможно написать $A \cup B$ или $A \cap B$ в только что описанном значении, как $\{a \cup b \mid a \in A, b \in B\}$ или $\{a \cap b \mid a \in A, b \in B\}$, так как символам $\cup$ и $\cap$ уже придан другой, изначальный смысл.

Сумма по Минковскому. Чему равна сумма по Минковскому $X + Y$, где

1) $X = B(x, r)$ – шар радиуса r с центром x, а $Y = B(y, s)$.

2) $X = \mathbb{R}x$, $Y = \mathbb{R}y$ – приямые, натянутые на векторы $x, y \neq 0$.

3) $X = \mathbb{R}x$, $Y = B(0, r)$

4) X – квадрат с вершинами $(\pm 1, \pm 1)$, Y – квадрат с вершинами $(\pm 1, 0)$, $(0, \pm 1)$.

Задача. Пусть $*$ – композиция на X, а $A, B, C \subseteq X$. Доказать, что

i) $A * (B \cup C) = (A * B) \cup (A * C)$ и $(A \cup B) * C = (A * C) \cup (B * C)$.

ii) $A * (B \cap C) \subseteq (A * B) \cap (A * C)$ и $(A \cap B) * C \subseteq (A * C) \cap (B * C)$. Всегда ли здесь имеет место равенство?

Тема 3. МОНОИДЫ

В этой главе мы изучим простейший тип алгебраических систем: моноиды.

§ 1. Полугруппы

1. Первые примеры полугрупп. Мы уже видели пример полугруппы, не являющейся моноидом: это $\mathbb{N}$ относительно сложения. Приведем еще несколько важных примеров.

• **Полурешетки.** Пусть теперь, вообще $(X, \vee, \&)$ – любая решетка. Как мы знаем, операции $\vee$ и $\&$ ассоциативны, но нейтральные элементы для этих операций, 0 и 1, не обязаны существовать. Так что в общем случае $(X, \vee)$ и $(X, \&)$ являются полугруппами, но не моноидами.

• **НОД и НОК в $\mathbb{N}$.** Специализируя предыдущий пример, рассмотрим $X = \mathbb{N}$ с порядком, определенным делимостью. Тогда $(\mathbb{N}, \mathrm{lcm})$ является моноидом с нейтральным элементом 1. В то же время $(\mathbb{N}, \gcd)$ полугруппа, но не моноид.

• **Полугруппа левых/правых нулей.** Определим на X бинарную операцию $\rightarrow$, полагая $x \rightarrow y = y$. Эта операция ассоциативна (проверьте!), и таким образом превращает X в полугруппу, которая, однако, не является моноидом, если $|X| \geq 2$. Эта полугруппа называется **полугруппой правых нулей**. Теперь мы можем присоединить к X еще один не принадлежащий X элемент, который мы обозначим через e, и доопределить умножение, полагая $x \rightarrow e = x = e \rightarrow x$ для всех $x \in X^1 = X \cup \{e\}$. Это превращает X^1 в моноид (играющий, кстати, довольно важную роль в теории конечных автоматов). Разумеется, можно построить моноид и отправляясь от **полугруппы левых нулей**, в которой операция $\leftarrow$ определяется посредством $x \leftarrow y = x$.

Эти полугруппы обладают следующим замечательным свойством: все их элементы **идемпотентны**. Напомним, что элемент $z \in S$ полугруппы S называется идемпотентным, или, коротко, **идемпотентом**, если $z^2 = z$. Полугруппы левых и правых нулей настолько далеки от коммутативности, насколько это вообще можно себе представить. Ясно, что любой элемент обязан коммутировать сам с собой. Полугруппа называется **нигде не коммутативной** (nowhere commutative), если никаких других пар коммутирующих элементов нет, т.е. если из того, что $xy = yx$ для некоторых $x, y \in Z$ вытекает, что $x = y$.

Задача. Докажите, что $\leftarrow$ и $\rightarrow$ представляют собой идемпотентные нигде не коммутативные операции.

Определенная в последнем примере операции допускают следующее интересное обобщение.

• **Прямоугольная связка.** Пусть X и Y – произвольные множества. Определим бинарную операцию на $X \times Y$, полагая $(x_1, y_1)(x_2, y_2) = (x_1, y_2)$ для любых $x_1, x_2 \in X$ и $y_1, y_2 \in Y$. Эта операция ассоциативна (проверьте!) и таким образом, превращает $X \times Y$ в полугруппу, называемую **прямоугольной связкой** на множестве $X \times Y$. Но, за исключением тривиального случая $|X| = |Y| = 1$, эта полугруппа **никогда** не является моноидом. В случае когда $|X| = 1$ это в точности полугруппа правых нулей, а в случае, когда $|Y| = 1$ – полугруппа левых нулей. Чтобы объяснить название в общем случае нарисуйте картинку для случая, когда $X = Y = \mathbb{R}$.

Полугруппа называется **связкой**, если все ее элементы идемпотентны, так что прямоугольная связка действительно является связкой. Изучение коммутативных связок сводится к изучению частично упорядоченных множеств (а именно, положим $x \leq y$, если $xy = yx = x$, тогда произведение в полугруппе есть не что иное, как инфимум в этом частично упорядоченном множестве). Легко видеть, что прямоугольная связка нигде не коммутативна.

§ 2. Нейтральные элементы

1. Нейтральный элемент. Пусть X – множество с одной бинарной операцией, которую мы пока продолжаем обозначать через $*$. Говорят, что e – **левый нейтральный** элемент относительно $*$, если $e * x = x$ для любого $x \in X$. Аналогично определяется **правый нейтральный** элемент e, для которого $x * e = x$ для всех $x \in X$. Левые и правые нейтральные элементы называются **односторонними**. Вообще говоря, в множестве может быть много односторонних нейтральных элементов, либо не быть ни одного, но если существуют как левые, так и правые нейтральные, то картина меняется.

Лемма. *Если для $*$ существует левый нейтральный элемент e_1 и правый нейтральный элемент e_2, то $e_1 = e_2$.*

Доказательство. В самом деле, по определению односторонних нейтральных элементов получаем $e_1 = e_1 * e_2 = e_2$.

Определение. *Элемент $e \in X$ называется* **нейтральным** *элементом операции $*$, если он является как левым, так и правым нейтральным, т.е. если $e * x = x = x * e$ для любого $x \in X$.*

Иногда эмфатически в этом случае говорят о **двусторонних нейтральных** элементах. Выбор буквы ‘e’ для обозначения единичного элемента, единичной матрицы и т.д. стандартен и связан с немецким называнием нейтрального элемента: `Einheit` – единица.

2. Примеры нейтральных элементов.

• 0 является нейтральным элементом относительно сложения чисел.

• 1 является нейтральным элементом относительно умножения чисел.

• 1 является правым нейтральным элементом относительно операции возведения в степень. Левого нейтрального для операции возведения в степень нет.

• $\varnothing$ является нейтральным элементом относительно объединения и симметрической разности в 2^X.

• X является нейтральным элементом относительно пересечения в 2^X,

• id является нейтральным элементом относительно композиции отображений в X^X.

• $\Delta = \{(x, x), x \in X\}$ является нейтральным элементом относительно композиции отношений в в $2^{X \times X}$.

• пустое слово Λ является нейтральным элементом относительно композиции в свободной моноиде.

§ 3. Моноиды, простейшие примеры

Простейшей алгебраической структурой являются моноиды – множества с одной ассоциативной бинарной операцией.

1. Моноиды. Сейчас мы определим простейшую алгебраическую структуру.

Определение. *Непустое множество* $(X, *)$ *с бинарной операцией* $*$ *называется* **моноидом**, *если операция* $*$ *ассоциативна и обладает нейтральным элементом* e.

Иными словами, предполагается, что

M1) $\forall x, y, z \in X$, $(x * y) * z = x * (y * z)$ (ассоциативность),

M2) $\exists e \in X$, $\forall x \in X$, $e * x = x = x * e$ (нейтральный элемент).

При этом нейтральный элемент можно рассматривать как заданную на X нульарную операцию и часто, чтобы указать все элементы структуры моноида, пишут $(X, *, e)$. Термин 'моноид' происходит от греческого '$\mu\grave{o}\nu o\varsigma$', означающего 'один', 'единственный'.

2. Аддитивная и мультипликативная нотация. Для записи операции в моноидах чаще всего используются две нотации: аддитивная и мультипликативная. В случае **аддитивной** нотации операция называется **сложением** и обозначается знаком '+', так что вместо $x * y$ пишут $x + y$. При этом операнды называются **слагаемыми**, а результат – **суммой**. Нейтральный элемент называется обычно **нулем** и обозначается 0, а обратный элемент называется **противоположным** и обозначается $-x$ (если он существует). При этом X называется **аддитивным моноидом**. Это обозначение используется особенно часто, если моноид X **коммутативен**, т.е. если $x * y = y * x$ для любых $x, y \in X$.

Другая часто используемая нотация – **мультипликативная**. При этом операция называется **умножением** и обозначается знаком '$\cdot$', который, к тому же, обычно опускается, так что вместо $x * y$ пишут $x \cdot y$ либо просто xy. При этом операнды называются **сомножителями**, а результат – **произведением**. Нейтральный элемент называется обычно **единицей** и обозначается 1, а обратный элемент обозначается x^{-1} (если он существует). При этом X называется **мультипликативным моноидом**.

3. Первые примеры моноидов. Напомним встречавшиеся нам примеры моноидов. В следующем параграфе мы определим ключевые новые примеры, свободные моноиды и свободные коммутативные моноиды.

• **Мультипликативный моноид натуральных чисел.** Множество $\mathbb{N}$ является моноидом относительно умножения. При этом 1 является нейтральным элементом. **Основная теорема арифметики** утверждает, что $\mathbb{N}$ – свободный коммутативный моноид свободно порожденный множеством простых чисел (см. § ?). Этот пример чрезвычайно важен, так как многие встречающиеся в математике моноиды изоморфны моноиду $\mathbb{N}$.

• **Аддитивный моноид неотрицательных целых чисел.** Множество $\mathbb{N}$ не является моноидом относительно сложения, так как оно не содержит нейтрального элемента. Множества с одной всюду определенной ассоциативной бинарной операцией называются **полугруппами** ('моноиды без единицы'). Таким образом, $\mathbb{N}$ – аддитивная полугруппа, а $\mathbb{N}_0$ – аддитивный моноид. В действительности $\mathbb{N}_0$ – свободный моноид свободно порожденный 1.

• **Симметрический моноид.** Моноиды, рассмотренные в двух предыдущих примерах, коммутативны. Приведем теперь важнейший пример некоммутативного моноида. Пусть Y – какое-то множество и $X = \mathrm{Map}(Y, Y)$. Тогда X является моноидом относительно композиции отображений: $(X, \circ, \mathrm{id}_Y)$. При $n \geq 2$ этот моноид некоммутативен.

• **Моноид бинарных отношений.** Пусть теперь $X = \mathrm{Rel}(Y)$. Снова композиция определяет на X структуру моноида, нейтральным элементом которого является тождественное отношение.

• **Противоположный моноид.** Определим на моноиде $(X, *, e)$ новую операцию $\circ$, полагая $x \circ y = y * x$ для любых $x, y \in X$. Тогда $(X, \circ, e)$ также является моноидом, называемым моноидом, **противоположным** к X и обозначаемым X^o.

• **Мультипликативный моноид кольца.** Пусть R – произвольное ассоциативное кольцо с 1. Забывая о том, что на R определено сложение, и рассматривая R только с операцией умножения, мы получаем мультипликативный моноид. Однако обычно выражение мультипликативный моноид кольца R употребляется в следующей ситуации. Пусть R – целостное кольцо. Это означает, что $xy \neq 0$ для любых $x, y \in R \setminus \{0\}$. Таким образом, для целостного кольца $R \setminus \{0\}$ будет образовывать моноид относительно умножения. В качестве примеров можно рассмотреть $\mathbb{Z} \setminus \{0\}$ или $K[t] \setminus \{0\}$, где $K[t]$ – кольцо многочленов над полем.

• **Моноид функций и моноид подмножеств.** Все перечисленные в §§ ? – ? общие конструкции применимы к моноидам. Например, если $(Z, *, e)$ – моноид, а Y – любое множество, то $X = \mathrm{Map}(Y, Z)$ также снабжается структурой моноида, в котором операция задается как операция на функциях, т.е. $(f * g)(y) = f(y) * g(y)$ для любого $y \in Y$, а нейтральным элементом является функция, тождественно равная e. Как другой пример укажем, что $X = 2^Z$ является моноидом относительно закона композиции $A * B = \{a * b \mid a \in A, b \in B\}$, нейтральным элементом которого является $\{e\}$.

4. Моноид классов гомеоморфизма связных компактных поверхностей. Пусть M – множество классов гомеоморфизма связных компактных поверхностей. Тогда M является коммутативным моноидом относительно операции связной суммы, нулевым элементом которого является класс изоморфизма сферы. Напомним, что **связная сумма** двух компактных поверхностей X и Y определяется следующим образом: в X и Y вырезаются *маленькие* открытые диски, после чего получившиеся поверхности склеиваются по границам этих дисков. Пусть P, K и T – классы изоморфизма (вещественной) проективной плоскости, бутылки Клейна и тора, соответственно.

Задача. Элементарная топология учит нас, что M порождается классами P и T (т.е. любая компактная поверхность получается из сферы приклеиванием 'пленок' и 'ручек'), причем T порождает в M подмоноид, изоморфный $\mathbb{N}_0$, а именно, nT – это компактная *ориентированная* поверхность с n ручками. Кроме того, $2P = K$, а $3P = P + K = P + T$. Вывести отсюда, что вообще $(2n+1)P = P + nT$, а $(2n+2)P = K + nT$ и, тем самым, любой элемент M **однозначно** представляется в виде $mP + nT$, где $m = 0, 1, 2$, а $n \in \mathbb{N}_0$.

§ 4. Обратимые элементы

Прежде, чем перейти к дальнейшим примерам, введем еще два **чрезвычайно** важных определения, иллюстрирующие роль ассоциативности.

1. Обратимые элементы. Пусть $x \in X$. Говорят, что x **обратим слева**, если существует такое $y \in X$, что $y * x = e$. В этом случае y называется **левым**

обратным для x. Аналогично определяются **обратимость справа** и **правые обратные**. А именно, z называется правым обратным для x, если $x*z=e$. Элемент, для которого существует левый или правый обратный называется **односторонне обратимым**. Вообще говоря, для элемента может существовать много односторонних обратных (либо не существовать ни одного). Но в моноидах левый обратный обязан совпадать с правым, если оба существуют.

Лемма. *Пусть $(X,*)$ – моноид и $x\in X$. Если y – левый обратный, а z – правый обратный для x, то $y=z$.*

Доказательство. В самом деле, $y=y*e=y*(x*z)=(y*x)*z=e*z=z$.

Заметим, что в этом доказательстве **самым** существенным образом использована ассоциативность операции в X. В Главе 2 мы приведем примеры, показывающие, что у бесконечной матрицы может существовать бесконечно много двусторонних обратных. Разумеется, это возможно **только** потому, что умножение бесконечных матриц неассоциативно.

Следствие. *Если у элемента $x\in X$ существует больше одного левого/правого обратного, то у него не существует правого/левого обратного.*

Предостережение. Существование единственного левого обратного необходимо, но не достаточно для обратимости. Приведите контр-пример!!

Задача. Рассмотрим симметрический моноид $\mathbb{N}^{\mathbb{N}}$. Докажите, что у отображения $\phi:\mathbb{N}\longrightarrow\mathbb{N}$, $n\mapsto n+1$, бесконечно много левых обратных.

Ответ. Левые обратные к ϕ имеют вид ψ_m, где $\psi_m(n)=n-1$ для $n\geq 2$, а $\psi_m(1)=m$.

Определение. *Пусть $(X,*)$ – моноид. Элемент $x\in X$ называется* **обратимым**, *если он обратим как слева, так и справа, т.е. если найдется такой $y\in X$, что $y*x=e=x*y$. В этом случае y называется* **обратным** *к x.*

Иногда эмфатически говорят о **двусторонне обратных**. Термин ‘обратный’ подсказан, конечно, обозначением $*$ как умножения, см. ниже. Более педантичные авторы говорят в общем случае об y как о **симметричном** к x элементе. В любом моноиде есть по крайней мере один обратимый элемент, а именно сам e, называемый **тривиальным** обратимым элементом.

Элемент x моноида X называется **инволюцией**, если $x^2=e$. Тем самым, инволюция – это такой обратимый элемент моноида, что $x^{-1}=x$.

Задача. Докажите, что произведение двух коммутирующих инволюций снова является инволюцией. Тем самым, инволюции в коммутативном моноиде M образуют подгруппу в группе M^* его обратимых элементов.

Элемент моноида называется **идемпотентом**, если $x^2=x$.

Задача. Может ли идемпотент быть обратимым?

§ 5. Регулярные элементы

1. Регулярные элементы. Элемент x моноида X называется **регулярным слева**, если для любых $a,b\in X$ из $x*y=x*z$ вытекает $y=z$. Аналогично, x называется **регулярным справа**, если из $y*x=z*x$ вытекает $y=z$. Иными словами, элемент x регулярен слева/справа, если на него можно **сокращать слева/справа**. Элемент называется **регулярным**, если он регулярен слева и

справа. Таким образом, на регулярный элемент можно сокращать как слева, так и справа.

Из § ? Главы 0 мы знаем, что элемент симметрического моноида $\mathrm{Map}(X, X)$ в том и только том случае регулярен, когда он является биекцией. Как показывает пример 4.6, даже в коммутативном случае не каждый элемент моноида регулярен. А именно, классы гомеоморфизма проективной плоскости P и бутылки Клейна K **не являются регулярными** элементами моноида M. В самом деле, $P + K = P + T$ и $K + K = K + T$, в то время как $K \neq T$.

• Все элементы $\mathbb{R}$ регулярны относительно сложения.

• Все элементы $\mathbb{R}$, кроме 0 регулярны относительно умножения ('на ноль сокращать нельзя').

• $f \in X^X$ регулярно слева в том и только том случае, когда f инъекция.

• $f \in X^X$ регулярно справа в том и только том случае, когда f сюръекция.

• $f \in X^X$ регулярно в том и только том случае, когда f биекция.

• $\varnothing$ является единственным регулярным элементом относительно $\cap$ в 2^X.

• X является единственным регулярным элементом относительно $\cup$ в 2^X.

2 . Моноид с сокращением. Моноид M называется моноидом с сокращением, если все его элементы регулярны. Иными словами, для любых $x, y, z \in M$ из равенства $xy = xz$ следует $y = z$, а из равенства $xz = yz$ следует $x = y$. Ясно, что M в том и только том случае моноид с сокращением, когда для каждого $x \in M$ левая трансляция $L_x : M \longrightarrow M$, $y \mapsto xy$, и правая трансляция $R_x : M \longrightarrow M$, $y \mapsto yx$, инъективны.

3. Обратимые и регулярные элементы. На регулярный элемент можно сокращать, но это не значит, что он обратим. Например, **все** элементы мультипликативного моноида $\mathbb{N}$ и аддитивного моноида $\mathbb{N}_0$ регулярны, в то время как никаких нетривиальных обратимых элементов там нет. Однако из ассоциативности вытекает, что обратимый элемент обязательно регулярен.

Лемма. *Обратимый слева/справа элемент регулярен слева/справа.*

Доказательство. Пусть, например, w – левый обратный к x. Домножив обе части равенства $x * y = x * z$ на w, и воспользовавшись ассоциативностью, получаем,

$$y = e * y = (w * x) * y = w * (x * y) = w * (x * z) = (w * x) * z = e * z = z.$$

Доказательство для случая, когда x обратим справа, аналогично.

Задача. Докажите, что если $x \in X$ обратим слева/справа и регулярен справа/слева, то он обратим.

Решение. Пусть $yx = 1$. Тогда $(xy)x = x(yx) = x = 1x$. Следовательно, $xy = 1$.

§ 6. Гомоморфизм

1. Булевы полурешетки, изоморфизм моноидов. Пусть $X = 2^Z$ – множество подмножеств какого-то фиксированного множества Z. Тогда X является моноидом относительно объединения и пересечения. Точнее, на X определены две структуры моноида $(X, \cup, \varnothing)$ и $(X, \cap, Z)$. Как они связаны между собой? Следующее понятие является *архетипичным* и будет в дальнейшем возникать в разных ситуациях.

Определение. *Пусть* $(X, *_X, e_X)$ *и* $(Y, *_Y, e_Y)$ *– два моноида. Отображение* $f : X \longrightarrow Y$ *называется* **гомоморфизмом** X *в* Y*, если* $f(e_X) = e_Y$ *и для любых* $x, y \in X$ *выполняется равенство* $f(x *_X y) = f(x) *_Y f(y)$*. Биективный гомоморфизм называется* **изоморфизмом***. Моноиды* X *и* Y *называются* **изоморфными***, если существует изоморфизм* X *на* Y*.*

Слово 'гомоморфизм' образовано от греческих корней '$\grave{o}\mu\grave{o}\varsigma$ – 'равный', 'подобный' и $\mu o\rho\varphi\grave{\eta}$ – 'форма', 'тип'. Первый компонент слова 'изоморфизм' – греческий корень $\grave{\iota}\sigma o\varsigma$ – 'тот же самый', 'равный'.

Рассмотрим отображение X в себя, переводящее подмножество $A \subseteq Z$ в его дополнение $Z \setminus A$ (обозначаемое обычно $\overline{A}$, A' либо $\mathbf{C}A$). Тогда очевидно $\overline{\varnothing} = Z$ и $\overline{Z} = \varnothing$, а **законы де Моргана** утверждают, что $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$ и $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$. Таким образом, взятие дополнения задает гомоморфизм моноида $(X, \cup, \varnothing)$ в моноид $(X, \cap, Z)$ (и, наоборот, моноида $(X, \cap, Z)$ в моноид $(X, \cup, \varnothing)$. Поскольку в действительности отображение $A \mapsto \overline{A}$ является биекцией X на себя, структуры моноида, заданные пересечением и объединением изоморфны.

§ 7. Полугруппа матричных единиц, грассманов моноид,

В этом параграфе мы построим менее тривиальные примеры полугрупп и моноидов, играющие колоссальную роль в дальнейшем.

1. Полугруппа матричных единиц. Сейчас мы определим вероятно вообще самую важную из всех полугрупп. Пусть X – произвольное множество, а 0 - элемент, не принадлежащий $X \times X$. Введем на множестве $M(X) = X \times X \cup \{0\}$ структуру **полугруппы с нулем**, полагая, что $0 \cdot (x, y) = 0 = (x, y) \cdot 0$ для всех $x, y \in X$, а $(x, y)(u, v) = (x, v)$, если $y = u$ и 0 в противном случае (проверьте, что это умножение действительно ассоциативно!).

В этом контексте элементы $X \times X$ обычно называются **матричными единицами** и обозначаются $(x, y) = e_{xy}$, $x, y \in X$, а формулу умножения записывают в виде $e_{xy}e_{uv} = \delta_{yu}e_{xv}$, где δ_{yu} – символ Кронекера, равный 1 при $y = u$ и 0 при $y \neq u$, при этом подразумевается, что $1 \cdot e_{xv} = e_{xv}$. Легко видеть, что если $|X| \geq 2$, то это умножение некоммутативно. Действительно, возьмем $x, y \in X$, $x \neq y$. Тогда $e_{xx}e_{xy} = e_{xy}$, в то время как $e_{xy}e_{xx} = 0$.

Замечание. Эта полугруппа является одним из важнейших объектов алгебры. А именно, алгебра матриц $M(n, R)$ над коммутативным кольцом R состоит из формальных линейных комбинаций матричных единиц e_{ij}, $i, j \in \underline{n} = \{1, \ldots, n\}$, с коэффициентами из R и с умножением, продолжающим умножение матричных единиц по линейности. Иными словами, квадратные матрицы являются функциями на $M(n) = M(\underline{n}) = \{0, e_{ij}, 1 \leq i, j \leq n\}$, отображающими $0 \in M(n)$ в $0 \in R$, причем умножение матриц задается как **свертка функций** посредством умножения на $M(n)$. На техническом языке кольцо квадратных матриц $M(n, R)$ представляет собой **сжатую полугрупповую алгебру** ('contracted semigroup algebra') полугруппы $M(n)$ над R. Замечательно, что хотя полугруппа $M(n)$ и не является моноидом, если $n \geq 2$, в алгебре матриц $M(n, R)$ единица появляется. А именно, роль единицы в $M(n, R)$ играет единичная матрица $e = e_{11} + \ldots + e_{nn}$ (т.е. функция, принимающая значение 1 на матричных единицах e_{ii} и 0 на всех остальных элементах полугруппы $M(n)$).

2. Грассманов моноид. Пусть X – некоторое множество, а 0 – символ, не принадлежащий 2^X. Определим на $G(X) = 2^X \cup \{0\}$ структуру моноида, полагая $A \vee B = A \cup B$, если $A \cap B = \varnothing$ и $A \vee B = 0$ в противном случае. Операция $\vee$ называется **внешним произведением** или **джойном** (от английского join). Заметим, что часто, следуя Анри Картану, операция в грассмановом моноиде обозначается двойственным образом, т.е. вместо $A \vee B$ пишется $A \wedge B$. Мы же, чтобы подчеркнуть аналогию с объединением и пересечением, обозначим через $\wedge$ операцию **мит** (от английского meet), определенную посредством $A \wedge B = A \cap B$, если $A \cup B = X$ и $A \wedge B = 0$ в противном случае.

Задача. 1) Доказать, что $\vee$ и $\wedge$ ассоциативны, а нейтральными элементами для них являются $\varnothing$ и X, соответственно.

2) Показать, что моноиды $(G(X), \vee)$ и $(G(X), \wedge)$ изоморфны.

Замечание. Грассманов моноид играет примерно такую же роль по отношению к внешней алгебре (которую мы изучаем в 3-м семестре) как полугруппа матричных единиц по отношению к алгебре матриц. Однако точно описать эту роль несколько сложнее, так как умножение во внешней алгебре подкручено при помощи знака ± 1.

§ 8. Свободные моноиды

1. Свободный моноид. Сейчас мы определим важнейший пример моноида, суть которого лучше всего проясняется следующей максимой Анатолия Моисеевича Вершика: “свободный моноид — это не моноид, это просто набор слов”. Эта фраза является не шуткой, а настоящим математическим определением. Как поясняет в этом месте Скотт Картер, “Mathematicians use the term “word” to mean any finite sequence of letters and numbers. This practice can freak out people who are not hip to the lingo”. Вот формальное определение для пешеходов.

Зафиксируем некоторое множество X, называемое в дальнейшем **алфавитом**. Элементы X называются **буквами**. **Словом** в алфавите X называется любая конечная последовательность букв. При этом не исключается и случай пустой последовательности, называемой также **пустым словом** и обозначаемой Λ (это не греческая буква Λ, а перевернутая буква V, от английского void[272]). Пусть $W(X)$ – множество всех слов в алфавите X. **Длина** слова $w \in W(X)$ это просто количество входящих в него букв, она обозначается обычно через $l(w)$. Например, если X – обычный латинский алфавит, то $l(bububu) = 6$.

Определим теперь операцию над словами, называемую конкатенацией (alias приписыванием) слов. Если w_1 и w_2 два слова, то их **конкатенацией** называется слово $w_1 * w_2$, получающееся приписыванием слова w_2 справа к слову w_1. При этом $l(w_1 * w_2) = l(w_1) + l(w_2)$. Например, если X – обычный русский алфавит, то

кон∗катенация=конка∗тенация=конкате∗нация=конкатенация.

Очевидно, что так определенная операция ассоциативна и имеет Λ в качестве нейтрального элемента (приписывание пустого слова к произвольному слову как справа, так и слева не меняет это слово). Таким образом, $W(X)$

[272]на самом деле, от итальянского vuoto.

превращается в моноид, называемый **свободным моноидом** в алфавите X. Говорят также, что $W(X)$ **свободно порождается** множеством X.

Все элементы этого моноида регулярны, но ни один из них, кроме пустого слова, не является обратимым. К этому моноиду применимы все данные выше определения. Например, можно говорить о степенях слов. В частности, $bububu = (bu)^3$. При $|X| \geq 2$ множение в этом моноиде настолько далеко от коммутативности, насколько это только возможно. Например, $ub \neq bu$ и $(bu)^3 \neq b^3u^3$.

2. Свободный коммутативный моноид.

§ 9. Действие моноида на множестве

Нас будут интересовать главным образом действия групп, но мы дадим основные определения в чуть большей общности. Впрочем, нужно иметь в виду, что многие простейшие свойства групповых действий существенным образом зависят от того, что все выполняемые преобразования обратимы, и *не обобщаются* на действия моноидов.

1. Действие моноида. Начнем с основного определения.

Определение. *Пусть M – моноид, а X – множество. Говорят, что M* **действует на X слева**, *если задано отображение* $\mathrm{act} : M \times X \longrightarrow X$, $(f, x) \mapsto fx$, *такое, что*

1) **внешняя ассоциативность**: $(fg)x = f(gx)$ *для всех* $f, g \in M$, $x \in X$;

2) **унитальность**: $ex = x$.

*При этом X называется M-***множеством**.

Про элемент fx говорят, что он получается из x **применением** элемента f или что он является **образом** x под действием f. Иногда для действия моноида M на X используются и другие системы записи, например, образ x под действием f обозначается через $f + x$, $f \circ x$, $f \cdot x$, $f \bullet x$, $f(x)$, ${}^f x$ или как нибудь еще, но чаще всего мы будем использовать обычную мультипликативную запись.

Аналогично определяется **правое** действие $X \times M \longrightarrow X$ моноида M на множестве X. При этом внешняя ассоциативность приобретает вид $x(fg) = (xf)g$. Таким образом, различие состоит в том, что при левом действии первым действует *второй* множитель, а при правом действии первым действует *первый* множитель. Результат применения f к x при правом действии часто записывается еще как x^f, при этом внешняя ассоциативность выражается обычной формулой $x^{fg} = (x^f)^g$.

2. Связь правых и левых действий. Изучение правых действий легко сводится к изучению левых действий. В самом деле, пусть M^o – **противоположный** к M моноид. Напомним, как множество M^o совпадает с M, но при этом операция в M^o определяется как $f \circ g = gf$. Часто используется другое соглашение, а именно, чтобы подчеркнуть, что $f \in M$ рассматривается как элемент M^o, его обозначают через f^o, а операция в M^o записывается как умножение, но отображение $M \mapsto M^o$, переводящее f в f^o является не изоморфизмом, а **антиизоморфизмом**, т.е. $f^o g^o = (gf)^o$. Тогда правое действие M на X это по существу то же самое, что левое действие M^o на X. А именно, полагая $f^o x = xf$ мы превращаем правое M-множество в левое M^o-множество.

В дальнейшем мы будем как правило говорить лишь о левых действиях, имея в виду, что при помощи этой конструкции все определения и результаты автоматически переносятся и на правые действия.

3. Естественное действие моноида эндоморфизмов. Опишем важнейший пример действия моноидов, который, в действительности, является универсальным. А именно, пусть $M = \mathrm{End}(X) = \mathrm{Map}(X, X)$ – моноид **эндоморфизмов** множества X, т.е. всех отображений X в себя. В тех случаях, когда обозначение $\mathrm{End}(X)$ сопряжено с двусмысленностью (например, если множество X несет дополнительную структуру и эндоморфизмами называются лишь отображения X в себя, сохраняющие эту структуру), вместо $\mathrm{End}(X)$ используется обозначение $\mathrm{Map}(X, X)$ или X^X.

Тогда по самому определению M действует на X слева посредством $fx = f(x)$. В самом деле, операция в M *определяется* так, чтобы выполнялась внешняя ассоциативность. Действительно, умножение в M – это *композиция* отображений, для которой $(fg)(x) = f(g(x))$, но это и есть просто другая запись внешней ассоциативности. В свою очередь, унитальность это просто определение *тождественного отображения* $e = \mathrm{id}_X$. Это действие $\mathrm{End}(X)$ на X называется **естественным** действием $\mathrm{End}(X)$ на X. Сейчас мы увидим, что произвольное действие на множестве X выражается в терминах естественного действия $\mathrm{End}(X)$.

4. Действие на X как гомоморфизм в $\mathrm{End}(X)$. Пусть X есть M-множество. Зададим отображение $\theta_f = \theta_f^X : X \longrightarrow X$ посредством $x \mapsto fx$. Тогда внешняя ассоциативность означает, что $\theta_{fg} = \theta_f\theta_g$, в унитальность – что $\theta_e = \mathrm{id}_X$. Таким образом, отображение $\theta : M \longrightarrow \mathrm{End}(X)$, $f \mapsto \theta_f$, является гомоморфизмом моноидов. Обратно, если $\theta : M \longrightarrow \mathrm{End}(X)$, $f \mapsto \theta_f$, произвольный гомоморфизм моноидов, то, очевидно, формула $fx = \theta_f(x)$ задает левое действие моноида M на X. Этим устанавливается взаимно однозначное соответствие между всеми *левыми* действиями M на X и всеми *гомоморфизмами* M в $\mathrm{End}(X)$.

Так как правое действие M на X сводится к левому действию M^o на X, то существует такое же взаимно однозначное соответствие между *правыми* действиями M на X и *антигомоморфизмами* M в $\mathrm{End}(X)$.

5. Морфизмы M-множеств. Как всегда, как только вводится новый класс математических объектов, нужно сразу же определить допустимый класс отображений между этими объектами.

Определение. *Пусть X и Y суть два M-множества. Тогда отображение $\psi : X \longrightarrow Y$ называется* **морфизмом** *M-множеств или M-***эквивариантным** *отображением, если для любого $f \in M$ и любого $x \in X$ имеет место равенство $\psi(fx) = f\psi(x)$.*

В обозначениях предыдущего пункта эквивариантность означает, что для каждого $f \in M$ следующий квадрат отображений

$$\begin{array}{ccc} X & \xrightarrow{\theta_f^X} & X \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\psi} \\ Y & \xrightarrow[\theta_f^Y]{} & Y \end{array}$$

коммутативен, т.е. $\psi\theta_f^X = \theta_f^Y\psi$.

Множество всех M-эквивариантных отображений из X в Y бужет обозначаться через $\mathrm{Map}_M(X,Y)$. Биективное эквивариантное отображение называется **изоморфизмом** M-множеств. Два M-множества X и Y называются **изоморфными**, если существует изоморфизм $\psi : X \longrightarrow Y$. Одной из наших первых основных целей является классификация групповых действий с точностью до изоморфизма.

6. Тривиальное действие. Для любого моноида M и любого множества X отображение $M \longrightarrow \mathrm{End}(X)$, $f \mapsto \mathrm{id}_X$, является как гомоморфизмом, так и антигомоморфизмом (**тривиальный** гомоморфизм). Этому гомоморфизму отвечает **тривиальное** действие M на X, для которого $fx = x$ для всех $f \in M$, и всех $x \in X$.

7. Действие моноида на себе сдвигами. Еще один важнейший пример действия – действие моноида на себе сдвигами. Умножение в моноиде M определяет действие моноида M на себе **левыми сдвигами**. А именно, в этом случае $X = M$ и действие $M \times M \longrightarrow M$ определяется посредством $(f,x) \mapsto fx$. Иными словами, в этом случае $\theta_f = f_L : x \mapsto fx$ представляет собой умножение на f *слева*. При этом внешняя ассоциативность совпадает с ассоциативностью умножения в моноиде, а унитальность – это просто определение нейтрального элемента.

Аналогично можно определить действие моноида на себе **правыми сдвигами**, когда $\theta_f = f_R : x \mapsto xf$ представляет собой умножение на f *справа*. Используемые здесь символы f_L и f_R являются стандартными обозначениями левого и правого сдвига на f, соответственно. При этом, разумеется, 'L' является сокращением от 'Left', а 'R' – от 'Right'. Тот факт, что отображение $X \longrightarrow \mathrm{Map}(X,X)$, $f \mapsto f_L$, представляет собой гомоморифзм моноидов, представляет собой просто переформулировку ассоциативности и определения нейтрального элемента. Аналогично, $X \longrightarrow \mathrm{Map}(X,X)$, $f \mapsto f_R$, представляет собой антигомоморфизм моноидов.

8. Действие двойными сдвигами. Действие моноида на себе левыми и правыми сдвигами можно объединить в действие некоторого нового моноида. Напомним, что действие M на себе правыми сдвигами можно рассматривать как действие M^o на M *левыми* сдвигами: $(g^o,x) \mapsto g_R(x) = xg$. Так как левые и правые сдвиги коммутируют, $f_L g_R = g_R f_L$ для любых $f,g \in M$, то это действие можно объединить с действием M на себе девыми сдвигами. А именно, рассмотрим моноид $M \times M^o$. Тогда $M \times M^o$ действует на M посредством $((f,g^o),x) \mapsto fxg$. Иными словами, для этого действия $\theta_{(f,g^o)} = f_L g_R$.

§ 10. Группа Гротендика

1. Моноид разностей. Пусть $(M,+,0)$ – аддитивно записанный коммутативный моноид, S – подмоноид моноида M. Рассмотрим множество пар $M \times S$ и введем на нем отношение эквивалентности. Для $a,b \in M$, $u,v \in S$ мы полагаем

$$(a,u) \sim (b,v) \iff \exists w \in S, a+v+w = b+u+w,$$

Упражнение. Докажите, что это отношение эквивалентности является конгруэнцией относительно операции $+$.

Обозначим класс эквивалентности (a, u) через $[a - u]$. Так как это конгруэнция, то

$$[a - u] + [b - v] = [(a + b) - (u + v)]$$

корректно определяет сложение классов. Таким образом, $M_S = M \times S/\sim$ представляет собой моноид относительно этой операции, $0 = [0 - 0]$.

Отображение $M \longrightarrow M_S$, $a \mapsto [a - 0]$, является мономорфизмом моноидов, который в том и только том случае инъективен, когда S состоит из регулярных элементов, т.е. $a + u = b + u \Longrightarrow a = b$ для всех $a, b \in M$, $u \in S$. Элементы $[u - 0]$, $u \in S$, обратимы в M_S, так как $-[u - 0] = [0 - u]$.

Построенный так моноид M_S называется **моноидом разностей** (difference monoid, Differenzenmonoid). В случае, когда M записывается мультипликативно, вместо этого обычно говорят о **моноиде частных** (quotient monoid, Quotientenmonoid) – не путать с фактор-моноидом!!

2. Универсальное свойство. Моноид разностей можно охарактеризовать следующим универсальным свойством. Если $\phi : M \longrightarrow N$ – гомоморфзм моноидов такой, что $\phi(S) \subseteq N^*$, то существует единственный гомоморфизм моноидов $\phi_S : M_S \longrightarrow N$ такой, что диаграмма

$$\begin{array}{ccc} M & \xrightarrow{\iota} & M_S \\ & N & \end{array}$$

коммутативна: $\phi = \phi_S \circ \iota$. При этом $\psi_S([a - u]) = \phi(a) - \phi(u)$.

3. Группа Гротендика. Важнейший частный случай описанной выше конструкции состоит в следующем. В моноиде M_M все элементы обратимы, т.е. этот моноид в действительности является группой. Эта группа обозначается через $G(M)$ и называется **группой Гротендика** моноида M. Иными словами, группа Гротендика характеризуется следующими универсальными свойством

$$\begin{array}{ccc} M & \xrightarrow{\iota} & G(M) \\ & G & \end{array}$$

для любого гомоморфизма моноида M в абелеву группу G существует единственный гомоморфизм групп $\psi : G(M) \longrightarrow G$, такое, что $\phi = \psi \circ \iota$.

Отображение $\iota : M \longrightarrow G(M)$ в том и только том случае является вложением, когда M моноид с сокращением, т.е. все его элементы регулярны.

Сопоставление $G \rightsquigarrow G(M)$ функториально. Иными словами, любому гомоморфизму моноидов $\phi : M \longrightarrow N$ отвечает единственный гомоморфизм $G(\phi) : G(M) \longrightarrow G(N)$ такой, что

$$\begin{array}{ccc} M & \xrightarrow{\phi} & N \\ \downarrow & & \downarrow \\ G(M) & \xrightarrow[G(\phi)]{} & G(N) \end{array}$$

вертикальные стрелки которой – это канонические гомоморфизмы $a \mapsto [a-0]$. А именно, $G(\phi)$ определяется посредством $G(\phi)([a-b] = [\phi(a) - \phi(b)]$.

4. Примеры групп Гротендика. Следующие два примера групп Гротендика изучаются в младших классах средней школы.

- $\mathbb{N}_0$ – аддитивный моноид с сокращением, $G(\mathbb{N}_0) = \mathbb{Z}$.
- $\mathbb{N}$ – мультипликативный моноид с сокращением, $G(\mathbb{N}) = \mathbb{Q}_{>0}$.

5. Полукольца. В действительности, целые числа можно не только складывать, но и умножать. **Полукольцо** (semiring, Halbring) то непустое множество S с операциями $+$ и $\cdot$, причем S образует коммутативный моноид по $+$, а $\cdot$ двусторонне дистрибутивно относительно $\cdot$. Иными словами, в полукольце выполняются все аксиомы кольца, кроме аксиомы А3, гарантирующей существование противоположных элементов. Поэтому весьма суггестивно американское название полуколец **rig**, что переводится как 'ring without negatives'.

Задача. Пусть S – полукольцо, а $G(S)$ – группа Гротендика аддитивного моноида $S+$.

i) Вводя на $G(S)$ умножение формулой

$$[a-b] \cdot [c-d] = [(ac+bd) - (bc+ad)],$$

мы превращаем $G(S)$ в кольцо.

ii) Это единственная структура кольца на $G(S)$, относительно которой $\iota : S \longrightarrow G(S)$ является мультипликативным гомоморфизмом.

iii) Если $S^\times$ ассоциативно, то $G(S)$ ассоциативно.

Снова первый пример этой конструкции известен из младших классов начальной школы: $G(\mathbb{N}_0) = \mathbb{Z}$ как кольца, а не только как адиитивные группы.

Тема 5. ОБОБЩЕНИЯ ПОНЯТИЯ ОПЕРАЦИИ

До сих пор мы имели дело преимущественно с наиболее важным случаем внутренних бинарных операций. Сейчас мы коротко обсудим унарные операции и внутренние операции высших арностей, а также внешние операции, операции бесконечной арности и частичные операции. При этом мы ограничимся обсуждением нескольких примеров.

§ 1. Нульарные операции

Как мы установили в § 1, нулевая степень любого непустого множества равна $\{\varnothing\}$, так что нульарная операция сводится к выбору константы в X. Наиболее важными константами являются, конечно, 0 и 1 (которые могут принимать в разных контекстах разные обличия, например, 0 для объединения множеств – это $\varnothing$, а 1 для композиции отображений – это id, см. следующий параграф). Тремя константами в алгебре отношений являются тривиальное, тождественное и тотальное отношения. Еще одна важнейшая константа в Z – это база системы счисления, среди которых наиболее употребимыми являются 2 (двоичная система), 8 (восьмеричная система), 10 (десятичная система), 16 (шестнадцатиричная система, используемая обычно в компьютерах), 60 (вавилонская шестидесятиричная система, рефлексы которой сохранились в измерении времени, углов, etc.). Тремя другими замечательными константами в поле $\mathbb{C}$ комплексных чисел являются мнимая единица i, основание натурального логарифма e и число π. Одной из самых красивых в математике является формула Эйлера, связывающая все эти константы между собой: $e^{\pi i} = -1$, см. Главу 3.

Пусть теперь A и B – два множества с отмеченной точкой.

Определение. Букетным произведением *$A \vee B$ множеств A и B с отмеченной точкой называется их амальгамированная сумма $A \coprod_C B$ под одноэлементным множеством $C = \{*\}$.*

Чтобы $A \coprod_C B$ было множеством с отмеченной точкой, отображения f и g здесь должны быть морфизмами множеств с отмеченной точкой и, поэтому определены однозначно: $f(*) = *_A \in A$, $g(*) = *_B \in B$. Тогда $A \coprod_C B$ представляет собой фактор $A \coprod B$ по отношению эквивалентности, все классы которого одноэлементны, за исключением ровно одного двухэлементного класса $\{(*_A, 1), (*_B, 2)\}$, который и является отмеченной точкой фактор-множества $A \coprod B/\sim_C$. Таким образом, $A \coprod_C B$ можно представлять себе как свободное объединение множеств A и B, в котором отмеченная точка $*_A \in A$ отождествлена с отмеченной точкой $*_B \in B$.

2. Примеры букетных произведений. Ниже нарисовано букетное произведение двух окружностей и букетное произведение двух отрезков, выделенные точки которых являются их серединами.

картинка — картинка – картинка

3. Вложение букетного произведения в прямое произведение. Заметим, что букетное произведение множеств с отмеченной точкой может быть естественным образом реализовано не только как *фактор-множество* свободного объединения соответствующих множеств, но и как *подмножество* их прямого произведения. А именно, букетное произведение A и B проще всего представлять себе как

$$A \vee B = \{(a, *_B) \in A \times B \mid a \in A\} \cup \{(*_A, b) \in A \times B \mid b \in B\}.$$

Совершенно ясно, что два множества, объединение которых рассматривается в правой части, пересекаются ровно по одному элементу, а именно, по $(*_A, *_B)$.

4. Смятое произведение множеств с отмеченной точкой. Смятым произведением (smash product) множеств с отмеченной точкой A и B называется фактор-множество $A \sharp B = A \times B/\sim$ их прямого произведения $A \times B$ по наименьшему отношению эквивалентности $\sim$, для которого все элементы $A \vee B$ попадают в один класс. Это отношение эквивалентности определяется следующим образом: $(a_1, b_1) \sim (a_2, b_2)$, в том и только том случае, когда $(a_1, b_1) = (a_2, b_2)$ или $(a_1, b_1), (a_2, b_2) \in A \vee B$. Смятое произведение довольно интересная операция.

Задача. Убедитесь, что $S^1 \sharp S^1 \cong S^2$.

§ 2. Унарные операции

2. Унарные операции. По определению **унарная операция** это просто отображение $f : X \longrightarrow X$. Однако обычно термин 'унарная операция' применяется не к произвольным отображениям такого вида, а только к отображениям, либо естественно связанным с бинарными операциями, либо удовлетворяющим особенно простым *функциональным уравнениям*. Отметим два наиболее важных и часто используемых тождества:

• **Инволютивность** $f \circ f = \mathrm{id}$. Таким образом, для инволютивной операции $f(f(x)) = x$ для любого $x \in X$.

• **Идемпотентность** $f \circ f = f$. Таким образом, для идемпотентной операции $f(f(x)) = f(x)$ для любого $x \in X$.

3. Примеры унарных операций. Вот несколько примеров инволютивных операций:

• **Противоположный элемент** $x \mapsto -x$

• **Обратный элемент** $x \mapsto x^{-1}$

• **Симметричная точка на сфере** Пусть S^n – n-мерная сфера единичного радиуса (например, S^2 – обычная сфера в трехмерном пространстве) и $x \mapsto x'$ – переход к симметричной точке.

• **Симметричное отношение.** Пусть $X = \mathrm{Rel}(X)$ – бинарное отношение и $R \mapsto R'$ – переход к симметричному отношению.

• **Комплексное сопряжение.** Здесь $X = \mathbb{C}$ и $z \mapsto \overline{z}$.

Следующие операции идемпотентны.

• **Абсолютная величина. идемпотентна**: $||f|| = |f|$.

• **Положительная и отрицательная часть.** $f^+ = f \cup 0$, $f^- = -f \cup 0$, иными словами,

$$f^+(x) = \begin{cases} f(x), & \text{если } f(x) \geq 0, \\ 0, & \text{если } f(x) < 0. \end{cases}$$

$$f^-(x) = \begin{cases} -f(x), & \text{если } f(x) \leq 0, \\ 0, & \text{если } f(x) > 0. \end{cases}$$

Покажите, что $f = f^+ - f^-$.

• **Кванторы существования и всеобщности.** Пусть x – переменная, а f – формула, содержащая эту переменную. Тогда $\exists_x f$ и $\forall_x f$ также представляют собой формулы.

• **Дифференцирование.** Пусть $K[t]$ – кольцо многочленов от одной переменной, положим $f \mapsto df/dt$.

3. Теорема косинусов.

• **Квадрат.** $x \mapsto x^2$.

В коммутативном кольце R таком, что $2 \in R^*$, умножение выражается в терминах сложения и квадрата, соответствующая формула называется **теоремой косинусов**:

$$xy = \frac{1}{2}((x+y)^2 - x^2 - y^2).$$

Эти свойства широко используются для проверки того что некоторое подмножество коммутативного кольца (например, кольца функций) само является кольцом относительно тех же операций.

В общем случае, когда кольцо R не коммутативно и/или $2 \notin R^*$ через сложение и квадрат можно выразить лишь **антикоммутатор** в R:

$$x \circ y = xy + yx = (x+y)^2 - x^2 - y^2.$$

4. Унарные операции на матрицах. Вот несколько наиболее известных унарных операций на матрицах.

• **Транспонированная матрица.** Пусть K произвольное поле. Транспонирование $x \mapsto x^t$, сопоставляет матрице $x = (x_{ij}) \in M(n, K)$ ее транспонированную x^t, у которой на метсе (i, j) стоит x_{ij}. Для матриц степени 2

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^t = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

• **Сопряженная матрица.** Пусть K – поле с инволюцией $z \mapsto \overline{z}$, например, $K = \mathbb{C}$ – поле комплексных чисел, $\overline{z}$ – комплексное сопряжение. Сопряжение $x \mapsto \overline{x}$ сопоставляет матрице $x = (x_{ij}) \in M(n, K)$ сопряженную матрицу $\overline{x}$, у которой на месте (i, j) стоит $\overline{x}_{ij}$. Для матриц степени 2:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^t = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}.$$

• **Эрмитовски сопряженная матрица.** Пусть, по-прежнему, K – поле с инволюцией $x \mapsto \overline{x}$. Тогда $x \mapsto x^*$ сопоставляющее матрице $x \in M(n, K)$ ее эрмитовски сопряженную, определяет инволютивную бинарную операцию на $M(n, K)$.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^* = \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix}.$$

• **Присоединенная матрица.**

Следующие две операции определены на множестве $\mathrm{GL}(n, K)$ обратимых матриц.

• **Обратная матрица.**

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

• **Контраградиентная матрица.**

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^* = \frac{1}{ad - bc} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}.$$

• **Гессиан.** Пусть f – функция n переменных $x_1, \ldots, x_n$. Тогда определитель

$$H(f) = \det \begin{pmatrix} \dfrac{\partial^2 f}{\partial x_1 \partial x_1} & \cdots & \dfrac{\partial^2 f}{\partial x_1 \partial x_n} \\ & \cdots & \\ \dfrac{\partial^2 f}{\partial x_n \partial x_1} & \cdots & \dfrac{\partial^2 f}{\partial x_n \partial x_n} \end{pmatrix},$$

где $\dfrac{\partial^2 f}{\partial x_i \partial x_j}$ обозначает вторую частную производную f_i по x_i и x_j, сам является функцией переменных $x_1, \dots, x_n$, называемой **гессианом** функции f. Этот определитель был введен О.Гессе в 1844 году.

Предостережение. В теории Морса термин гессиан часто применяется к самой матрице $\left(\dfrac{\partial^2 f}{\partial x_i \partial x_j}\right)$, а также к квадратичной форме с этой матрицей. Видимо, чтобы различать эти понятия, было бы правильнее говорить **определитель Гессе**, **матрица Гессе**, **форма Гессе**. Кроме того, в теории функций нескольких комплексных переменных рассматривается **комплексный гессиан** $\left(\dfrac{\partial^2 f}{\partial z_i \partial \overline{z}_j}\right)$.

4. Унарные операции в топологии. Следующие четыре примера возникают в топологии. Пусть $X = 2^Z$ – множество подмножеств множества Z. Топологию на Z можно описать в терминах некоторых унарных операций на X. Операция дополнения инволютивна, а операции внутренности и замыкания идемпотентны.

- **Дополнение.** $Y \mapsto Z \setminus Y$
- **Внутренность.** $Y \mapsto \mathrm{Int}(Y)$
- **Замыкание.** $Y \mapsto \mathrm{Clos}(Y)$
- **Граница.** $Y \mapsto \mathrm{Fr}(Y)$

Отображение Fr удовлетворяет тождеству $\mathrm{Fr} \circ \mathrm{Fr} \circ \mathrm{Fr} = \mathrm{Fr} \circ \mathrm{Fr}$, аналогичному тождеству идемпотентности, иными словами, для любого подмножества $Y \subseteq Z$ имеем $\mathrm{Fr}(\mathrm{Fr}(\mathrm{Fr}(Y))) = \mathrm{Fr}(\mathrm{Fr}(Y))$.

Задача. Покажите, что переход к дополнению является изоморфизмом $(2^Z, \mathrm{Clos})$ и $(2^Z, \mathrm{Int})$, а именно,

$$\mathrm{Clos}(\overline{Y}) = \overline{\mathrm{Int}(Y)}, \qquad \mathrm{Int}(\overline{Y}) = \overline{\mathrm{Clos}(Y)}.$$

§ 4. Операции высших арностей

1. Внутренние n-арные операции. Напомним, что **внутренней n-арной операцией** на X называется любое отображение $f : X \times \ldots \times X \longrightarrow X$. На элементарном уровне довольно затруднительно привести *содержательные* примеры внутренних тернарных операций и операций более высокой арности, за исключением операций, очевидным образом получающихся суперпозицией бинарных операций. Заметим, впрочем, что такие содержательные примеры существуют – и мы встретим некоторые из них в полилинейной алгебре. Приведем пока несколько бессодержательных примеров.

- **Проекции.** Пусть $X \times \ldots \times X$ – произведение n экземпляров множества X, а $\mathrm{pr}_j : X \times \ldots \times X \longrightarrow X$, $(x_1, \dots, x_n) \mapsto x_j$ –проекция на j-й множитель.

2. Производные операции. Если на множестве X заданы несколько бинарных операций, то комбинируя их можно получать операции более высокой арности, например, $(x, y, z) \mapsto x + yz$. Известными примерами таких **производных операций** являются

- взятие **среднего арифметического**

$$(x_1, \dots, x_n) \mapsto \frac{x_1 + \ldots + x_n}{n}$$

или **среднего геометрического**

$$(x_1, \dots, x_n) \mapsto \sqrt[n]{x_1 \dots x_n}.$$

- **Полиномиальные функции.** Пусть K – поле, $f \in K[x_1, \dots, x_n]$ – многочлен от n переменных над K. Тогда f определяет полиномиальное отображение $\widetilde{f} : K \times \ldots \times K \longrightarrow K$, $c = (c_1, \dots, c_n) \mapsto f(c_1, \dots, c_n)$, которое можно

рассматривать как n-арную операцию на K. Эта операция является производной по отношению к бинарным операциям сложения и умножения и нескольким нульарным операциям (константы, равные коэффициентам многочлена f).

Отметим пока еще один пример, который обьясняет, как операции более высокой арности могут возникать из бинарных операций не на самом множестве X, а на каком-то большем множестве.

• **Операции на смежных классах по подгруппе.** Рассмотрим множество $X = 2^Z$ четных чисел. Сумма двух нечетных чисел четна, но сумма **трех** нечетных чисел снова нечетна, так что $(x, y, z) \mapsto x + y + z$ представляет собой **тернарную** операцию на X. Точно такая же конструкция применима к множеству $S_n \setminus A_n$ всех нечетных перестановок. Произведение двух нечетных перестановок является четной перестановкой, но произведение **трех** нечетных перестановок снова нечетно. Поэтому на множестве нечетных перестановок имеется естественное **тернарное** произведение.

3. Содержательные примеры n-арных операций. Все рассматривавшиеся до сих пор примеры носят несколько искусственный характер, но вот нетривиальный и *весьма содержательный* пример производной тернарной операции.

• **Тензор кривизны.** Пусть M – дифференцируемое многообразие, на котором задана линейная связность ∇. Определим на $\mathrm{Vect}(M)$ тернарный закон композиции R, полагая

$$R(X, Y, Z) = \nabla(X, \nabla(Y, Z)) - \nabla(Y, \nabla(X, Z)) - \nabla([X, Y], Z).$$

В дифференциальной геометрии этот закон композиции обычно называется **тензором кривизны**.

Комментарий. В общей теории относительности этот закон композиции принято называть **тензором Римана-Кристоффеля**, отсюда обозначающая его буква R. Смысл этой операции очень наглядно обьясняется в книге В.И.Арнольда[273]. А именно, при обходе вдоль маленьких параллелограммов, задаваемых в каждой точке $x \in M$ касательными векторами X и Y, вектор Z переходит в вектор $R(X, Y, Z)$. *На первый взгляд* векторные поля X и Y, с одной стороны, и поле Z, с другой стороны, участвуют в этом определении совершенно несимметричным образом. Однако в действительности, для реально рассматриваемых в римановой геометрии связностей, операция R удовлетворяет нескольким *совершенно замечательным тождествам*, в частности **тождеству Якоби**:

$$R(X, Y, Z) + R(Y, Z, X) + R(Z, X, Y) = 0,$$

показывающим, среди прочего, полное равноправие векторных полей X, Y и Z.

Два следующих примера n-арных операций определяются в терминах определителя. Они естественно возникают во многих вопросах алгебры, анализа, дифференциальной геометрии и топологии, и теории дифференциальных уравнений.

• **Якобиан.** Пусть $f_1, \dots, f_n$ – функции n переменных $x_1, \dots, x_n$. Тогда определитель

$$J(f_1, \dots, f_n) = \det \begin{pmatrix} \dfrac{\partial f_1}{\partial x_1} & \cdots & \dfrac{\partial f_1}{\partial x_n} \\ & \cdots & \\ \dfrac{\partial f_n}{\partial x_1} & \cdots & \dfrac{\partial f_n}{\partial x_n} \end{pmatrix},$$

где $\dfrac{\partial f_i}{\partial x_j}$ обозначает частную производную f_i по x_j, сам является функцией переменных $x_1, \dots, x_n$, называемой **якобианом** функций $f_1, \dots, f_n$.

[273]В.И.Арнольд, Математические методы классической механики, 1979, Приложение 1.

• **Вронскиан.** Пусть $f_1, \dots, f_n$ – функции одной переменной x. Тогда определитель

$$W(f_1, \dots, f_n) = \det \begin{pmatrix} f_1 & \dots & f_n \\ f_1' & \dots & f_n' \\ & \dots & \\ f_1^{(n-1)} & \dots & f_n^{(n-1)} \end{pmatrix},$$

где $f_i^{(j)}$ обозначает j-ю производную f_i по x, сам является функцией x, называемой **вронскианом** функций $f_1, \dots, f_n$.

§ 5. 'Общая' алгебра

Одно из определений алгебры, которое приходится слышать, состоит в следующем: "Алгебра - это наука о множествах с заданными на них операциями". Действительно, такие множества называются **универсальными алгебрами** (в смысле Биркгофа) и изучаются разделом алгебры, известным под названием 'универсальной' или 'общей' алгебры[274,275]. Иногда цель этого раздела формулируется чуть более широко, как изучение **алгебраических систем**, т.е. множеств с заданными на них операциями и отношениями[276]. Пусть X – множество с заданными на нем операциями арностей $n_1, \dots, n_t$, соответственно. В этом случае говорят, что X – универсальная алгебра **сигнатуры** $(n_1, \dots, n_t)$.

Приведем несколько примеров универсальных алгебр

• **полугруппа**: сигнатура (2) (умножение),

• **моноид**: сигнатура $(2, 0)$ (умножение и нейтральный элемент),

• **группа**: сигнатура $(2, 1, 0)$ (умножение, обратный элемент, нейтральный элемент),

• **кольцо**: сигнатура $(2, 2, 1, 0)$ (сложение, умножение, противоположный элемент, 0),

• **кольцо Ли**: сигнатура $(2, 2, 1, 0)$ (сложение, скобка Ли, противоположный элемент, 0),

• **кольцо с 1**: сигнатура $(2, 2, 1, 0, 0)$ (сложение, умножение, противоположный элемент, 0 и 1),

• **решетка**: сигнатура $(2, 2)$ (супремум и инфимум),

• **ограниченная решетка**: сигнатура $(2, 2, 0, 0)$ (супремум, инфимум, 0 и 1),

• **булева алгебра**: сигнатура $(2, 2, 1, 0, 0)$ (объединение, пересечение, дополнение, 0 и 1).

Рассматриваются и алгебры с большим числом операций, скажем, например,

• **алгебра Пуассона**: сигнатура $(2, 2, 2, 1, 0, 0)$ (сложение, ассоциативное умножение, скобка Пуассона, противоположный элемент, 0 и 1)

• **реляционная алгебра**: сигнатура $(2, 2, 2, 1, 1, 0, 0, 0)$ (объединение, пересечение, композиция, дополнение, транспонирование, тривиальное отношение, тождественное отношение и тотальное отношение).

Однако в действительности проблематика 'универсальной алгебры' составляла исчезающе малую часть алгебраических исследований. Основная масса содержательных результатов относилась к полудюжине классических структур, таких как **группы**, **поля**, **решетки**, **ассоциативные кольца**, **алгебры Ли** и связанные с ними **алгебры близкие к ассоциативным (йордановы, альтернативные)**, **модули**. В последние десятилетия к этому можно добавить еще **коалгебры** и **алгебры Хопфа**, которые, кстати, вообще не являются 'универсальными алгебрами' в указанном выше смысле, так как их структура задается другими отображениями , не являющимися 'алгебраическими операциями', в смысле данного выше определения. Как замечает И.Р.Шафаревич [Sh], действительно интересный вопрос состоит не в том, чтобы дать подобное схоластическое определение, а в том, чтобы понять, почему *именно эти* структуры приобрели такое значение.

В римановой геометрии, где есть возможность поднятия и опускания индексов, любое тензорное поле валентности $n+1$ может рассматриваться как n-арная алгебраическая операция на $\mathrm{Vect}(X)$. В отсутствие же метрики это не так. Упомянутые выше и другие подобные им структуры задаются тензорами вида $A \otimes \dots \otimes A \longrightarrow A \otimes \dots \otimes A$, которые не сводятся к обычным алгебраическим операциям вида $A \otimes \dots \otimes A \longrightarrow A$.

---

[274] П.Кон, Универсальная алгебра. – М., Мир, 1968, с.1–351.

[275] А.Г.Курош, Лекции по общей алгебре, М., 1962, с.1–396.

[276] А.И.Мальцев

§ 6. Внешние бинарные операции

Для начала вернемся к определению алгебраической операции. Как мы уже отмечали, в самом общем виде алгебраическая операция – это просто отображение $f : X_1 \times \ldots \times X_n \longrightarrow Y$, где $X_1, \ldots, X_n$ суть непустые множества. Однако при этом до сих пор мы рассматривали преимущественно случай, когда, во-первых, $n = 2$ (т.е. операция f бинарна), и, во-вторых, $X_1 = X_2 = Y$ (т.е. операция f внутренняя). Сейчас мы приведем несколько примеров **внешних бинарных** операций, когда, по-прежнему, $n = 2$, но множества X_1, X_2 и Y могут быть различны.

Нам встречались уже следующие примеры.

• **Композиция отношений.** Пусть снова X, Y, Z – три множества. Тогда определена операция $\mathrm{Rel}(X, Y) \times \mathrm{Rel}(Y, Z) \longrightarrow \mathrm{Rel}(X, Z)$, $(R, S) \mapsto R \circ S$, сопоставляющее паре бинарных отношений их композицию.

• **Сворачивание индекса.** Операция в полугруппе матричных единиц допускает следующее обобщение, лежащее в основе умножения неквадратных матриц. Пусть X, Y, Z – три множества, а 0 – элемент, не принадлежащий $X \times Z$. Зададим отображение $(X \times Y) \times (Y \times Z) \longrightarrow X \times Z \cup \{0\}$, полагая для любых $(x, y) \in X \times Y$ и $(u, z) \in Y \times Z$ их произведение $(x, y)(u, z)$ равным (x, z), если $y = u$, и равным 0 в противном случае.

• **Джойн.** Пусть X – произвольное множество, тогда определена операция $\star : X^m \times X^n \longrightarrow X^{m+n}$ известная как **джойн** или **соединение** списков (list join):

$$(x_1, \ldots, x_m) \star (y_1, \ldots, y_n) = (x_1, \ldots, x_m, y_1, \ldots, y_n).$$

Комментарий. Первым математиком, который **сознательно** использовал внешние алгебраические операции, был, по всей видимости, Мебиус. В опубликованном в 1827 году ‘Барицентрическом исчислении’ он рассматривал операции над векторами и точками (сумма точки и вектора, разность двух точек, и т.д.). Позже такими операциями широко пользовался Гамильтон в своих ‘Лекциях о кватернионах’ (1853).

§ 7. Внешние операции на функциях

• **Значение отображения.** Пусть X и Y – два произвольных множества, а $Z = \mathrm{Map}(X, Y)$ – множество отображений из X в Y. Тогда сопоставление отображению $f \in \mathrm{Map}(X, Y)$ и точке $x \in X$ значения $f(x) \in Y$ определяет алгебраическую операцию $\mathrm{Map}(X, Y) \times X \longrightarrow Y$. Заметим, что при таком подходе стирается различие между элементами множеств X и Z, т.е. элементы X можно рассматривать как функции на Z. Эта идея – рассмотрение значений аргумента как функций на множестве функций от этого аргумента – является одной из ключевых идей математики XX века.

• **Композиция отображений.** Пусть X, Y, Z – три множества. Тогда определена операция $\mathrm{Map}(Y, Z) \times \mathrm{Map}(X, Y) \longrightarrow \mathrm{Map}(X, Z)$, $(f, g) \mapsto f \circ g$, сопоставляющее паре отображений их композицию.

• **Прямое произведение отображений.** Пусть X, Y, U, V – четыре множества. Определим прямое произведение отображений

$$U^X \times V^Y \longrightarrow (U \times V)^{X \times Y}, \quad (f, g) \mapsto f \times g$$

как $(f \times g)(x, y) = (f(x), g(y))$.

• **Тензорное произведение функций.** Следующая операция является ключевой в теории многомерного интегрирования. Пусть R – кольцо (например, $R = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ или $\mathbb{C}$), а X и Y – два множества. Определим тензорное произведение функций

$$R^X \times R^Y \longrightarrow R^{X \times Y}, \quad (f, g) \mapsto (f \otimes g),$$

следующим образом: $(f \otimes g)(x, y) = f(x)g(y)$. Это определение соответствует точке зрения, что множества являются частным случаем векторных пространств.

Задача. Проверьте, что тензорное произведение функций линейно по каждому аргументу, т.е.

$$(f_1 + f_2) \otimes g = f_1 \otimes g + f_2 \otimes g,$$

$$f \otimes (g_1 + g_2) = f \otimes g_1 + f \otimes g_2,$$

$$\lambda f \otimes g = \lambda(f \otimes g) = f \otimes \lambda g.$$

Комментарий. Начиная с 60-х годов многие алгебраисты рассматривают именно **тензорное** произведение функций как **основную** операцию над функциями, а операция умножения функций при этом трактуется как **производная**, а именно, как композиция диагонального вложения и тензорного произведения:

$$X \longrightarrow X \times X \longrightarrow R, \quad x \mapsto (x, x) \mapsto f(x)g(x).$$

Эта точка зрения доминирует в алгебраической геометрии, теории алгебраических групп и теории алгебр Хопфа и получает все большее распространение в других разделах алгебры. Впрочем, на само тензорное произведение можно смотреть как на производную операцию, а именно, как на композицию прямого произведения с умножением в основном кольце

$$X \times Y \longrightarrow R \times R \longrightarrow R, \quad (x, y) \mapsto (f(x), g(y)) \mapsto f(x)g(y).$$

Таким образом, в конечном счете произведение функций оказывается композицией *трех* отображений:

$$\begin{array}{ccccccc} X & \longrightarrow & X \times X & \longrightarrow & R \times R & \longrightarrow & R, \\ x & \longmapsto & (x, x) & \longmapsto & (f(x), g(x)) & \longmapsto & f(x)g(x). \end{array}$$

Предостережение. Если F – некоторое семейство функций $X \longrightarrow R$, а G – некоторое семейство функций $Y \longrightarrow R$, то $F \otimes G$ обычно понимается не по Минковскому, а как

$$F \otimes G = \{f_1 \otimes g_1 + \ldots + f_n \otimes g_n \mid n \in \mathbb{N}_0, f_i \in F, g_i \in G\}.$$

Иными словами, $F \otimes G$ это не множество **разложимых тензоров** вида $f \otimes g$, $f \in F$, $g \in G$, а множество их конечных сумм!

§ 8. Внешние операции на матрицах

• **Умножение прямоугольных матриц.** Пусть K – поле, а m, n, p – три натуральных числа. Тогда определена операция

$$\times : M(m,n,K) \times M(n,p,K) \longrightarrow M(m,p,K),$$

сопоставляющая паре матриц $x \in M(m,n,K)$, $y \in M(n,p,K)$ их **произведение**, т.е. такую матрицу $xy \in M(m,p,K)$, коэффициент которой в позиции (i,j) равен $(xy)_{ij} = x_{i1}y_{1j} + \ldots + x_{in}y_{nj}$.

• **Прямая сумма матриц.** Пусть l, m, n, p – четыре натуральных числа, тогда определена операция

$$\oplus : M(l,m,K) \times M(n,p,K) \longrightarrow M(l+n, m+p, K),$$

сопоставляющая паре матриц $x \in M(l,m,K)$, $y \in M(n,p,K)$ их **прямую сумму** $x \oplus y$, которую проще всего представлять себе как блочную матрицу вида

$$x \oplus y = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \in M(l+m, n+p, K).$$

• **Тензорное произведение матриц.** Пусть l, m, n, p – четыре натуральных числа, тогда определена операция

$$\otimes : M(l,m,K) \times M(n,p,K) \longrightarrow M(lm, np, K),$$

сопоставляющая паре матриц $x \in M(l,m,K)$, $y \in M(n,p,K)$ их **тензорное произведение** $x \otimes y$, которую проще всего представлять себе как блочную матрицу вида

$$x \otimes y = \begin{pmatrix} x_{11}y & \ldots & x_{1m}y \\ & \ldots & \\ x_{l1}y & \ldots & x_{lm}y \end{pmatrix} \in M(lm, np, K).$$

В `Mathematica` тензорное произведение матриц x и y вычисляется встроенной функцией `Outer[Times,x,y]`.

• **Кронекерова сумма матриц.** Пусть m, n – два натуральных числа, тогда определена операция

$$\boxplus : M(m,K) \times M(n,K) \longrightarrow M(mn,K),$$

сопоставляющая паре матриц $x \in M(m,K)$, $y \in M(n,K)$ их **кронекерову сумму** (alias **симметрическую сумму**) $x \boxplus y = x \otimes e_n + e_m \otimes y$, где через e_l обозначена единичная матрица степени l.

Операции прямой суммы и тензорного произведения чаще всего используются для *квадратных* матриц. В этом случае они строят по паре матриц $x \in M(m,K)$, $y \in M(n,K)$ матрицы $x \oplus y \in M(m+n,K)$ и $x \otimes y \in M(mn,K)$. Приведем для примера явные формулы, описывающие результат применения этих операций к квадратным матрицам степени 2:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \oplus \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & e & f \\ 0 & 0 & g & h \end{pmatrix},$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae & af & be & bf \\ ag & ah & bg & bh \\ ce & cf & de & df \\ cg & ch & dg & dh \end{pmatrix}.$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \boxplus \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & f & b & 0 \\ g & a+h & 0 & b \\ c & 0 & d+e & f \\ 0 & c & g & d+h \end{pmatrix}.$$

§ 9. Операторы

3. Операторы. Наиболее часто встречающийся случай внешних операций – это так называемые операторы. А именно, говорят, что элементы множества X действуют на Y в качестве **операторов**, если задана алгебраическая операция $X \times Y \longrightarrow Y$. Именно этот случай будет нам встречаться чаще всего.

• **Степень.**

• **Сверхстепень.** Пусть $x \in \mathbb{R}_{>0}$, а $n \in \mathbb{N}$. Определим n-ю сверхстепень (hyperpower) ${}^n x$ числа x как $x^{x^{\cdots^x}}$, где количество x равно n. Программисты часто обозначают эту операцию как $x \uparrow\uparrow n$. Сверхстепень изучали Эйлер, Эйзенштейн и Даниил Хармс. Положим ${}^\infty x = \lim\limits_{n\to\infty} ({}^n x)$. Априори совершенно непонятно, почему ${}^\infty x$ должно существовать хоть для одного $x \neq 0, 1$, однако Эйлер показал, что в действительности этот предел существует[277] для всех $x \in [(\frac{1}{e})^e, e^{1/e}]$,

• **Умножение вектора на скаляр.** Пусть V – множество векторов на обычной эвклидовой плоскости (или в трехмерном пространстве). Тогда определена операция $\mathbb{R} \times V \longrightarrow V$, $(\lambda, v) \mapsto \lambda v$, умножения вектора на скаляр. Таким образом, скаляры можно рассматривать как операторы на множестве точек.

• **Умножение вектора на матрицу.** Специализируя пример 5) для случая, когда $m = n$, а $p = 1$ мы получаем операцию $M(n, R) \times R^n \longrightarrow R^n$, которая превращает $M(n, R)$ в множество операторов на R^n.

• **Сложение векторов и точек.** Пусть X - множество точек эвклидовой плоскости (или трехмерного пространства), а V – соответствующее множество векторов. Тогда определена операция $V \times X \longrightarrow X$, сопоставляющая точке $x \in X$ и вектору $v \in V$ точку $x + v \in X$. Таким образом, векторы можно рассматривать как операторы на множестве точек.

• **Перестановки.** Вообще, пусть X - какое-то множество, а $S(X)$ – симметрическая группа множества X, состоящая из всех биективных преобразований X на себя. Применяя к этой специальной ситуации пример 1), о котором шла речь выше, получим действие $S(X) \times X \longrightarrow X$ группы $S(X)$ как операторов на X.

• **Сумма рационального и иррационального числа.** Пусть $\mathbb{Q}$ – множество рациональных чисел, а $\mathbb{I}$ – множество иррациональных чисел. Тогда сумма чисел определяет отображение $\mathbb{Q} \times \mathbb{I} \longrightarrow \mathbb{I}$, которое превращает $\mathbb{Q}$ в операторы на $\mathbb{I}$.

[277] R.A.Knoebel, Exponentials reiterated. – Amer. Math. Monthly, v.?, 1981, N.4, p.235–252.

§ 10. Формы

В действительности, нам будет встречаться, хотя и несколько реже, еще один тип бинарных операций, а именно, отображения вида $X \times X \longrightarrow Y$. Такие операции обычно называются **формами**. Не пытаясь обсуждать такие операции более подробно, отметим несколько примеров форм, к которым мы вернемся в разделе, посвященном линейной алгебре.

• **Скалярное произведение.** Пусть V - множество векторов на обычной эвклидовой плоскости (или в трехмерном пространстве). Тогда определена операция $V \times V \longrightarrow \mathbb{R}$, сопоставляющая паре векторов $u, v \in V$ их скалярное произведение.

• **Разность точек.** Пусть, как в примере 5) выше, X – множество точек эвклидовой плоскости (или трехмерного пространства), а V – соответствующее множество векторов. Тогда определена операция $X \times X \longrightarrow V$, сопоставляющее точкам $x, y \in X$ вектор $y - x$ с началом x и концом y.

Можно рассматривать формы большей арности.

• **Смешанное произведение.** Пусть $V = K^3$ - множество векторов в трехмерном пространстве над полем K. Тогда определена операция $V \times V \times V \longrightarrow K$, сопоставляющая паре векторов $u, v, w \in V$ их **смешанное произведение** $(u, [v, w])$. В случае $K = \mathbb{R}$ эта форма выражает ориентированный объем параллелепипеда, натянутого на u, v, w.

• **Определитель как форма от столбцов.** Смешанное произведение является частным случаем определителя. А именно, можно рассмотреть форму $\det : V \times V \longrightarrow K$, сопоставляющая набору столбцов $u_1, \ldots, u_n \in V = K^n$, определитель составленной из них матрицы $\det(u_1, \ldots, u_n)$. Смешанное произведение получается здесь при $n = 3$.

Самым известным примером тернарной формы является генетический код (см., например, книгу Гоппа[278])

§ 11. Бесконечноместные операции

Типичной отличительной чертой дисциплин аналитического цикла является рассмотрение операций **бесконечной арности**, обычно называемых **бесконечноместными**, и таких операций конечной арности, которые определяются в терминах бесконечноместных операций. Разумеется, такие операции обычно не бывают всюду определенными. В действительности можно даже утверждать, что, за исключением тривиальных случаев (типа постоянных операций), бесконечноместная операция, обладающая естественными свойствами, **никогда** не бывает всюду определенной. Так, легко видеть, что произведение бесконечного числа элементов в группе существует в том и только том случае, когда эта группа **тривиальна**, т.е. состоит из одного элемента. Это значит, что определить *ассоциативную* сумму бесконечного числа вещественных чисел можно ровно в одном случае, а именно, когда все числа равны 0. Таким образом, при определении бесконечноместных операций нужно отказаться

⋆ либо от того, чтобы они были всюду определенными,

⋆ либо от того, чтобы они обладали обычными свойствами,

⋆ либо и от того и от другого сразу,

⋆ либо, наконец, как это обычно делается в алгебре, от того, чтобы операция была *внутренней*, т.е. от того, чтобы результат был числом в *обычном* понимании.

Напомним, что результат применения алгебраической операции $*$ к конечному числу элементов обычно определяется по индукции как $x*y*z = (x*y)*z$, $x*y*z*w = ((x*y)*z)*w$ и

[278]В.П.Гоппа, Введение в алгебраическую теорию информации, М., 1995.

т.д. Если исходная операция ассоциативна, то, как будет показано в следующем параграфе, для любого конечного числа операндов результат не зависит от расстановки скобок. Чтобы пояснить читателю, в чем состоит проблема определения бесконечных композиций, приведем следующее известное 'доказательство' того, что $0 = 1$:

$$0 = (1-1) + (1-1) + \ldots = 1 - (1-1) - (1-1) + \ldots = 1$$

(напомним, что сложение вещественных чисел ассоциативно!) Самое замечательное, что это доказательство, хотя и *не совсем* верное для чисел, имеет **глубокий математический смысл** и широко применяется в алгебре и топологии (**трюк Эйленберга** в линейной алгебре и **трюк Мазура** в теории векторных расслоений). В то же время вслед за Лейбницем, Абелем и Чезаро[279] некоторые алгебраисты *верят*, а большинство аналитиков *знают*, что для вещественных чисел

$$1 - 1 + 1 - 1 + \ldots = \frac{1}{2}.$$

В связи с тем, что бесконечноместные операции не могут быть всюду определенными, основной вопрос анализа как раз и состоит в нахождении условий, когда же именно имеет смысл применять ту или иную операцию, – т.е. акцент переносится с тождеств на **вопросы сходимости**. Типичной бесконечноместной операцией является операция взятия предела lim. В терминах этой операции определяются бесконечные суммы, произведения etc., а также такие унарные операции, как дифференцирование и интегрирование функций, etc.

Громадные усилия многих поколений математиков на протяжении многих веков были посвящены вопросу о том, в каком именно смысле можно определить результат бесконечноместной операции. До XVIII века главенствовала греческая точка зрения 'исчерпывания', которая и до сих пор является преобладающей в стандартных учебниках (стандартного) математического анализа. Она состоит в том, что $x_1 * x_2 * \ldots * x_n * \ldots$ считается определенным, если результат применения $*$ к бесконечному хвосту $x_n * x_{n+1} * \ldots$ может быть сделан сколь угодно близок к нейтральному элементу относительно $*$ при росте n. Впрочем, как показывает внимание, уделяемое философами, вплоть до новейшего времени, так называемым 'апориям Зенона', даже понимание банальностей, подобных равенству

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots = 1,$$

сопряжено с некоторыми психологическими трудностями.

В XVIII – XX веках появились гораздо более интересные воззрения на то, как следует определять результат бесконечноместной операции. Например, для сумм и произведений вещественных чисел различные (небанальные и, вообще говоря, не совпадающие между собой!) ответы на этот вопрос дают, среди прочего, бесконечная комбинаторика, p-адический анализ, теория функций комплексного переменного и нестандартный анализ. Так, например, с комплексно аналитической точки зрения имеет место равенство

$$1 + 2 + 3 + \ldots = -\frac{1}{12}$$

(формула Эйлера для $\zeta(-1)$), в то время как с точки зрения исчерпывания значение суммы $1 + 2 + 3 + \ldots$ в левой части не определено и большинство традиционных учебников 'математического анализа' назовут этот ряд 'расходящимся'. Разумеется, манипуляции с бесконечными суммами такого вида требуют навыка и внимания, так как они не удовлетворяют обычным тождествам алгебры. Гуру такого рода манипуляций в XVIII веке был Эйлер, а в XX веке – Рамануджан. Самое замечательное, что при их выполнении они никогда (или почти никогда!) не ошибались. С точки зрения p-адического анализа сходящимся является ряд $1 + p + p^2 + p^3 + \ldots$, где p – простое число, например, ряд $1 + 2 + 4 + 8 + \ldots$ сходится 2-адически.

[279] Ж.-П.Рамис, Расходящиеся ряды и асимптотическая теория. – Ижевск, Ин-т Компьютерных Иссл., 2002, с.1–79.

§ 12. Частичные операции

Как уже упоминалось выше, в математике часто естественно возникают не всюду определенные операции.

Определение. Частичной внутренней n-арной операцией *на непустом множестве X называется отображение $f : Y \longrightarrow X$, где $Y \subseteq X \times \ldots \times X$.*

Обычно для обозначения частичных отображений используется пунктирная стрелка, таким образом, чтобы указать n-арную частичную операцию на X мы пишем $X \times \ldots \times X \dashrightarrow X$. Приведем несколько примеров частичных внутренних бинарных операций.

?) Вычитание и деление. Вычитание и деление являются частичной операцией на множестве $\mathbb{N}$ натуральных чисел. Деление является частичной операцией в $\mathbb{Z}$. Оно продолжает оставаться частичной операцией в любом поле: деление на 0 невозможно.

?) Возведение в степень.

Все данные выше определения, относящиеся к случаю всюду определенных операций, нуждаются в уточнении, учитывающем тот факт, что теперь наша операция не всюду определена. Например, частичная внутренняя операция $*$ на множестве X называется **ассоциативной**, если для любых трех элементов $x, y, z \in X$ из того, что одно из произведений $(xy)z$ и $x(yz)$ определено, следует, что определено и второе и они равны между собой.

?) Композиция путей. Пусть снова, как в примере 20 выше, X – топологическое пространство, $x_0, x_1 \in X$. **Путем** в пространстве X с началом x_0 и концом x_1 называется непрерывное отображение $f : [0,1] \longrightarrow X$ такое, что $f(0) = x_0$ и $f(1) = x_1$. Будем писать $x_0 = S(f)$ и $x_1 = T(f)$ (от английского 'source' и 'target' или 'terminus', соответственно). Если f и g – две пути такие, что $T(f) = S(g)$, то их **композицией** называется отображение $f * g : [0,1] \longrightarrow X$ заданное посредством $(f * g)(t) = f(2t)$, если $t \in [0, 1/2]$ и $(f * g)(t) = g(2\mathrm{e} - 1)$, если $t \in [1/2, 1]$. Легко видеть, что $f * g$ снова путь в пространстве X такой, что $S(f * g) = S(f)$ и $T(f * g) = T(g)$. На самом деле эта композиция не является ассоциативной и в топологии обычно рассматривают не саму композицию путей, а индуцированную композицию на гомотопических классах путей, которая ассоциативна.

?) Умножение матриц. Пусть X - множество всех матриц конечного размера с коэффициентами из некоторого кольца (например, с целыми, вещественными или комплексными коэффициентами). Тогда умножение матриц есть *частичная* операция на этом множестве. В самом деле, пусть $R(x)$ есть число строк матрицы x, а $C(x)$ – число ее столбцов. Тогда произведение xy матриц x и y определено в том и только том случае, когда $C(x) = R(y)$. Мы будем подробно обсуждать умножение матриц в Главе ?. Как выяснится при этом, умножение матриц ассоциативно.

?) Композиция связок.

?) Композиция морфизмов в категории. Все три приведенных выше примера являются частными случаями следующей общей конструкции. Пусть C – категория, объекты которой образуют множество. Рассмотрим множество $\mathrm{Mor}(C)$ *всех* морфизмов этой категории, т.е. объединение всех множеств $\mathrm{Hom}(a, b)$, где $a, b \in \mathrm{Ob}(C)$.

Иногда возникают частичные внешние операции.

• **Операции, определенные инцидентностью.** Пусть X и Y – множества точек и прямых эвклидовой плоскости, соответственно. Зададим *частичное* отображение $X \times X$ в Y следующим образом. Пусть x и y – две *различные* точки. Сопоставим им проходящую через них прямую. Совершенно аналогично определяется и частичное отображение $Y \times Y$ в X. Пусть l и m – две непараллельные прямые. Сопоставим им их точку пересечения. Существенным здесь является то, что эти отображения определены *почти всюду*, т.е. для пар элементов, находящихся 'в общем положении'. Ясно, что этот пример легко обобщается на пространства большего числа измерений. Например, три точки в общем положении в трехмерном пространстве определяют плоскость, а три плоскости в общем положении точку, чем определяются частичные *тернарные* операции. Аналогично, прямая и плоскость в общем положении определяют точку, а прямая и точка в общем положении – плоскость, что задает частичные внешние бинарные операции.

• **Склейка отображений.** Пусть X, Y, Z – три множества. Определим **склейку** $f \uplus g$ отображений $f \in Z^X$, $g \in Z^Y$,

$$Z^X \times Z^Y \dashrightarrow Z^{X \cup Y}, \qquad (f, g) \mapsto f \uplus g,$$

как такое отображение $X \cup Y \longrightarrow Z$, значение которого в точке $x \in X \cup Y$ определяется как $(f \uplus g)(x) = f(x)$, если $x \in X$, и $(f \uplus g)(x) = g(x)$, если $x \in Y$. Ясно, что склейка отображений f и g в том и только том случае будет отображением, когда $f_{X \cup Y} = g_{X \cap Y}$.

Логика

> Small Girl: I'm **so** glad I don't like asparagus!
> Sympathetic Friend: Why, my dear?
> Small Girl: Because, if I did, I should have to eat it – and I ca'n't bear it!
>
> Lewis Carroll: The Small Girl and her Sympathetic Friend

Исчисление высказываний

Низшим уровнем логического анализа является **исчисление высказываний** (называемое также **пропозициональным исчислением**), которое позволяет сделать заключение об истинности или ложности составного предложения исходя из истинности или ложности входящих в его состав простых предложений.

Высказывания, элементарные высказывания. Высказыванием называется **повествовательное** предложение, которому можно приписать определенное значение истинности. Большинство математиков пользуется так называемой **классической логикой**, в которой имеется **два** значения истинности – любое высказывание может быть объявлено **истинным** либо **ложным**. Например,

(a) Сократ есть кот;

(b) Земля имеет форму додекаэдра;

(c) Несчастья Тристрама начались за девять месяцев до его рождения;

(d) Утверждение 'Неверно, что ефрейтор Пилипенко – творец всего живого на земле' не имеет места;

(e) Нет, не было и никогда не будет власти более гуманной и справедливой, чем власть императора Клавдия Тиберия;

(f) Динозавры не смогли или не захотели осуществить план полного уничтожения млекопитающих;

(g) Если Луна сделана в Гамбурге, то она сделана из зеленого сыра;

(h) Панург в том и только том случае женится, если он не останется холостым;

(j) Нет, как же, ты не сидел тут на месте А и я не стоял тут на месте Б;

(k) Книга важнее хлеба, книга важнее стен в доме;

суть высказывания, которые могут быть объявлены истинными или ложными, в зависимости от точки зрения и политических взглядов говорящего. С другой стороны, вопросительные и восклицательные предложения не являются высказываниями. Так, например, не выражают никаких высказываний следующие фразы:

(l) Дорогой, не забыл ли ты завести часы?

(m) В каком году Альфред Вегенер открыл, что земля имеет форму додекаэдра?

(n) Господа офицеры, левое плечо вперед!

(o) Да здравствует император Цинь Ши Хуан, лучший друг всех китайских ученых!

Некоторые логики различают высказывания и предложения. При этом они говорят, что высказывание есть **смысл** предложения, т.е. то, что оно означает. В качестве примеров этого различия обычно приводятся следующие. Рассмотрим фразу (a) и следующую английскую фразу:

(p) Socrates is a cat.

Эти две фразы представляют собой, по мысли этих авторов, два **предложения**, выражающие одно и то же **высказывание**. Мне так не кажется. Во-первых, в английской фразе нет никакого намека на пол Сократа, ее предикат 'to be a cat' мог бы быть переведен на русский язык фразой 'быть котом или кошкой'. Во-вторых, что гораздо важнее, наша способность заявить, что смысл фраз (a) и (j) совпадает, зависит от нашей способности понимать русский и английский языки. Будет ли столь же очевидно что (a) и

(q) Сокулатесу — по-японски

выражают 'одно и то же' высказывание? Другой пример, который часто приводится в этом контексте, это предложения '$1 > 2$' и '$2 < 1$', якобы выражающие 'одно и то же' высказывание. Опять же, с моей точки зрения, это заблуждение, основанное на том, что мы понимаем смысл знаков '$>$' и '$<$' (в действительности, эти фразы **становятся** равнозначными после того, как отношение '$<$' **определяется** таким образом, что $x < y$ выполняется тогда и только тогда, когда $y > x$). Если бы мы писали 'xGy' вместо '$x < y$' и 'xDy' вместо '$x > y$', то равнозначность предложений '$1D2$' и '$2G1$' уже не была бы столь очевидна (по крайней мере для читателя, не владеющего французским языком).

Поэтому мы будем понимать под высказыванием, как сказано выше, само повествовательное предложение, **как оно есть** ('as is'), в полном отвлечении от его семантики, но, как будет описано в следующем пункте, частично учитывая его внутреннюю структуру. Мы считаем, что **любое** изменение формы высказывания меняет его смысл: "forma mutata, mutatur substantia".

Некоторые высказывания не имеют **никакой** дальнейшей внутренней структуры, с точки зрения исчисления высказываний. Таковы, например, высказывания (a)–(c) выше. Такого рода высказывания будут называться **элементарными** или **атомарными** и про них на уровне исчисления высказываний нельзя сказать ничего, кроме того, что им произвольным образом может быть приписано одно из двух значений истинности.

§ ?. Пропозициональные связки, составные высказывания

1. Пропозициональные связки. Все остальные высказывания строятся из элементарных высказываний при помощи союзов, называемых в математической логике **пропозициональными связками**. Высказывания, построенные из других высказываний при помощи пропозициональных связок, называются **составными**, например, высказывания (d)–(f) выше – составные. В классической логике традиционно рассматривается пять пропозициональных связок $\neg$, $\&$, $\vee$, $\Longrightarrow$, $\Longleftrightarrow$ (в действительности, все они могут быть выражены через подходящие две из них, остальные вводятся лишь для сокращения формул), называемых соответственно, негацией, конъюнкцией, дизъюнкцией, импликацией и эквиваленцией. (или, сокращенно, на латыни 'non', 'et', 'vel', 'seq' и 'aeq')). Опишем последовательно смысл этих связок. Связка $\neg$ является **унарной**, т.е. она строит новое высказывание по **одному** исходному высказы-

ванию, все же остальные связки – **бинарные**, т.е. требуют **двух** высказываний для образования нового составного высказывания.

2. Негация $\neg$, называемая также **отрицанием**, соответствует функции NOT информатики. Пусть p есть некоторое высказывание. Тогда $\neg p$ есть **отрицание** высказывания p. В живом языке негация передается частицей 'не' ('не p'), оборотами типа 'неверно, что p', 'p не имеет места' или более сложными конструкциями. Например, высказывание (d) имеет вид $\neg p$ для подходящего высказывания p (для какого?). Отрицанием высказывания (a) является высказывание 'Неверно, что Сократ есть кот' или, чаще, 'Сократ не есть кот' (перевод формул обратно в разговорный язык обычно не является однозначным!). Многие языки (русский, французский, итальянский и т.д.) дублируют отрицание, т.е. использую конструкцию $\neg\neg p$ для отрицания высказывания p, сравни "je ne le sais pas", где присутствуют **две** отрицательные частицы 'ne' и 'pas'. С логической точки зрения это довольно удивительно, так как (в классической логике) второе отрицание совпадает с исходным утверждением, т.е. 'не не p' имеет тот же смысл, что и 'p'. В действительности в русском языке теоретически могут строиться сколь угодно длинные цепочки отрицаний, а фразы, содержащие пять-шесть отрицаний, типа "Я нигде никогда никому ничего не говорил" (см. Колпакчи "Дружеские встречи с английским языком") звучат абсолютно естественно. Английский язык гораздо более логичен в этом отношении. В нем, чтобы опровергнуть фразу "Я где-то когда-то кому-то что-то сказал" достаточно использовать одно отрицание "I never told anything anybody anywhere" или "I ever told anything nobody anywhere". Именно в силу этой особенности русского языка в математической речи предпочтительно использовать либо глагольное отрицание (частицу 'не', еще лучше со вспомогательным глаголом 'не есть', 'не является'), либо отрицать все предложение в целом ('неверно, что ...'), избегая конструкций с кратным отрицанием.

3. Конъюнкция $\&$ соответствует функции AND информатики. Пусть p и q суть два высказывания. Тогда высказывание $p \ \& \ q$ означает, что выполняются **оба** высказывания p и q. В обычном языке конъюнкция чаще всего передается запятой ('p, q') или союзом 'и' ('p и q'), но может выражаться и другими, эмфатическими средствами 'и p и q', 'p одновременно с q', 'как p, так и q', 'не только p, но и q', 'не только q, но и p', 'p, несмотря на q', 'q, несмотря на p' и т.д. Например, высказывание (e) представляет собой конъюнкцию **шести** элементарных высказываний, истинность каждого из которых может рассматриваться по отдельности: 'нет власти более гуманной, чем власть императора Клавдия Тиберия', 'не было власти более гуманной, чем власть императора Клавдия Тиберия', 'никогда не будет власти более гуманной, чем власть императора Клавдия Тиберия' и три аналогичных высказывания с заменой 'гуманности' на 'справедливость'. В отдельных случаях конъюнкция в разговорном языке может передаваться даже союзом 'или', но мы никогда не будем использовать 'или' в этом значении.

4. Дизъюнкция $\vee$ соответствует функции OR информатики. Напомним, что это **неразделительное** (alias **неисключительное**, или, как говорят логики, 'неэксклюзивное') 'или'. Таким образом, по двум высказываниям p и q строится высказывание $p \vee q$ означающее, что выполняется **по крайней мере одно** из высказываний p и q – **или оба**. В обычном языке дизъюнкция чаще всего передается союзом 'или' ('p или q'), но может выражаться и другими,

эмфатическими средствами ‘p или q или оба’, ‘p и/или q’ (эта форма пришла в русский язык сравнительно недавно под влиянием английского юридического и делового ‘and/or’), ‘хотя бы одно из p или q’, ‘p, если не q’, ‘q, если не p’ и т.д. Кстати, генетически символ $\vee$ представляет собой просто первую букву латинского союза ‘vel’ – ‘или’, а символ для конъюнкции $\&$ – перевернутый символ $\vee$. Например, высказывание (f) представляет собой дизъюнкцию двух высказываний: ‘динозавры не смогли существить план полного уничтожения млекопитающих’ и ‘динозавры не захотели осуществить план полного уничтожения млекопитающих’.

5. Эксклюзивная дизъюнкция. В этой связи заметим, что имеется еще одна пропозициональная связка, не имеющая, впрочем, общепринятого названия и обозначения, которая отвечает функции XOR информатики, т.е. **разделительному** (alias **исключительному** или, как говорят логики, **эксклюзивному**) ‘или’. Эта связка, которую мы будем обозначать через $\triangle$, строит по двум высказываниям p и q новое высказывание $p \triangle q$, состоящее в том, что выполняется **ровно одно** из высказываний p либо q, **но не оба**. В обычном языке разделительная дизъюнкция чаще всего выражается конструкциями ‘или p, или q’, ‘либо p, либо q’, или же, если нужна особая точность, то конструкциями ‘p либо q, но не оба’, ‘ровно одно из p или q.

6. Выражение дизъюнкции в разговорном и научном языке. Различие между разделительным и неразделительным значениями ‘или’ четко прослеживается в латыни, где в разделительном смысле используется исключительно союз ‘aut’, как в следующем выражении: “aut Caesar, aut nihil” (“либо пан, либо пропал”). Выбор из **двух взаимоисключающих** возможностей, как в этом случае, называется **альтернативой** или, иногда, **дихотомией**. Современные языки не всегда столь однозначны. Клини [Kl] приводит следующий пример. Увидев в туристском меню ресторана фразу “чай или кофе бесплатно”, мы должны быть готовы заплатить, заказав одновременно и то и другое. Во фразе Кьеркегора “или – или” (по-датски “enten – eller”, по-английски “either – or”, по-немецки “entweder – oder”) имеется в виду именно альтернатива. С другой стороны, произнося фразу “x либо дурак, либо мерзавец”, говорящий не имеет, как правило, намерения исключать возможность того, что x попадает в обе эти категории одновременно. Чтобы запутать положение еще больше, в разговорном языке дизъюнкция часто передается союзом ‘и’. Так, фразу “книги бывают хорошие и плохие” не следует, видимо, понимать как конъюнкцию двух утверждений “существуют хорошие книги” и “существуют плохие книги”. Скорее всего, говорящий имел в виду следующее утверждение “любая книга является либо хорошей, либо плохой”.

Ясно, что такое смешение совершенно недопустимо там где нужна точность, в частности, в научном языке. Поэтому в дальнейшем мы будем использовать ‘и’ только для обозначения конъюнкции, ‘или’ только для обозначения неразделительной дизъюнкции (т.е. как перевод латинского ‘vel’), а ‘либо’ только для обозначения разделительной дизъюнкции (т.е. как перевод латинского ‘aut’). Таким образом, фраза “каждое ненулевое целое число является положительным и отрицательным” неверна (при обычном понимании входящих в нее слов!), а фразы “каждое ненулевое целое число является положительным или отрицательным” и “каждое ненулевое целое число является либо положительным, либо отрицательным” обе верны, но вторая точнее, так как она исключает воз-

можность того, что какое-то число одновременно является и положительным и отрицательным.

7. Импликация $\Longrightarrow$ строит по двум высказываниям p и q новое высказывание $p \Longrightarrow q$, означающее, что 'p влечет q' (или, как говорят логики, 'p имплицирует q'). На обычном языке $p \Longrightarrow q$ обычно выражается фразами типа 'если p, то q', 'p, только если q', 'в случае p, имеет место q', 'p достаточно для q', 'для p необходимо q', 'p сильнее, чем q'. Часто удобно рассматривать обратную импликацию $\Longleftarrow$. По определению $p \Longleftarrow q$ означает 'p следует из q', alias 'p вытекает из q', 'p, если q', 'p является следствием q', 'для p достаточно q', 'p необходимо для q', 'p каждый раз как q', 'p в предположении q', 'p слабее, чем q'.

8. Эквиваленция $\Longleftrightarrow$ строит по двум высказываниям p и q новое высказывание $p \Longleftrightarrow q$, являющееся сокращением для конъюнкции двух импликаций $p \Longrightarrow q$ и $p \Longleftarrow q$. Таким образом, высказывание $p \Longleftrightarrow q$ означает, что 'p равносильно q', alias 'p эквивалентно q'. В обычном языке высказывание $p \Longleftrightarrow q$ передается конструкциями 'p, если и только если q', 'p тогда и только тогда, когда q', 'p в случае q и только в этом случае', 'из p вытекает q и обратно', 'из p следует q и обратно', 'если p, то q и обратно', 'p каждый раз как q и обратно', 'для p необходимо и достаточно q', 'p необходимо и достаточно для q'. В математическом языке высказывания вида $p \Longleftrightarrow q$ встречаются настолько часто, что остро ощущается отсутствие в обычном языке простого союза со значением $\Longleftrightarrow$. Чтобы исправить положение некоторые англоязычные математики используют выдуманный союз 'iff' в качестве сокращения для 'if and only if'. Были предложения переводить это на русский союзом 'ттогда' (='тогда и только тогда').

9. Составные высказывания. Теперь мы в состоянии дать точный рецепт построения всех высказываний исходя из элементарных высказываний.

1) Элементарные высказывания являются высказываниями.

2) Если p и q – высказывания, то $\neg p$, $p \ \& \ q$, $p \vee q$, $p \Longrightarrow q$, $p \Longleftrightarrow q$ также являются высказываниями.

Высказывание, содержащее хотя бы одну пропозициональную связку, называется **составным**.

10. Иерархия пропозициональных связок. Для обозначения порядка применения пропозициональных связок обычно используются круглые скобки. Например, $p \ \& \ (q \vee r)$ и $(p \ \& \ q) \vee r$ суть два разных высказывания – первое из них является конъюнкцией высказывания p и дизъюнкции q с r, а второе – дизъюнкцией конъюнкции p и q с высказыванием r. Кстати, на этом примере можно оценить, насколько формула проще и точнее ее словесного описания. Чтобы уменьшить количество скобок, на пропозициональных связках вводят следующую иерархию $\Longleftrightarrow$, $\Longrightarrow$, $\vee$ и $\&$, $\neg$, в которой каждая следующая связка является более сильной, чем предыдущая, т.е. связывает сильнее и должна применяться в первую очередь. Это значит, например, что $p \Longrightarrow q \ \& \ r$ нужно понимать как $p \Longrightarrow (q \ \& \ r)$, а не как $(p \Longrightarrow q) \ \& \ r$. Аналогично, $\neg p \vee q$ означает $(\neg p) \vee q$, а вовсе не $\neg(p \vee q)$. Подобное соглашение хорошо знакомо нам из школьной арифметики, где также вводится иерархия арфиметических операций и $a + b \cdot c$ понимается как $a + (b \cdot c)$, а не как $(a + b) \cdot c$.

В приведенной выше иерархии связок мы не случайно написали '$\vee$ и $\&$ '. Мы считаем $\vee$ и $\&$ связками **одинакового** ранга и **всегда** ставим скобки в

тех случаях, когда порядок их применения может вызывать сомнение. Дело в том, что хотя многие логики считают, что $\vee$ связывает сильнее, чем $\&$ (т.е. располагают связки в порядке $\Longleftrightarrow$, $\Longrightarrow$, $\&$, $\vee$, $\neg$) для меня нет никаких убедительных аргументов в пользу такого соглашения. Наоборот, психологически $\&$ является аналогом умножения, а $\vee$ – сложения и, поэтому, казалось бы, $\&$ должно связывать сильнее, чем $\vee$. В самом деле, в АЛГОЛе и многих других языках программирования связки располагаются в порядке $\Longleftrightarrow$, $\Longrightarrow$, $\vee$, $\&$, $\neg$.

§ ?. Оценки истинности, булевы функции

Двоякий, поистине, мир этот: истина и ложь составляют его; и нет третьего.

Шатапатха-Брахмана

1. Значения истинности. Высказываниям можно приписывать различные **значения истинности**. В классической логике имеется только два значения истинности, а именно **ложь** и **истина**. **Оценкой истинности** называется сопоставление каждому высказыванию некоторого значения истинности, согласованное с пропозициональными связками, в смысле, который намереваемся уточнить. Иными словами, оценка истинности – это функция v, определенная на высказываниях и принимающая значения 0 ('ложь') и 1 ('истина'). Высказывание p, для которого $v(p) = 0$ называется **ложным** (относительно данной оценки v), а высказывание p, для которого $v(p) = 1$ называется **истинным**.

Часто значения истинности обозначаются иначе. Например, в англоязычной и ориентирующейся на нее литературе принято обозначение 'F' для 'лжи' от английского 'false' и 'T' для 'истины' от английского 'true', (впрочем, я слышал от немецких математиков версию, что F и T являются первыми буквами слов 'Falsch' и 'Trivial': 'Das ist Falsch oder Trivial'). В литературе на романских языках для истинностных значений обычно используются буквы 'F' и 'V' (от французского 'faux' и 'vrai' или итальянского 'falso' и 'vero'). Впрочем, для последующего абсолютно неважно, как именно обозначаются (и как называются) истинностные значения, важно лишь, что их только два и что сопоставление высказываниям их истинностных значений перестановочно с пропозициональными связками. Можно, например, классифицировать высказывания на белые и черные, важно лишь так определить на значениях истинности 'белое' и 'черное' действие связок, чтобы выполнялись равенства 'белое и черное = белое', 'белое или черное = черное' и т.д.

2. Оценки истинности. Сформулируем теперь чуть точнее, в чем состоит условие на оценку истинности. 1) Сопоставление истинности элементарным высказываниям совершенно произвольно. (В действительности, конечно, это не совсем так, но причины, по которым те или иные элементарные высказывания провозглашаются истинными или ложными, лежат за пределами логики высказываний.) 2) Истинностное значение, сопоставляемое составным высказываниям $\neg p$, $p \ \& \ q$, $p \vee q$, $p \Longrightarrow q$, $p \Longleftrightarrow q$ зависит не от самих высказываний p и q, а только от их истинностных значений – это и имелось в виду выше, когда мы говорили о 'перестановочности' оценки со связками. Это значит, что коль скоро мы знаем $v(p)$ для всех **элементарных** высказываний, мы можем **вычислить** значение v на всех остальных высказываниях. В этом и состоит задача исчисления высказываний.

3. Булевы функции. Разумеется, чтобы говорить о том, что оценка истинности 'перестановочна' с пропозициональными связками, мы должны еще определить результат применения этих связок к значениям истинности. Пусть α – **булева переменная**, т.е. переменная, принимающая значения 0 и 1. Функция, аргументами которой являются булевы переменные и которая сама принимает значения 0 и 1 называется **булевой функцией** (или **булевой операцией**, но термин булева операция часто понимается в чуть другом смысле). Мы должны сопоставить каждой пропозициональной связке некоторую булеву функцию от одного или двух аргументов, так, чтобы ее определение соответствовало интуитивному смыслу этой связки. При этом мы сохраним для этих булевых функций те же названия и обозначения, что и для соответствующих пропозициональных связок. Совершенно ясно, как следует понимать **негацию** $\neg\alpha$, а именно, мы должны положить $\neg 0 = 1$ и $\neg 0 = 1$.

Точно так же, формальные определения остальных связок на парах булевых переменных α и β должны соответствовать их интуитивному смыслу, объясненному в предыдущем пункте. Так, например, конъюнкция двух высказываний должна быть истинным высказыванием в том и только том случае, когда оба высказывания истинны. Это значит, что мы определяем **конъюнкцию** булевых переменных $\alpha \ \& \ \beta$ следующим образом: $1 \ \& \ 1 = 1$ и $\alpha \ \& \ \beta = 0$ во всех остальных случаях (т.е. $0 \ \& \ 0 = 0$, $0 \ \& \ 1 = 0$, $1 \ \& \ 0 = 0$). Иными словами, $\&$ – это в точности то, что естественно понимать под **произведением** булевых переменных α и β.

Аналогично, дизъюнкция двух высказываний должна быть истинным высказыванием в том и только том случае, когда хотя бы одно из этих высказываний истинно. Это значит, что мы определяем **дизъюнкцию** булевых переменных $\alpha \vee \beta$ следующим образом: $0 \vee 0 = 0$ и $\alpha \vee \beta = 1$ во всех остальных случаях (т.е. $0 \vee 1 = 1$, $1 \vee 0 = 1$, $1 \vee 1 = 1$). Дизъюнкция не есть то, что понимается под суммой двух булевых переменных в информатике ('сумма по модулю 2'). Напомним, что сумма $\alpha + \beta$ двух булевых переменных определяется почти так же, как дизъюнкция, но $1 + 1 = 0$. Таким образом, сумма булевых переменных в точности соответствует **разделительной** дизъюнкции, а для собственно дизъюнкции имеет место формула $\alpha \vee \beta = \alpha + \beta + \alpha \ \& \ \beta$.

Как и другие бинарные булевы операции (т.е. булевы функции от двух аргументов), конъюнкция, дизъюнкция и разделительная дизъюнкция (сумма) нагляднее всего изображается при помощи своих **таблиц Кэли**. Строки таблицы Кэли соответствуют значениям переменной α, а столбцы – значениям переменной β, причем на пересечении строки с номером α со столбцом с номером β ставится значение функции f на паре аргументов α и β (в таком порядке). Изобразим таблицы Кэли этих операций:

$\&$	0	1
0	0	0
1	0	1

$\vee$	0	1
0	0	1
1	1	1

$+$	0	1
0	0	1
1	1	0

Перейдем теперь к построению булевых функций, отвечающих оставшимся связкам $\Longrightarrow$, $\Longleftarrow$ и $\Longleftrightarrow$. По смыслу импликации из истины должна следовать только истина, а из лжи – что угодно (как всегда, это относится лишь к классической логике, в логике конструктивистов из лжи следует не что угодно, а лишь второе отрицание чего угодно). Это значит, что $1 \Longrightarrow 0 = 0$ и $\alpha \Longrightarrow \beta = 1$

во всех остальных случаях (т.е. $0 \vee 0 = 1$, $0 \vee 1 = 1$, $1 \vee 1 = 1$).

$\Longrightarrow$	0	1
0	1	1
1	0	1

$\Longleftarrow$	0	1
0	1	0
1	1	1

$\Longleftrightarrow$	0	1
0	1	0
1	0	1

Впрочем, логики часто изображают булевы функции не посредством таблиц Кэли, а посредством **таблиц истинности**, которые становятся удобнее, если рассматриваются функции от трех или четырех аргументов (изображение таблиц истинности для функций большего числа аргументов становится совершенно непрактичным). В таблице истинности до вертикальной черты изображаются все возможные наборы значений аргументов (число таких наборов равно 2^n для n аргументов)

§ ?. Исчисление предикатов

Исчисление высказываний анализирует построение составных высказываний из элементарных высказываний. **Исчисление предикатов** идет на один шаг глубже в своем анализе. В нем, кроме того, рассматривается **субъектно-предикатная структура** элементарных высказываний.

Субъект и предикат. С точки зрения исчисления предикатов элементарное высказывание состоит из субъекта (или субъектов) и предиката. Как показывают названия, субъект и предикат связаны с подлежащим и сказуемым в грамматике, но в логике они обычно трактуются более широко. Неформально, **субъект** есть то, **о чем** говорится в предложении, а **предикат** есть то, **что** говорится в предложении.

В простейшем случае предложение имеет один субъект. Например, в рассмотренной выше фразе (а) субъектом является ‘Сократ’, а предикатом – свойство быть котом. Унарный предикат P можно рассматривать как **пропозициональную функцию**, которая сопоставляет каждому значению аргумента x некоторое высказывание $P(x)$, в нашем случае высказывание ‘x есть кот’. Если x рассматривается как переменная, то фраза ‘x есть кот’ не является высказыванием, она является

Однако в обычном языке (например, русском) как субъект, так и предикат могут передаваться различными членами предложения. Кроме того, предложение может иметь несколько субъектов. Например, с логической точки зрения прямое дополнение обычно является субъектом предложения – в пассивной конструкции оно становится подлежащим. Возьмем, например, предложение “Хосров любит Ширин”, хотя с точки зрения грамматики ‘Хосров’ и ‘Ширин’ входят сюда неравноправно (‘Хосров’ – подлежащее, а ‘Ширин’ – прямое дополнение), с точки зрения логики и ‘Хосров’ и ‘Ширин’ являются субъектами этого предложения, а ‘любить’ – предикатом. Это предложение может быть преобразовано в “Ширин любима Хосровом”, где ‘Ширин’ становится подлежащим, а ‘Хосров’ – дополнением. В отличие от рассмотренных ранее унарных предикатов предикат ‘любить’ является бинарным. Это значит, что он требует двух аргументов для образования высказывания.

§ ?. Кванторы

?. Свободные и связанные переменные.

?. Законы де Моргана для кванторов. Следующие два правила перестановки отрицания с кванторами, называемые **законами де Моргана** были открыты фон Лейбницем в конце XVII века.

$$\neg\forall x, P(x) \quad \Longleftrightarrow \quad \exists x, \neg P(x),$$

$$\neg\exists x, P(x) \quad \Longleftrightarrow \quad \forall x, \neg P(x).$$

Таким образом, чтобы опровергнуть, что $P(x)$ выполняется для всех x (необходимо и) достаточно доказать, что $P(x)$ не выполняется хотя бы для одного x. Аналогично, чтобы опровергнуть, что $P(x)$ выполняется хотя бы для одного x необходимо (и достаточно) доказать, что $P(x)$ не выполняется для всех x.

?. Эффективные и экзистенциальные доказательства. В классической логике законы де Моргана можно переписать еще в такой форме:

$$\forall x, P(x) \quad \Longleftrightarrow \quad \neg\exists x, \neg P(x),$$

$$\exists x, P(x) \quad \Longleftrightarrow \quad \neg\forall x, \neg P(x).$$

Таким образом, для того, чтобы доказать, что объект x со свойством P существует, достаточно доказать, что не любой объект обладает свойством $\neg P$. Однако некоторые логические школы (интуиционисты и конструктивисты) не считают, это доказательством существования. Они считают, что левая часть этого выражения означает, что "x существует", а правая – что "x не может не существовать", а с их точки зрения это совсем не одно и то же. Доказательство того, что $\exists x, P(x)$ путем предъявления x с нужным свойством они называют **эффективным** или **конструктивным**, а доказательство того, что $\neg\forall x, \neg P(x)$ – **экзистенциальным** (в старомодном русском переводе "чистое доказательство существования"). Радикальные представители этих течений полностью отрицают, что экзистенциальное доказательство говорит нам что-либо о существовании x. Тем самым, например, полностью отрицаются все доказательства, использующие аксиому выбора.

Однако подавляющее большинство работающих математиков мало интересуется подобными тонкими различиями. Платон сказал "Все существующее свободно от противоречий, а все свободное от противоречий существует" (см. [Пуанкаре], в старом неточном переводе эта фраза была искажена до неузнаваемости: "все действительное разумно, а все разумное действительно"). Большинство математиков, вслед за Платоном, верит, что существует (exists) все что может существовать, а все, что не может не существовать – существует с необходимостью, или, на жаргоне физиков **действительно** существует (really exists). Однако конструктивисты, признают только такие вещи, которые **действительно** действительно существуют (really really exist) или же только такие вещи, которые **действительно** действительно действительно существуют (really really really exist) и так далее, по восходящей, в зависимости от степени верности всепобеждающему учению. Однако математики убеждены, что подобный подход не приносит в математику ничего нового, кроме некоторой вычурности языка.

Типичным примером экзистенциального доказательства является доказательство Кантора существования трансцендентных чисел, которое мы разбираем в Главе I. Вещественных чисел **строго больше**, чем алгебраических

в некотором точно определенном смысле, поэтому трансцендентные числа **не могут не существовать**. В то же время, предъявить хотя бы одно трансцендентное число, не говоря уже о том, чтобы доказать трансцендентность данного числа, совсем непросто. Доказательства Лиувилля, Эрмита, Линдеманна дают **эффективные** (впрочем, не уверен, конструктивные ли) доказательства существования трансцендентных чисел.

?. Неперестановочность кванторов. Нет сомнения, что два одноименных квантора $\forall$ и $\exists$ по различным переменным перестановочны между собой, т.е.

$$\forall x \forall y, P(x,y) \quad \Longleftrightarrow \quad \forall y \forall x, P(x,y),$$
$$\exists x \exists y, P(x,y) \quad \Longleftrightarrow \quad \exists y \exists x, P(x,y).$$

На самом деле, два одноименных квантора могут быть истолкованы как **один** квантор, по более широкой области переменных.

В то же время, два разноименных квантора вообще говоря не перестановочны. Верна лишь следующая импликация:

$$\exists x \forall y, P(x,y) \quad \Longrightarrow \quad \forall y \exists x, P(x,y),$$

однако обратная импликация не имеет места. В самом деле, если у каждой женщины деревни Аль-Фатх есть муж, отсюда, вообще говоря, не следует, что существует мужчина, который является мужем всех женщин этой деревни. А вот и математический пример. Пусть, например, $P(x,y)$ выражает отношение $x+y=0$. Тогда $\forall x \exists y, P(x,y)$ означает, что для любого x найдется y такое, что $x+y=0$, весьма правдоподобное свойство. Весьма сомнительно, чтобы отсюда чисто логически, без каких-либо дополнительных предположений о свойствах 0 и $+$, вытекало, что $\exists y \forall x, P(x,y)$, т.е. что найдется такое y, что $x+y=0$ для всех x.

Один из наиболее известных математических примеров неперестановочности кванторов – это определения поточечной сходимости и равномерной сходимости последовательности вещественных функций.

$$\forall \epsilon \in \mathbb{R}_+ \forall x \in \mathbb{R} \exists n \in \mathbb{N} \forall m \geq n, |f_m(x) - f(x)| < \epsilon,$$

$$\forall \epsilon \in \mathbb{R}_+ \exists n \in \mathbb{N} \forall x \in \mathbb{R} \forall m \geq n, |f_m(x) - f(x)| < \epsilon.$$

Ясно, что из второго утверждения следует первое, но не наоборот. В самом деле, во второй формуле утверждается, что 'найдется n' (одно и то же для всех x), а в первой формуле – что 'для каждого x найдется n' (для каждого свое).

?. Недистрибутивность кванторов относительно конъюнкции и дизъюнкции. Очевидно, что $\forall$ дистрибутивно относительно $\&$, а $\exists$ дистрибутивно относительно $\vee$, т.е.

$$\forall x, (P(x) \ \& \ Q(x)) \quad \Longleftrightarrow \quad (\forall x, P(x) \ \& \ \forall x, Q(x)),$$
$$\exists x, (P(x) \vee Q(x)) \quad \Longleftrightarrow \quad (\exists x, P(x) \vee \exists x, Q(x)).$$

В то же время, квантор $\forall$, вообще говоря, не дистрибутивен с $\vee$, а квантор $\exists$, вообще говоря, не дистрибутивен относительно $\&$. В действительности имеют место лишь следующие импликации:

$$(\forall x, P(x) \vee \forall x, Q(x)) \quad \Longrightarrow \quad \forall x, (P(x) \vee Q(x)),$$

$$\exists x, (P(x) \ \& \ Q(x)) \quad \Longrightarrow \quad (\exists x, P(x) \ \& \ \exists x, Q(x)).$$

Обратные импликации могут не выполняться. В самом деле, пусть x пробегает целые числа, P – свойство быть четным, а Q – свойство быть нечетным. Тогда любое x является четным или нечетным, но неверно, что любое x является четным или любое x является нечетным. Это показывает невозможность обратить первую импликацию. В тех же обозначениях существует четное x и существует нечетное x, но это не значит, что существует x, которое одновременно является четным и нечетным. Это показывает невозможность обратить вторую импликацию.

В действительности, правильное обращение с кванторами в подобных случаях состоит в том, чтобы ввести новую связанную переменную. Как мы знаем, $\forall x, P(x)$ означает то же самое, что $\forall y, P(y)$, а $\exists x, P(x)$ означает то же самое, что $\exists y, P(y)$. Таким образом, на самом деле нужно трактовать переменную x в $\forall x, P(x) \vee \forall x, Q(x))$ как две **разные** переменные, так что

$$(\forall x, P(x) \vee \forall x, Q(x)) \quad \Longleftrightarrow \quad \forall x \forall y (P(x) \vee Q(y))$$

и, по той же причине,

$$(\exists x, P(x) \ \& \ \exists x, Q(x)) \quad \Longleftrightarrow \quad \exists x \exists y (P(x) \ \& \ Q(y)).$$

§ ?. Математика и логика

Логика и математика тесно связанные, но глубоко различные науки. В первую очередь различны руководящие идеи и методы этих наук и, в особенности, ментальность математиков и логиков. Логика всегда интересовалась главным образом разложением доказательств на возможно большее число возможно меньших шагов, в то время как основная цель математики – поиск наиболее мощных и экономичных способов рассуждения, позволяющих охватывать одним взглядом громадные области внешне не связанных между собой явлений. Основные критерии ценности в чистой математике – это сила, красота и эффективность.

В целом связь математики с логикой не более тесная, чем, скажем, с физикой, астрономией, лингвистикой, музыкой или биологией. Многие математики глубоко интересовались логикой – но, видимо, еще больше таких, кто глубоко интересовался физикой и естественными науками, или, скажем, музыкой, искусством, историей или психологией.

Роль логики в математике в целом такая же, как роль грамматики в литературном творчестве. Как показывает опыт, знание грамматики не является, вообще говоря, ни необходимым,ни достаточным для грамотного письма. Изучение грамматики в школе может частично компенсировать отсутствие у ученика навыка грамотности, но целью обучения как раз и является выработка автоматизма, после чего все грамматические правила могут быть благополучно забыты. Точно так же роль логики в математике состоит в том, чтобы избегать очевидных ошибок в рассуждениях. Но одной из целей обучения математике как раз и является выработка автоматизма, после чего логические правила могут быть забыты. Более того, грамотному письму можно научить и иначе, без формальной грамматики, “по образцам”. Именно так обычно и происходит изучение стандартных логических

Логика, подобно грамматике – это леса, нужные, чтобы построить здание; после того, как оно построено, о них забывают. Знание законов акустики не только само по себе не делает владеющего им человека оперным певцом, но, и строго говоря, не является необходимым для успешной карьеры

Немногие математики дали себе труд познакомиться хотя бы с основами логики и никто из остальных не пострадал от своего невежества в этой области. Во всяком случае можно встретить первокласных специалистов по математическому анализу, дифференциальным уравнениям или теории вероятностей, которые никогда не слышали о “теории доказательств” или “языке первого порядка”, что нисколько не мешает им делать замечательные математические открытия и доказывать Ван Хао выразил это следующими словами: “Традиционная логика больше мешает, чем помогает нашему рассуждению, которое вполне удовлетворяется нашими естественными способностями. Это видно из того факта, что чем более чисто рациональной является деятельность, тем менее эта логика нужна.”

Я думаю, что подавляющее большинство математиков подпишется под следующей фразой Юрия Манина: “Вероятно, логика способна обосновать математику не в большей мере, чем биология – обосновать жизнь”.

> Mais, si la logique est l’hygiène du mathematicien, ce n’est pas elle qui lui fournit sa nouritture; le pain quotidien don’t il vit, ce sont les grandes problèmes.
>
> Andrè Weil “L’Avenir des Mathematiques”, Collected Works, 1947a.

> Довольно этой канцелярщины, Генрих. Напишите там, “Брак считается совершившимся” и давайте кушать. Ужасно кушать хочется.
>
> Е.Л.Шварц ‘Дракон’

§ ?. Аксиоматика

Рассматривая модели, лучше иметь их две, чем одну, так как это устраняет соблазн придавать какой-нибудь из них чрезмерное значение. Наши геометрические рассуждения опираются только на аксиомы.

Г.С.М.Коксетер, "Введение в геометрию", М., Наука, 1966, 648с. с.419

§ 7. Метод математической индукции

Многие доказательства проводятся 'по индукции'. В простейшем случае принцип индукции выглядит так.

1. Принцип математической индукции. Пусть имеется некоторый предикат P определенный на множестве $\mathbb{N}$ натуральных чисел. Предположим, что выполнены следующие два утверждения: 1) $P(1)$ истинно (**база индукции**), 2) Для любого $n \in \mathbb{N}$ истинность $P(n)$ (**индукционное предположение**) влечет истинность $P(n+1)$ (**шаг индукции alias индукционный переход**). Тогда $P(n)$ истинно для всех $n \in \mathbb{N}$.

Сформулированный выше принцип называется также **аксиомой индукции**, так как он фигурировал (под номером 5) в списке **аксиом Пеано**. Говоря по-простому, если какое-то подмножество $X \subseteq \mathbb{N}$ содержит 1 и вместе с каждым натуральным числом n содержит также $n+1$, то $X = \mathbb{N}$. Формализация этой аксиомы присутствует и в **формальной арифметике**, но, разумеется, там она гораздо слабее, так как теперь ее можно применять не ко всем предикатам, а лишь к тем из них, которые выражаются формулами языка первого порядка.

Вот несколько известных задач, легко решаемых методом индукции.

2. Задача. Чему равна сумма углов n-угольника?

3. Задача. Докажите, что шахматную доску с удаленной угловой клеткой можно замостить костяшками тримино в форме 'уголков'.

Указание. Воспользуйтесь принципом Лагранжа и считайте, что $8 = 2^n$.

4. Задача. На сколько частей делят плоскость n прямых в общем положении. (Говорят, что прямые находятся **в общем положении**, если никакие две из них не параллельны и никакие три не пересекаются в одной точке.)

5. Задача. На сколько частей делят плоскость прямые, проведенные через всевозможные пары n точек в общем положении. (Говорят, что точки находятся **в общем положении**, если никакие три из них не лежат на одной прямой и никакие три прямые, проведенные через пары этих точек, не пересекаются в точке, отличной от исходных.)

Указание. Внимание! Прямые, проведенные через n точек в общем положении, не образуют $\binom{n}{2}$ прямых в общем положении, если $n \geq 4$. Эта задача очень близка к задаче, упомянутой на с.58 книги А.И.Кострикина.

6. Задача. Чтобы закрепить понятие **общего положения**, посчитайте, на сколько частей делят пространство n плоскостей в общем положении. (Говорят, что плоскости находятся в **общем положении**, если никакие две из них не параллельны, никакие три не проходят через одну прямую, любые три имеют общую точку, никакие четыре не проходят через одну точку – первые три из этих условий означают просто, что никакие три плоскости не параллельны одной прямой).

7. Задача. Пусть H_n обозначает n-е **гармоническое число**,

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}.$$

Найти формулу для $H_1 + \ldots + H_m$.

Указание. Решающей подсказкой является слово 'найти' в формулировке задачи, которое указывает на то, что такая формула существует. После того, как вы догадаетесь до ответа $H_1+\ldots+H_m = (m+1)(H_{m+1}-1)$, доказательство его по индукции совершенно стандартно. Существует, разумеется, и стандартный метод нахождения ответа в подобных ситуациях, не требующий никакого угадывания, а именно, восходящий к Эйлеру и Лапласу метод **производящих функций**, называемый по-английски 'generatingfunctionology'.

7. Александр Македонский не существовал. В сборнике "Физики шутят" приводится доказательство теоремы, утверждающей, что Александр Македонский не существовал. Это доказательство основано на трех леммах, из которых для нас представляет интерес следующая

8. 'Лемма'. Все предметы одного цвета.

'Доказательство'. База индукции. Один предмет одного цвета.

Шаг индукции. Предположим, что любые n предметов одного цвета. Возьмем $n + 1$ предмет. Выбросим один из этих предметов, по индукционному предположению оставшиеся n предметов одного цвета. Выбросим теперь один из этих n предметов и добавим выброшенный ранее $n + 1$-й предмет. Снова по индукционному предположению эти n предметов одного цвета, следовательно, цвет $n + 1$-го предмета совпадает с цветом первых n предметов, что и требовалось доказать.

9. Принцип домино. Это 'доказательство' показывает, что нужно быть осторожным с тем, что в действительности является базой индукции – если мы хотим, чтобы заключение выполнялось для всех натуральных чисел, индукционный шаг должен проходить для **всех** натуральных n, начиная с 1, а в этом случае он предполагает, что пересечение двух n-элементных подмножеств $n + 1$-элементного множества непусто, т.е. нарушается в случае $n = 1$. И действительно, повседневный опыт подсказывает нам, что существуют два предмета разного цвета.

Наглядно индукционное рассуждение может быть проиллюстрировано следующим образом. Расставим (счетное) множество костяшек домино в цепочку друг за другом, так, чтобы достаточно близко за каждой костяшкой стояла ровно одна непосредственно следующая и перед каждой костяшкой, кроме ровно одной, называемой 'первой', стояла ровно одна непосредственно предшествующая. Предположим, теперь, что выполняются два условия: 1) мы толкнули первую костяшку с силой, достаточной, чтобы она упала (база индукции); 2) для каждой костяшки верно, что падая (индукционное предположение) она толкнет непосредственно следующую костяшку с силой, достаточной, чтобы опрокинуть и ее (шаг индукции). Тогда принцип математической индукции, называемый в просторечии **принципом домино**, гласит, что **все** костяшки упадут.

10. Варианты индукции. Часто возникают различные варианты индукции. Упомянем некоторые наиболее часто встречающиеся из них.

Во-первых, индукция может начинаться не с $n = 1$ а с какого-то натурального $n > 1$, в этом случае также и заключение индукции справедливо начиная с этого n.

Кратная индукция.

.

Совместная индукция. В большинстве настоящих доказательств индукция встречается как **совместная индукция** по нескольким параметрам. Это значит, что

Раздел. III. Совсем наивная теория категорий

> Что именно подразумевается под словом "категория" у Аристотеля, у Канта и у Гегеля, я, признаться, никогда не был в состоянии понять.
>
> Бертран Рассел, История Западной Философии (М., 1959, С.223)

Гл. ?. Основные определения

§ 1. Категории

В этом параграфе мы определим основную структуру сегодняшней математики.

Математика как теория категорий. Точка зрения, что математика *является* теорией множеств многократно декларировалась и мы обсуждали ее в § ?. Однако за прошедшие полвека перспектива изменилась. В 1945 году Эйленберг и Маклейн ввели категории, функторы и естественные эквивалентности. Сегодня, спустя более чем полвека, можно определенно утверждать, что теория категорий дает обоснование математики не просто альтернативное к теории множеств, а гораздо более глубокое, включающее в себя теорию множеств, как нулевой уровень, но далеко выходящее за ее пределы.

Неформально отличие теории категорий от теории множеств можно описать следуюшим образом. Теория множеств выражает все в терминах понятия *принадлежности*. В отличие от нее теория категорий выражает все остальные математические понятия (в том числе и принадлежность) в терминах понятия *бинарного отношения* (которое при этом не отождествляется со своим графиком, а воспринимается как первичное понятие). Часто говорят, что теория категорий выражает все в терминах *отображений*, но это не совсем точно. Основной пример категории – это категория множеств, морфизмами которой являются бинарные отношения. Иными словами, теория множеств связана с 'внутренними' свойствами объектов, а теория категорий – с их 'внешними' свойствами. Замечательным открытием теории категорий является то, что все свойства объекта могут быть выражены в терминах его связей с другими объектами. Это уже привело к изменению многих точек зрения в математике. Для человека, воспитанного на классической математике, многие конструкции теории категорий могут показаться чрезмерно абстрактными и туманными, но объективные медицинские исследования показывают, что изучение теории категорий стимулирует деятельность мозга и в большинстве случаев приводит к появлению дополнительных нейронов.

2. Категория. Вот основное определение этой главы.

Определение. Категория $\mathcal{C}$ *состоит из следующих данных:*

i) *класса объектов* $\mathrm{Ob}(\mathcal{C})$*, элементы которого называются* **объектами** *категории* $\mathcal{C}$*;*

ii) *набора множеств* $\mathrm{Hom}(A,B)$ *по одному каждых двух объектов* $A,B\in\mathcal{C}$*, элементы которых называются* **морфизмами** *категории* $\mathcal{C}$*;*

iii) *набора отображений* $\mathrm{Hom}(A,B)\times\mathrm{Hom}(B,C)\longrightarrow\mathrm{Hom}(A,C)$*, по одному для каждой тройки объектов* $A,B,C\in\mathrm{Ob}(C)$*, называемых* **композицией** *морфизмов категории* $\mathcal{C}$*;*

удовлетворяющих следующим трем аксиомам:

(C1) *Множества* $\mathrm{Hom}(A,B)$ *попарно не пересекаются.*

(C2) *Композиция морфизмов ассоциативна.*

(C3) *Для каждого объекта* $A\in\mathcal{C}$ *существует морфизм* $1_X\in\mathrm{Hom}(A,A)$*, являющийся двусторонним нейтральным элементом относительно композиции.*

3. Класс морфизмов категории. Поясним это определение. Прежде всего заметим, что для краткости обычно пишут просто $A\in\mathcal{C}$ вместо $A\in\mathrm{Ob}(\mathcal{C})$. Обозначим через $\mathrm{Mor}(\mathcal{C})$ *класс* всех морфизмов категории (мы предполагаем, что для любых двух объектов $\mathrm{Hom}(A,B)$ является *множеством*, так что $\mathrm{Mor}(\mathcal{C})$ является объединением множеств, но индексы A и B этого объединения пробегают класс $\mathrm{Ob}(\mathcal{C})$, который не обязан быть множеством). Множество $\mathrm{Hom}(A,B)$ называется **множеством морфизмов из** A **в** B **в категории** $\mathcal{C}$. Если рассматривается одновременно несколько категорий, то, чтобы уточнить, о какой именно идет речь, часто пишут еще $\mathrm{Hom}_{\mathcal{C}}(A,B)$. Отметим, что многие авторы обозначают $\mathrm{Hom}(A,B)$ через $\mathrm{Mor}(A,B)$ или $\mathcal{C}(A,B)$.

4. Определение. *Категория называется* **малой***, если класс* $\mathrm{Ob}(\mathcal{C})$ *(или что то же самое, класс* $\mathrm{Mor}(\mathcal{C})$*) является множеством. В противном случае категория называется* **большой***.*

5. Область и кообласть. Аксиома (C1) утверждает, $\mathrm{Mor}(\mathcal{C})=\coprod\mathrm{Hom}(A,B)$, $A,B\in\mathcal{C}$), что для каждого морфизма $\phi\in\mathrm{Mor}(\mathcal{C})$ объекты $A,B\in\mathrm{Ob}(\mathcal{C})$ такие, что $\phi\in\mathrm{Hom}(A,B)$ определены однозначно. Объекты A и B такие, что $\phi\in\mathrm{Hom}(A,B)$, называются, соответственно, **областью** и **кообластью** (alias **областью определения** и **областью значений**) морфизма ϕ. Область и кообласть обозначаются через $\mathrm{Dom}(\phi)$ и $\mathrm{Cod}(\phi)$ через $D(\phi)$ и $R(\Phi)$ ('domain' и 'range') или, через $S(\phi)$ и $T(\phi)$ ('source' и 'target'). Морфизм из A в B обозначается $\phi:A\longrightarrow B$ или $A\xrightarrow{\phi}B$. Согласно iii для любых двух морфизмов $\phi\in\mathrm{Hom}(A,B)$ и $\psi\in\mathrm{Hom}(B,C)$ таких, что $S(\psi)=T(\phi)$ определен морфизм $\phi\psi\in\mathrm{Hom}(A,C)$, называемый **композицией** морфизмов ϕ и ψ в категории $\mathcal{C}$, такой, что $S(\phi\psi)=S(\phi)$, а $T(\phi\psi)=T(\psi)$.

Аксиомы (C2) и (C3) следует понимать в том смысле, как ассоциативность и нейтральный элемент понимаются для не всюду определенной операции. Иными словами, композиции $\chi(\phi\psi)$ и $(\chi\phi)\psi$ равны, *если хотя бы одна из них определена.* Точно так же, $1_{S(\phi)}\phi=\phi$ и $\phi 1_{T(\phi)}=\phi$

§ 2. Категория множеств, ее друзья и родственники

Важнейшим примером категории является категория множеств, объектами которой являются множества, морфизмами – отображения множеств, а композиция морфизмов это обычная композиция отображений. В настоящем параграфе мы обсудим эту категорию и некоторые близко связанные с ней категории, или, как говорил Винни Пух, 'friends-and-relations'.

1. Категория множеств и отображений $\mathcal{S}et$**.** Обозначим через $\mathcal{S}et$ категорию, которая фактически была только что описана. Объектами $\mathcal{S}et$ являются множества, причем для двух множеств $A,B\in\mathrm{Ob}(\mathcal{S}et)$ множество морфизмов $\mathrm{Hom}_{\mathcal{S}et}(A,B)$ совпадает с $\mathrm{Map}(A,B)$. Этак категория называется **категорией множеств** или, если нужна особая точность, **категорией множеств и отображений** и обозначается $\mathcal{S}et$ или $\mathcal{E}ns$ (от французского 'Ensemble')

Вопрос. Почему выполняется аксиома C1? Получим ли мы категорию, если положим $\mathrm{Hom}(A, B)$ равным множеству всех *семейств* элементов из B индексированных элементами A?

Единственное существенное отличие от того, что происходило в Гл. 1, состоит в том, что морфизмы в категории $\mathcal{S}et$, как и вообще в теории категорий, принято компоновать *слева направо*, а не справа налево, как мы это делали в теории множеств. Таким образом, первый действующий морфизм записывается первым, а не вторым, как до сих пор. Это значит, что если $\phi \in \mathrm{Hom}(A, B)$ и $\psi \in \mathrm{Hom}(B, C)$, то их **композицией** в категории $\mathcal{S}et$ принято называть морфизм $\phi\psi \in \mathrm{Hom}(A, C)$, который раньше обозначался через $\psi \circ \phi$. Такое изменение обозначений связано со следующим обстоятельством: раньше мы вынуждены были компоновать отображения справа налево поскольку мы писали функцию слева от аргумента. В теории же категорий мы не рассматриваем образы индивидуальных элементов и, поэтому, нет никакого препятствия к тому, чтобы записывать компонуемые отображения в *естественном порядке*, когда пришедшие первыми обслуживаются первыми – 'customers will be executed in strict order'.

2. Категория множеств, содержащихся в некотором универсуме $\mathcal{S}et_U$. Категория всех множеств очень велика – в терминологии § 1 она является большой категорией – и поэтому, с целью теоретико-множественной гигиены, часто рассматривают связанные с ней меньшие категории, объекты которых образуют множество. Наиболее популярный вариант состоит в том, чтобы зафиксировать некоторый универсум U и рассматривать в качестве объектов категории не все множества, а только те из них, которые принадлежат U. Морфизмы же и их композиция определяются обычным образом. Получающаяся так категория обозначается $\mathcal{S}et_U$. С точки зрения всех возможных приложений в обычной математике между категориями $\mathcal{S}et$ и $\mathcal{S}et_U$ нет никакой разницы, поскольку все множества, рассматриваемые в алгебре, анализе, геометрии, ..., являются элементами U. В то же время категория $\mathcal{S}et_U$ является малой, в том смысле, что класс ее объектов $\mathrm{Ob}(\mathcal{S}et_U) = U$ образует множество.

3. Категория конечных множеств $\mathcal{F}inSet$. Еще одна категория, связанная с категорией множеств, это категория $\mathcal{F}inSet$ конечных множеств, объектами которой являются конечные множества, а морфизмы и их композиция снова определяются обычным образом.

4. Категория множеств и отображений, подчиненных дополнительному условию. Рассмотрим какой-то класс отображений, обладающих тем свойством, что все тождественные отображения принадлежат этому классу и композиция двух отображений из этого класса снова принадлежит этому классу. Ясно, что этим свойством обладают, например, классы инъективных, сюръективных и биективных отображений. Таким образом, можно определить категории $\mathcal{I}nj$, $\mathcal{S}ur$, $\mathcal{B}in$, объектами которых являются множества, а морфизмами между двумя множествами A и B являются, соответственно, все инъективные, сюръективные и биективные отображения из A в B, иными словами, $\mathrm{Hom}_{\mathcal{I}nj}(A, B) = \mathrm{Inj}(A, B)$, $\mathrm{Hom}_{\mathcal{S}ur}(A, B) = \mathrm{Sur}(A, B)$, $\mathrm{Hom}_{\mathcal{B}ij}(A, B) = \mathrm{Bij}(A, B)$.

5. Категория множеств и бинарных отношений $\mathcal{B}in$. Чтобы у читателя не создалось впечатление, что морфизмы обязаны быть отображениями,

построим сразу же еще одну категорию, объектами которой являются множества, но морфизмы не отображения. А именно, обозначим через Bin категорию бинарных отношений. Объекты категории $\mathcal{B}in$ такие же, как и $\mathcal{S}et$, но для двух множеств $A, B \in \mathrm{Ob}(\mathcal{B}in)$ множество морфизмов $\mathrm{Hom}_{\mathcal{B}in}(A, B)$ совпадает с множеством $\mathrm{Rel}(A, B)$ всех бинарных отношений. При этом композиция морфизмов в $\mathcal{B}in$ – это обычная композиция бинарных отношений, причем именно в том порядке, как мы это делали в Главе ?.

6. Категория множеств и степенных отображений $\mathcal{P}ow$. Для некоторых целей удобно рассматривать категорию $\mathcal{P}ow$ еще более обширную, чем категория $\mathcal{B}in$. Ее объектами по прежнему являются множества, но морфизмами из множества A в множество B являются всевозможные отображения $2^A \longrightarrow 2^B$, иными словами, $\mathrm{Hom}_{\mathcal{P}ow}(A, B) = \mathrm{Map}(2^A, 2^B)$. При этом тождественным морфизмом объекта $A \in \mathrm{Ob}(\mathcal{P}ow)$ является тождественное отображение множества 2^A, а композиция двух морфизмов в $\mathcal{P}ow$ — это обычная композиция отображений.

7. Категория множеств с отмеченной точкой $\mathcal{S}et_\bullet$. Объектами категории $\mathcal{S}et_\bullet$ являются множества с отмеченной точкой $(A, *_A)$, а морфизмами — морфизмы множеств с отмеченнной точкой, т.е. такие отображения $f : A \longrightarrow B$, что $f(*_A) = *_B$. При этом, как и в категории $\mathcal{S}et$, морфизмы компонуются слева направо.

8. Категория пар множеств $\mathcal{P}air$. Объектами категории $\mathcal{P}air$ являются пары множеств (A, B), $B \subseteq A$ а морфизмами – морфизмы пар (см. § 4.?), т.е. для двух пар $C_1 = (A_1, B_1)$ и $C_2 = (A_2, B_2)$ множество $\mathrm{Hom}_{\mathcal{P}air}(C_1, C_2)$ состоит из таких отображений $f : A_1 \longrightarrow A_2$, для которых $f(B_1) \subseteq B_2$.

9. Категория реляционных систем $\mathcal{R}el$. Объектами этой категории являются реляционные системы, т.е. пары (A, R), где A – множество, а $R \subseteq A \times A$ – внутреннее бинарное отношение на A (см. § ?.?), а морфизмы – это морфизмы реляционных систем. Иными словами, для двух реляционных систем (A, R) и (B, S) множество $\mathrm{Hom}_{\mathcal{R}el}((A, R), (B, S))$ состоит из таких отображений $f : A \longrightarrow B$, для которых $(f, f)(R) \subseteq S$, где $(f, f) : A \times A \longrightarrow B \times B$ – покомпонентное отображение, определенное посредством $(f, f)(a, b) = (f(a), f(b))$ для $a, b \in A$.

10. Категория отображений $\mathcal{M}ap$. Объектами категории $\mathcal{M}ap$ являются отображения $f : X \longrightarrow Y$. При этом морфизмом отображения $f : X \longrightarrow Y$ в отображение $g : U \longrightarrow V$ называется **пара** отображений $h : X \longrightarrow U$, $i : Y \longrightarrow V$ таких, что $g \circ h = i \circ f$.

§ ?. Подкатегории

1. Определение. *Говорят, что категория $\mathcal{B}$ является* **подкатегорией** *категории $\mathcal{C}$, если выполняются следующие четыре условия:*

Sub1) *Каждый объект категории $\mathcal{B}$ является объектом категории $\mathcal{C}$, т.е.* $\mathrm{Ob}(\mathcal{B}) \subseteq \mathrm{Ob}(\mathcal{C})$*;*

Sub2) *Каждый морфизм категории $\mathcal{B}$ является морфизмом категории $\mathcal{C}$, с той же областью и кообластью, т.е. для любых двух $A, B \in \mathrm{Ob}(\mathcal{C})$ выполняется* $\mathrm{Hom}_{\mathcal{B}}(A, B) \subseteq \mathrm{Hom}_{\mathcal{C}}(A, B)$*;*

Sub3) *Композиция двух морфизмов из $\mathcal{B}$ в $\mathcal{B}$ совпадает с их композицией в $\mathcal{C}$;*

Sub4) *Тождественный морфизм любого объекта категории $\mathcal{B}$ в $\mathcal{B}$ совпадает с тождественным объектом этого объекта в $\mathcal{C}$.*

Задача. Приведите пример, показывающий, что условие Sub4 не вытекает из условий Sub1 – Sub3.

2. Определение. *Подкатегория $\mathcal{B}$ называется* **полной подкатегорией** *категории $\mathcal{C}$, если для любых двух объектов $A, B \in \mathrm{Ob}(\mathcal{B})$ выполняется равенство $\mathrm{Hom}_{\mathcal{B}}(A, B) = \mathrm{Hom}_{\mathcal{C}}(A, B)$.*

3. Первые примеры подкатегорий. Сейчас мы рассмотрим, какие из категорий, введенных в § 1, являются подкатегориями других введенных там категорий.

3.1) Категория $\mathcal{S}et$ является подкатегорией категории $\mathcal{B}in$, заведомо неполной, но такой, что $\mathrm{Ob}(Set) = \mathrm{Ob}(\mathcal{B}in)$;

3.2) Категория $\mathcal{F}inSet$ является полной подкатегорией категории $\mathcal{S}et$.

3.3)

ТОПОЛОГИЧЕСКИЕ ПРОСТРАНСТВА

Гл. ?. Топологические пространства

§ ?. Топологии

Структура топологического пространства является одной из основных в математике. Ее можно задавать многими различными (но эквивалентными между собой) способами. Обычный способ, приводящий к наиболее элегантным определениям, состоит в выделении на X топологии.

Определение. *Подмножество $T \subseteq 2^X$ называется* **топологией** *на множестве X, если оно удовлетворяет следующим трем аксиомам:*

O1) *T замкнуто относительно* **произвольных** *объединений: $U_\alpha \in T \Rightarrow \bigcup U_\alpha \in T$;*

O2) *T замкнуто относительно* **конечных** *пересечений: $U, V \in T \Rightarrow U \cap V \in T$;*

O3) *$\varnothing, X \in T$.*

Множество X вместе с заданной на нем топологией называется **топологическим пространством**. *При этом элементы $A \in T$, рассматриваемые как подмножества в X, называются* **открытыми** *множествами, а их дополнения в X –* **замкнутыми** *множествами.*

Если T_1, T_2 – две топологии на множестве X, то говорят, что T_1 **сильнее** (или **богаче** или **тоньше**), чем T_2 и пишут $T_1 \geq T_2$, если $T_1 \supseteq T_2$ как подмножество в 2^X. В этом случае про топологию T_2 говорят, что она **слабее** (или **беднее** или **грубее**), чем T_1. Среди всех топологий на X существует самая сильная топология $T = 2^X$, называемая **дискретной**, в которой **все** подмножества X открыты и самая слабая топология $T = \{\varnothing, X\}$, называемая **тривиальной**, единственными открытыми множествами в которой являются $\varnothing$ и само X. В любой топологии множества $\varnothing$ и X являются как открытыми, так и замкнутыми – такие множества называются **открыто-замкнутыми** (по-английски обычно используется обратный порядок 'clopen' = 'closed + open').

В алгебре топология обычно задается посредством задания системы **замкнутых** множеств.

Определение. *Подмножество $T' \subseteq 2^X$ называется '***топологией***' на множестве X, если оно удовлетворяет следующим трем аксиомам:*

(Z1) *T' замкнуто относительно* **произвольных** *пересечений: $Z_\alpha \in T' \Rightarrow \bigcap Z_\alpha \in T'$;*

(Z2) *T замкнуто относительно* **конечных** *объединений: $Y, Z \in T' \Rightarrow Y \cup Z \in T'$;*

(Z3) *$\varnothing, X \in T'$.*

Легко видеть, что эти понятия двойственны между собой:

Задача Проверьте, что если T' – 'топология' на X, то $T = \{\overline{Y} \mid Y \in T'\}$ – топология.

Задавать топологии, перечисляя все открытые множества, обычно довольно трудно, поэтому ограничимся несколькими очевидными примерами, оставляя

дальнейшие примеры до того момента, когда мы научимся более более эффективным способам вводить на X структуру топологического пространства.

Первые примеры топологий. 1) Как мы уже упомянули, на любом множестве можно ввести **дискретную** и **тривиальную** топологии.

2) Топология на конечном множестве X это то же самое, что подрешетка с 0 и 1 в решетке множеств 2^X.

3) Пусть теперь X – бесконечное множество, а T – подмножество в 2^X, состоящее из $\varnothing$ и тех множеств, дополнения к которым конечны. Эта топология называется **коконечной**.

Задача. Проверить, что T является топологией. Убедиться в том, что любые два непустых открытых множества этой топологии пересекаются.

В случае, когда X – множество точек некоторого поля (например, $X = \mathbb{Q}, \mathbb{R}, \mathbb{C}$), эта топология совпадает с **топологией Зарискоого**, которая будет определена в § ?.

Задача. Обобщить эту конструкцию, взяв в качестве открытых множеств $\varnothing$ и те множества, дополнения к которым конечны или счетны и т.д.

4) **Вещественная топология.** Пусть $X = \mathbb{R}$, а T состоит из всевозможных дизъюнктных объединений конечных или бесконечных интервалов (см. пример ?)

Задача. Доказать, что любая система попарно непересекающихся интервалов в $\mathbb{R}$ не более, чем счетна. Таким образом, в предшествующем определении можно говорить о **конечных либо счетных** семействах интервалов.
Указание. Любой непустой интервал содержит хотя бы одну рациональную точку.

Задача. Проверить, что T действительно является топологией. Привести пример бесконечного семейства открытых множеств этой топологии, пересечение которых не является открытым.
Ответ. $(-1/n, 1/n)$, $n \in \mathbb{N}$.

§ ?. Базы топологии

Рассматриваемые в анализе топологии обычно слишком богаты, чтобы можно было явно задать **все** открытые множества. В действительности уже в вещественной топологии в $\mathbb{R}^2$ перечислить все открытые множества было бы весьма затруднительно. Для большинства целей обычно перечислить достаточно указать лишь **образующие** T относительно операции (бесконечного!) объединения (либо относительно операций объединения и пересечения).

Определение. *Семейство $B \subseteq T$ открытых множеств называется* **базисом** *(или* **базой***) топологии T, если любое открытое множество можно представить как объединение множеств из B.*

Напомним, что семейство B называется **покрытием** X, если $X = \bigcup U$, $U \in B$.

Задача. Покажите, что $B \subseteq 2^X$ в том и только том случае образует базис некоторой топологии, когда

1) B является покрытием X,

2) для любых $U_1, U_2 \in B$ их пересечение можно представить в виде объединения подходящих множеств из B, т.е. $U_1 \cap U_2 = \bigcup V_\alpha$ для некоторых $V_\alpha \in B$.

Разумеется, уже сложность континуальных объединений не поддается никакому контролю.

§ ?. Фильтры

Определение. *Непустое подмножество $F \subseteq 2^X$ называется* **фильтром**, *если выполняются следующие две аксиомы:*

(F1) $A, B \in F \Rightarrow A \cap B \in F$,

(F2) $A \in F$, $A \subseteq B \Rightarrow B \in F$.

Очевидно, что если $\varnothing \in F$, то $F = 2^X$. Фильтр F называется **собственным**, если он отличен от 2^X, то есть если он не содержит пустого множества. Во многих книгах (в частности, в [B]) рассматриваются только собственные фильтры, т.е. фактически к определению фильтра добавляется еще следующая аксиома:

(F3) $\varnothing \notin F$.

По всей видимости, это делается с тем, чтобы говорить о **максимальных фильтрах** (alias **ультрафильтрах**) не оговаривая, что они максимальны среди **собственных** фильтров. Однако нам такое исключение представляется в высшей степени неестественным. Дело в том, что фильтры являются понятием, двойственным к понятию идеала. В теории колец само кольцо никогда не исключается из числа своих идеалов, а под максимальными идеалами понимаются идеалы, максимальные среди всех **собственных** идеалов. Чтобы подчеркнуть аналогию фильтров и идеалов, отметим, что условие (F2) можно сформулировать также в следующем виде:

(F2)' $A \in F$, $B \in 2^X \Rightarrow A \cup B \in F$.

Таким образом, фильтр **замкнут** относительно (конечных) пересечений и **устойчив** относительно объединений с произвольными элементами 2^X. Для сравнения заметим, что **идеалом** в булевой алгебре 2^X называется непустое подмножество **замкнутое** относительно (конечных) объединений и **устойчивое** относительно пересечений с произвольными элементами 2^X. Таким образом, идеал I удовлетворяет следующим двум условиям

(I1) $A, B \in I \Rightarrow A \cup B \in I$,

(I2) $A \in F$, $B \in 2^X \Rightarrow A \cap B \in F$.

При этом, чтобы подчеркнуть аналогию с приведенным выше определением фильтра, условие (I2) можно было бы сформулировать в следующем виде:

(I2)' $A \in I$, $B \subseteq A \Rightarrow B \in I$.

По аналогии с главными идеалами можно определить главные фильтры.

Определение. *Пусть $Y \subseteq X$ – произвольное подмножество в X. Тогда семейство $F_Y = \{Z \in 2^X \mid Z \supseteq Y\}$ называется* **главным фильтром**, *порожденным множеством Y.*

Ясно, что главный фильтр, порожденный множеством Y – это в точности наименьший фильтр в 2^X, содержащий Y. Для того, чтобы он был собственным, необходимо и достаточно, чтобы $Y \neq \varnothing$.

Задача ?. Показать, что если X конечно, то каждый фильтр в 2^X главный.

Решение. Фильтр F порождается множеством $Y = \cap Z$, где пересечение берется по всем $Z \in F$ (где здесь используется конечность множества X?).

Если множество X бесконечно, то в 2^X всегда существуют неглавные фильтры. Основным примером неглавного фильтра является семейство открытых множеств кокончной топологии.

Пример. Кокончным фильтром в 2^X называется фильтр Cof_X, состоящий их всех подмножеств $Y \subseteq X$, дополнение к которым конечно. Фильтр $\mathrm{Cof}_{\mathbb{N}}$ называется также **фильтром Фреше**.

Сейчас мы обобщим способ, которым строились главные фильтры, и построим фильтр, порожденный произвольным семейством D подмножеств в X. Прежде всего, очевидно, что если в D найдутся такие подмножества $Y_1, \dots, Y_n$, что $Y_1 \cap \dots \cap Y_n = \varnothing$, то любой фильтр, содержащий $Y_1, \dots, Y_n$ содержит $\varnothing$ и, поэтому, совпадает с несобственным фильтром 2^X. Это мотивирует следующее определение.

Определение. *Говорят, что семейство $D \subseteq 2^X$ обладает* **свойством конечных пересечений**, (*сокращенно* **FIP**) *если пересечение любой конечной совокупности множеств из D непусто.*

Как мы только что убедились, семейство, не обладающее **FIP**, не содержится ни в одном собственном фильтре. Оказывается, верно и обратное.

Задача ?. Докажите, что любое семейство $D \subseteq 2^X$, обладающее свойством конечных пересечений, содержится в некотором собственном фильтре F.

Решение. В качестве F можно взять

$$F_D = \{Z \in 2^X \mid \exists Y_1, \dots, Y_n \in D, Z \supseteq Y_1 \cap \dots \cap Y_n\}.$$

По определению **FIP** имеем $\varnothing \notin F_D$.

Про фильтр F_D мы будем говорить, что он **порожден** семейстом D, а само семейство D будет называться **системой образующих** фильтра F_D. Главный фильтр F_Y – это в точности фильтр, порожденный одноэлементным семейством $D = \{Y\}$. Как мы видели в Задаче ?, фильтр, порожденный **конечным** семейством $D = \{Y_1, \dots, Y_n\}$, в действительности является главным, так как он порождается $Y_1 \cap \dots \cap Y_n$.

Для любого собственного фильтра F в 2^X и любого подмножества $Y \subseteq X$ хотя бы одно из множеств Y, $\overline{Y}$ не принадлежит F (почему?).

Определение. *Собственный фильтр $F \subset 2^X$ называется* **ультрафильтром**, *если для любого подмножества $Y \subseteq X$ имеет место альтернатива: либо $Y \in F$, либо $\overline{Y} \in F$.*

Сейчас мы покажем, что ультрафильтры - это в точности максимальные фильтры. Напомним, что фильтр F называется **максимальным**, если он максимален среди **собственных** фильтров. При этом порядок на множестве фильтров индуцируется включением как подмножеств в 2^X. Пусть E и F – два фильтра на X такие, что E содержится в F, т.е. $E \subseteq F$. В этом случае, как и для топологий, часто говорят, что F сильнее, чем E, а E слабее, чем F.

Предложение ?. *Фильтр F в том и только том случае является ультрафильтром, когда он максимален.*

Доказательство. Пусть F – ультрафильтр и E – строго больший фильтр. Пусть $Y \in E \setminus F$. Тогда по определению ультрафильтра $\overline{Y} \in F \subseteq E$. Таким образом, $Y, \overline{Y} \in E$ и, значит, фильтр E не является собственным.

Обратно, пусть F не является ультрафильтром, то найдется такое подмножество $Y \subseteq X$, что ни само Y, ни его дополнение $\overline{Y}$ не принадлежат F. Тогда семейство $D = F \cup \{Y\}$ обладает свойством конечных пересечений. В самом деле, так как F фильтр, любое конечное пересечение элементов из D имеет вид $Z \cap Y$ для некоторого $Z \in F$, а (так как мы предположили, что $\overline{Y} \notin F$) такое пересечение не может быть пустым. В силу предыдущей задачи семейство D содержится в собственном фильтре E, причем $Y \in E \setminus F$, так что E строго больше, чем F.

В действительности, в теории колец есть класс идеалов гораздо более важный, чем класс максимальных идеалов, а именно, класс простых идеалов. Аналогом простого идеала для фильтров является следующее понятие. Фильтр F называется **простым**, если для любого $Y \in F$ из того, что $Y = Z_1 \cup Z_2$, следует, что $Z_1 \in F$ или $Z_2 \in F$. Разумеется, по индукции отсюда следует, что то же самое верно для любого представления $Y \in F$ в виде конечного объединения $Y = Z_1 \cup \ldots \cup Z_n$. В любом таком объединении хотя бы одно из Z_i принадлежит F. Как мы знаем, каждый максимальный идеал является простым.

Задача ?. Докажите, что каждый ультрафильтр прост. Решение. Пусть $Y = Z_1 \cup Z_2 \in F$, а $Z_1, Z_2 \notin F$. Тогда по определению ультрафильтра $\overline{Y} = \overline{Z_1} \cap \overline{Z_2} \in F$, так что $\varnothing = Y \cap \overline{Y} \in F$, что противоречит тому, что F собственный.

Как мы только что убедились, для любого фильтра имеет место следующая альтернатива: он либо является главным, либо не может быть порожден конечным числом своих элементов. Посмотрим, во что эта альтернатива превращается для ультрафильтров. Охарактеризовать главные ультрафильтры совсем просто.

Задача ?. Докажите, что единственными главными ультрафильтрами являются фильтры вида $F_x \in F_{\{x\}}$, $x \in X$, порожденные одноэлементными множествами. Решение. Ясно, что для подмножества $Y \subseteq X$ имеется альтернатива $x \in Y$ или $x \in \overline{Y}$, поэтому F_x – ультрафильтр. Обратно, если F_Y, $Y \subseteq X$, главный фильтр порожденный подмножеством Y, содержащим более одного элемента, а Z – непустое собственное подмножество в Y, то главный фильтр F_Z собственный и строго больше, чем F_Y.

Было бы совсем непросто столь же явно описать ультрафильтры, не являющиеся главными, однако они допускают следующую простую характеризацию, подчеркивающую фундаментальную важность коконечного фильтра Cof_X.

Предложение ?. *Ультрафильтр F в том и только том случае не является главным, когда он содержит* Cof_X.

Доказательсво. Если F – ультрафильтр, не являющийся главным, то для любой точки $x \in X$ имеем $\{x\} \notin F$. Тогда по определению ультрафильтра $\overline{x} = X \setminus \{x\} \in F$. Таким образом, для любого конечного множества $Y = \{x_1, \ldots, x_n\}$ его дополнение $\overline{Y} = \overline{x}_1 \cap \ldots \cap x_n$ принадлежит F, но это

и значит, что $F \geq \mathrm{Cof}_X$. Обратно, если F содержит Cof_X, то $\overline{x} \in F$ для всех $x \in X$ и, так как F собственный, то $\{x\} \notin F$.

§ ?. Фильтр окрестностей

Сейчас мы научимся задавать топологию набором **локальных** данных.

§ ?. Операции замыкания и внутренности

Структуру топологического пространства на X можно задавать и еще одним способом, посредством унарных операций на 2^X, удовлетворяющим нескольким естественным условиям.

Определение. *Унарная операция* $\mathrm{Cl} : 2^X \longrightarrow 2^X$ *на множестве подмножеств некоторого множества* X *называется* **операцией замыкания**, *если она удовлетворяет следующим четырем аксиомам:*

(C1) $\mathrm{Cl}(A \cup B) = \mathrm{Cl}(A) \cup \mathrm{Cl}(B)$,

(C2) $A \subseteq \mathrm{Cl}(A)$,

(C3) $\mathrm{Cl}(\mathrm{Cl}(A)) = \mathrm{Cl}(A)$,

(C4) $\mathrm{Cl}(\varnothing) = \varnothing$, $\mathrm{Cl}(X) = X$.

Если на множестве 2^X *задана операция замыкания, то для любого* $A \subseteq X$ *множество* $\mathrm{Cl}(A)$ *называется* **замыканием** *множества* A

Фигурирующие в этом определении аксиомы обычно называются **аксиомами Куратовского**, хотя, как отмечает сам Куратовский [Ku], аналогичные аксиомы вводились ранее Ф.Риссом.

Задача. Показать, что из аксиом Куратовского вытекают следующие свойства замыкания:

(C5) $A \subseteq B \Rightarrow \mathrm{Cl}(A) \subseteq \mathrm{Cl}(B)$,

(C6) $\mathrm{Cl}(A \cap B) \subseteq \mathrm{Cl}(A) \cap \mathrm{Cl}(B)$,

(C7) $\mathrm{Cl}(A \setminus B) \subseteq \mathrm{Cl}(A) \setminus \mathrm{Cl}(B)$.

Несложно привести примеры, показывающие, что включения в пунктах (C6) и (C7) не обязаны быть равенствами.

Легко определить операцию, двойственную к операции замыкания, нужно лишь обратить все знаки включения, поменять местами $\cap$ и $\cup$ и т.д.

Определение. *Унарная операция* $\mathrm{Int} : 2^X \longrightarrow 2^X$ *на множестве подмножеств некоторого множества* X *называется* **операцией внутренности**, *если она удовлетворяет следующим четырем аксиомам:*

(C1) $\mathrm{Int}(A \cap B) = \mathrm{Int}(A) \cap \mathrm{Int}(B)$,

(C2) $\mathrm{Int}(A) \subseteq A$,

(C3) $\mathrm{Int}(\mathrm{Int}(A)) = \mathrm{Int}(A)$,

(C4) $\mathrm{Int}(\varnothing) = \varnothing$, $\mathrm{Int}(X) = X$.

Если на множестве 2^X *задана операция внутренности, то для любого* $A \subseteq X$ *множество* $\mathrm{Int}(A)$ *называется* **внутренностью** *множества* A

Обозначения $\mathrm{Cl}(A)$ и $\mathrm{Int}(A)$ происходят от английских терминов ‘Closure’ и ‘Interior’. В традиционных книгах по топологии или анализу замыкание множества A обычно обозначается через $\overline{A}$ (или иногда через $[A]$), а внутренность через A°.

Задача ?. Доказать, что если на 2^X задана операция замыкания, то $\overline{\mathrm{Int}(A)} = \mathrm{Cl}(\overline{A})$ задает на 2^X операцию внутренности, для которой $\mathrm{Cl}(A) = \overline{\mathrm{Int}(\overline{A})}$. Таким образом, задание на 2^X операций замыкания и внутренности эквивалентно.

Если Cl и Int – операции замыкания и внутренности, построенные по одной и той же топологии T на множестве X, то они находятся в двойственности, описанной в Задаче ?, т.е. для любого подмножества $A \subseteq X$ выполняются равенства $\mathrm{Cl}(\overline{A}) = \overline{\mathrm{Int}(A)}$ и $\mathrm{Int}(\overline{A}) = \overline{\mathrm{Cl}(A)}$.

§ ?. Произведение топологий

Лемма.

Доказательство.

(C4) $A \subseteq B \Rightarrow \mathrm{Int}(A) \subseteq \mathrm{Int}(B)$,