В. Босс

ЛЕКЦИИ *по* МАТЕМАТИКЕ

ТОМ 16

Теория множеств: От Кантора до Коэна

МОСКВА

URSS

ББК 22 152я73

Босс В.

Лекции по математике. Т. 16: Теория множеств: От Кантора до Коэна. Учебное пособие. — М.: Книжный дом «ЛИБРОКОМ», 2011. — 208 с.

Настоящий том «Лекций» посвящен теории множеств в диапазоне от наивной трактовки проблематики до ее современного (аксиоматического) состояния. Наряду с простейшими понятиями и результатами о манипулировании бесконечностями рассматриваются довольно тонкие феномены: парадокс Банаха—Тарского, кардинальная и ординальная арифметика, базисы Гамеля. Излагаются и обсуждаются также элементы матлогики, теории моделей и их связь с аксиоматическим подходом к теории множеств.

Изложение отличается краткостью и прозрачностью.

Для студентов, преподавателей, инженеров и научных работников.

Издательство «Книжный дом "ЛИБРОКОМ"».
117335, Москва, Нахимовский пр-т, 56.
Формат 60×90/16. Печ. л. 13 Зак № ГН-78

Отпечатано в ООО «ЛЕНАНД».
117312, Москва, пр-т Шестидесятилетия Октября, 11А, стр. 11.

ISBN 978–5–397–02162–3

Содержание

Предисловие к «Лекциям»

Спасибо тебе, Господи, что ты создал все нужное нетрудным, а все трудное — ненужным.

Сковорода

Для нормального изучения любого математического предмета необходимы, по крайней мере, 4 ингредиента:

1) *живой учитель*;
2) *обыкновенный подробный учебник*;
3) *рядовой задачник*;
4) *учебник, освобожденный от рутины, но дающий общую картину, мотивы, связи, «что зачем»*.

До четвертого пункта у системы образования руки не доходили. Конечно, подобная задача иногда ставилась и решалась, но в большинстве случаев — при параллельном исполнении функций обыкновенного учебника. Акценты из-за перегрузки менялись, и намерения со второй-третьей главы начинали дрейфовать, не достигая результата. В виртуальном пространстве так бывает. Аналог объединения гантели с теннисной ракеткой перестает решать обе задачи, хотя это не сразу бросается в глаза.

«Лекции» ставят 4-й пункт своей главной целью. Сопутствующая идея — экономия слов и средств. Правда, на фоне деклараций о краткости и ясности изложения предполагаемое издание около 20 томов может показаться тяжеловесным, но это связано с обширностью математики, а не с перегрузкой деталями.

Необходимо сказать, на кого рассчитано. Ответ «на всех» выглядит наивно, но он в какой-то мере отражает суть дела. Обозримый вид, обнаженные конструкции доказательств, — такого сорта книги удобно иметь под рукой. Не секрет, что специалисты самой высокой категории тратят массу сил и времени на освоение математических секторов, лежащих за рамками собственной специализации. Здесь же ко многим проблемам предлагается короткая дорога, позволяющая быстро освоить новые области и освежить старые. Для начинающих «короткие дороги» тем более полезны, поскольку облегчают движение любыми другими путями.

В вопросе «на кого рассчитано» есть и другой аспект. На сильных или слабых? На средний вуз или физтех? Опять-таки выходит «на всех». Звучит странно, но речь не идет о регламентации кругозора. Простым языком, коротко и прозрачно описывается предмет. Из этого каждый извлечет свое и двинется дальше.

Наконец, последнее. В условиях информационного наводнения инструменты вчерашнего дня перестают работать. Не потому, что изучаемые дисциплины чересчур разрослись, а потому, что новых секторов жизни стало слишком много. И в этих условиях мало кто готов уделять много времени чему-то одному. Поэтому учить всему — надо как-то иначе. «Лекции» дают пример. Плохой ли, хороший — покажет время. Но в любом случае, это продукт нового поколения. Те же «колеса», тот же «руль», та же математическая суть — но по-другому.

Предисловие к шестнадцатому то́му

Существует достаточно света для тех, кто хочет видеть, и достаточно мрака для тех, кто не хочет.

Паскаль

Теорией множеств и основаниями математики занимаются единицы, а соприкасаются с ними — миллионы. И тут есть дефицит простой и понятной информации о путях, ведущих вглубь, — для тех, кому мало знакомства «по верхам», но нет охоты тратить силы и время на освоение аппарата, каковой потом не пригодится. Для этой аудитории и предназначен данный том.

Глава 1

Справочная

Надо так «пошевелить» определения — никто не знает как, — чтобы область «ожила».

Ниже собраны некоторые известные определения и набившие оскомину факты, каковые удобно держать в одном месте, чтобы не портить изложение отступлениями.

1.1. Теоретико-множественные операции

В пределах стандартных обозначений всегда есть люфт. Поэтому об исходных положениях необходимо договориться.

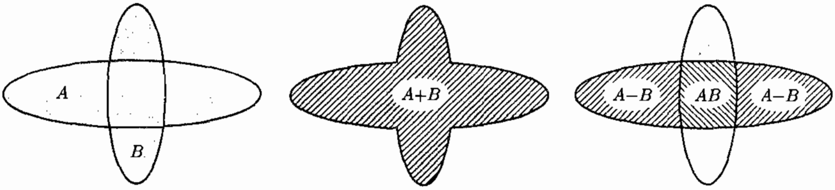
$x \in (\notin) X$ — элемент x принадлежит (не принадлежит) X. Тот же знак используется в ситуации $Z \in X$ — множество Z является элементом множества X. При этом $Z \in X$ не означает $Z \subset X$. Например, $X = \{2, 3\}$ не является элементом $Y = \{2, 3, 4\}$, но является элементом множества $\{\{2, 3\}, 3, 4\}$.

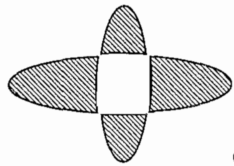
$X \cup Y$, $X \cap Y$, $X \setminus Y$ — *объединение*, *пересечение* и *разность множеств*. Используются также эквивалентные обозначения:

$$X + Y = X \cup Y, \quad X \cdot Y = X \cap Y, \quad X - Y = X \setminus Y.$$

Визуальные пояснения способствуют пониманию и запоминанию лучше [1)].

[1)] Идея *Гельвеция* насчет *знания общих принципов*, *возмещающего незнание отдельных фактов*, — в определенной степени обратима.





Симметрическая разность $A\Delta B$, состоит из элементов, которые принадлежат либо только A, либо только B. Операция Δ является *коммутативной*, *ассоциативной* и удовлетворяет следующему *дистрибутивному закону*:

$$A \cdot (B\Delta C) = (A \cdot B)\Delta(A \cdot C).$$

Любой класс множеств, замкнутый относительно симметрической разности Δ и пересечения $\cdot = \cap$, является коммутативным кольцом, в котором операции Δ и $\cap$ играют роль сложения и умножения.

Включение $X \subset Y$, «X подмножество Y», используется далее как эквивалент $X \subseteq Y$. Иначе говоря, у нас $X \subset Y$ означает $X \subseteq Y$. При необходимости оговорить *строгое включение* к $X \subset Y$ добавляется $X \neq Y$. В случае строгого включения $X \subset Y$ $(X \neq Y)$ множество X называется *собственным подмножеством* Y.

$X' = E \setminus X$ — *дополнение* множества X, определяемое как множество элементов некоторого *основного* множества E, не принадлежащих X.

$X \times Y$ обозначает *декартово произведение* множеств X и Y, т. е. множество пар элементов $\{x, y\}$, $x \in X$, $y \in Y$.

$\varnothing$ — пустое множество.

$\overline{\Omega}$ — замыкание Ω. Но «черта над» используется и в других целях, определяемых контекстом.

$\dot{\Omega} = \partial\Omega$ — граница Ω.

$2^{\Omega} = \mathcal{P}(\Omega)$ — множество всех подмножеств множества Ω.

$\mathbb{N}$ — множество натуральных чисел $\{1, 2, \ldots\}$.

$\mathbb{Z}$ — множество целых чисел $\{\ldots, -1, 0, 1, \ldots\}$.

Функция $f(x)$, преобразующая элементы множества X в элементы множества Y, обозначается как

$$f : X \to Y.$$

В случае $f(x) \equiv f_0(x)$ на $X_0 \subset X$ — функцию $f : X \to Y$ называют *продолжением* f_0 на X, а f_0 — *сужением* f на X_0.

Задание функции $f : X \to Y$ равносильно заданию ее *графика*, т. е. множества пар $\{x, y\}$, где $x \in X$, $y = f(x) \in Y$.

1.2. Алгебраические мотивы

В приложениях рассматриваемые множества являются, как правило, подмножествами некоторого основного множества E — например, сегмента $E = [0, 1]$. Однако вместо 2^E берутся чаще всего более узкие семейства подмножеств $\mathscr{E} \subset 2^E$, замкнутые относительно тех или иных теоретико-множественных операций и образующие на $\mathscr{E}$ вкупе с операциями $\{\cup, \cap, {}', \Delta\}$ какие-либо алгебраические структуры[2]. При этом определяющую роль играют свойства операций, некоторые из которых широко известны и просто устанавливаются. Например:

- *Коммутативность и ассоциативность объединения и пересечения*:

$$X + Y = Y + X, \qquad X \cdot Y = Y \cdot X;$$
$$(X + Y) + Z = X + (Y + Z), \quad (X \cdot Y) \cdot Z = X \cdot (Y \cdot Z).$$

[2] Например, систему *борелевских* или *измеримых* множеств.

- *Идемпотентные законы*:

$$X + X = X, \quad X \cdot X = X.$$

- *Дистрибутивные законы*:

$$(X + Y) \cdot Z = X \cdot Z + Y \cdot Z,$$
$$(X \cdot Y) + Z = (X + Z) \cdot (Y + Z).$$

- *Законы поглощения*:

$$X + X \cdot Y = X, \quad X \cdot (X + Y) = X.$$

- *Как правило, в $\mathscr{E}$ входят $\varnothing$ и само E*:

$$X + \varnothing = X, \quad X \cdot \varnothing = \varnothing,$$
$$X + E = E, \quad X \cdot E = X.$$

- *Свойства дополнения*:

$$X'' = X, \quad \varnothing' = E, \quad E' = \varnothing,$$
$$X + X' = E, \quad X \cdot X' = 0,$$
$$(X + Y)' = X' \cdot Y', \quad X' \cdot Y' = X' + Y' \quad (\textit{правила де Моргана}).$$

Симметрическая разность множеств,

$$X \Delta Y = (X - Y) + (Y - X) = (X + Y) - (X \cdot Y),$$

менее известна, но обладает уникальными особенностями. Тогда как операции сложения и умножения множеств необратимы, симметрическая разность обратима: уравнение $X \Delta Y = Z$ относительно X всегда имеет единственное решение $X = Y \Delta Z$. Другими словами, операция Δ имеет обратную, каковой является она сама[3].

Другие свойства Δ относительно привычны:

$$X \Delta Y = Y \Delta X \quad — \textit{коммутативность},$$

[3] С точки зрения алгебры это весьма удобное и довольно экзотическое свойство.

непосредственно вытекающая из определения; *ассоциативность* —

$$X\Delta(Y\Delta Z) = (X\Delta Y)\Delta Z,$$

устанавливаемая несколько громоздко; а также *дистрибутивность умножения* относительно Δ:

$$X \cdot (Y\Delta Z) = (X \cdot Y)\Delta(X \cdot Z).$$

Интересно что если Δ считать сложением, а $\cap$ — умножением, то их свойства совпадают со свойствами одноименных арифметических операций — в той части, которая касается определения *коммутативного кольца с единицей* [3, т. 8]. Поэтому теоретико-множественные вычисления с операциями Δ, $\cap$ — производятся так же, как в обычной арифметике, да еще с дополнительными удобствами в силу

$$X \cdot X = X, \quad X\Delta X = \varnothing.$$

А на множестве подмножеств 2^X симметрическая разность может служить групповой операцией. Группа $\{2^X, \Delta\}$ получается *абелевой* (коммутативной).

1.3. Упорядоченность и эквивалентность

На множествах вводятся, как правило, те или иные взаимоотношения между элементами: *эквивалентность*, различные виды *упорядоченности* и другие изыски, о которых речь будет идти в последующих главах.

Эквивалентность. Довольно часто используется отождествление некоторых элементов из X. Соответствующая операция — обозначаемая символом «$\sim$» — называется *эквивалентностью*, и по определению обязана быть

рефлексивной	$x \sim x$
симметричной	$x \sim y \leftrightarrow y \sim x$
транзитивной	$x \sim y, \ \ y \sim z \to x \sim z$

Перечисленные требования позволяют разбить множество X на *классы эквивалентных элементов*, совокупность которых называют *фактор-множеством*.

Другое сплошь и рядом используемое отношение на множестве X — **частичная упорядоченность**, каковой называют отношение «меньше или равно»: $\leqslant$, удовлетворяющее условиям:

рефлексивности	$x \leqslant x$
антисимметричности	$x \leqslant y, \ \ y \leqslant x \to x = y$
транзитивности	$x \leqslant y, \ \ y \leqslant z \to x \leqslant z$

При этом $x < y$ («меньше», или «строго меньше») подразумевает: $x \leqslant y$, но $x \neq y$.

• Необозримое число примеров частичной упорядоченности дает *полуупорядоченность с помощью конусов* [3, тт. 5, 15]: $x \geqslant y$ означает, что разность $x - y$ принадлежит конусу K.

• Широко распространенный вариант частичной упорядоченности: *отношение включения* $\subset$ на подмножествах некоторого множества X, а также отношение принадлежности: $X \in Y$ — множество X является элементом множества Y.

• На $\mathbb{N}$ неравенство $x \leqslant y$ иногда понимают как: y делится на x.

• Для функций из $\mathbb{N}$ в $\mathbb{N}$ неравенство $f \leqslant g$ можно понимать как $f(x) \leqslant g(x)$ для всех x за исключением их конечного числа. Проверьте, что это частичный порядок.

1.3.1. *Частичный порядок не предполагает сравнимость любых элементов. Если же любые два элемента $x, y \in X$ сравнимы, т. е. либо $x \leqslant y$, либо $y \leqslant x$, — то частичный порядок называется* ***линейным****, или просто порядком*[4].

---

[4] Таковы любые числовые множества с обычным отношением порядка.

• Широко распространен ***лексикографический порядок*** на упорядоченных наборах[5] $\{x_1, \dots, x_n\}$ элементов x_i линейно упорядоченного множества X:

$$\{x_1, \dots, x_n\} < \{y_1, \dots, y_n\}$$

означает, что при некотором i

$$x_i < y_i \quad \text{и} \quad x_j = y_j \quad \text{для всех} \quad j \leqslant i,$$

соотношение между x_j и y_j для $j > i$ — роли не играет. Порядок, очевидно, линеен[6].

1.3.2. *Элемент $z \in X$ частично упорядоченного множества X называют* ***наибольшим****, если он больше любого другого элемента $x \in X$, и* ***максимальным***[7]*, если не существует бо́льшего элемента в X.*

(!) *Наибольший элемент*, если существует, является обязательно единственным. *Максимальных элементов* может быть много, например, *оптимальных по Парето* [3, т. 7]. В случае линейного порядка понятия *наибольшего* и *максимального* элементов совпадают.

• Максимальные элементы несравнимы между собой. **(?)**

1.3.3. ***Полная упорядоченность****: Упорядоченное множество называется* ***вполне упорядоченным****, если каждое его непустое подмножество имеет наименьший элемент.*

• Натуральный ряд при естественном порядке элементов,

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

вполне упорядочен, но то же множество в случае задания порядка

$$\{\dots, n, \dots, 2, 1\}$$

уже не вполне упорядочено.

---

[5] На словах из некоторого алфавита.

[6] В данном случае мы вынуждены были говорить о разных порядках (между элементами и между наборами элементов), но пользовались одним и тем же знаком $<$, полагаясь на контекст и избегая усложнения обозначений типа $x <_1 y$, $u <_2 v$. Контекст и далее ставится во главу угла.

[7] Аналогично определяются ***наименьший*** и ***минимальный*** элементы.

1.3.4. Теорема. *Во вполне упорядоченном множестве не может быть бесконечных строго убывающих последовательностей.* **(!)**

◄ Допустим противное,

$$\ldots < x_2 < x_1 < x_0 \quad \text{и все} \quad x_i \in X.$$

Но тогда в силу полной упорядоченности X множество $\{x_1, x_2, \ldots\}$ обязано иметь наименьший элемент x_j, что дает противоречие. ►

1.3.5. *Всякий элемент x вполне упорядоченного множества*[8] *имеет непосредственно следующий за ним элемент z, но не всегда — предыдущий*[9]*. Как правило, используется обозначение $z = x + 1$.*

◄ Минимальный элемент в множестве $\{y : y > x\}$ является искомым. ►

1.3.6. *Ограниченное сверху подмножество вполне упорядоченного множества имеет точную верхнюю грань.*

◄ Таковой служит наименьшая среди верхних границ. ►

1.4. Логические инструменты

Некоторое представление о матлогике дает глава 7 (см. также [3, т. 6]), за пределами которой роль логических приспособлений незначительна, но кое-что нет-нет да и просачивается. Поэтому, для удобства, напомним азы, в несколько упрощенном виде.

Исходным материалом *двузначной логики* являются переменные $x, y, z \ldots$, принимающие одно из двух значений: $\{1, 0\}$ либо

[8] Кроме наибольшего, если таковой имеется.

[9] Элементы, не имеющие предыдущего, называются *предельными*.

{*истина* (И), *ложь* (Л)}. На уровне «первичности» находятся также *логические связки*:

$$\neg\ (\textit{отрицание «не»}), \quad \vee\ (\textit{или}), \quad \wedge\ (\textit{и}), \quad \to\ (\textit{следует}), \tag{1.1}$$

которые являются функциями, принимающими, как и аргументы, одно из двух значений, 0 или 1. Запоминанию смысла $\vee$, $\wedge$ помогает их сходство по очертаниям со знаками $\cup$, $\cap$, значение которых крепче сидит в подкорке. Для *отрицания* наряду с $\neg$ используется также «черта сверху».

Двуместную функцию $x \vee y$ («x *или* y или го и другое вместе») называют *дизъюнкцией*[10]; $x \wedge y$ («x *и* y»)[11] — *конъюнкцией. Импликация* $x \to y$ («*из* x *следует* y») не вполне соответствует обыденному пониманию «если x, то y». Как функция двух переменных $x \to y$ всюду принимает значение 1 за исключением случая $x = 1$, $y = 0$, где $x \to y$ равна 0. Другими словами, из «истины» не может следовать «ложь», все остальное — возможно.

Как в арифметике с помощью умножения и сложения выписываются сложные формулы, так и в логике комбинации связок позволяют задавать n-местные *логические формулы* $\varphi(x_1, \ldots, x_n)$, каковые могут включать в себя *кванторы общности* $\forall\ x$ — «для всех x», и *кванторы существования* $\exists\ x$ — «существует x». В предметных областях логический язык расширяется добавлением в алфавит *констант языка*, а также *функциональных* и *предикатных символов*[12], — объединяемых в *сигнатуру*, о которой, собственно, и говорят при упоминании языка. Язык теории групп, например, $L = \{\times,\ ^{-1},\ e\}$ включает бинарную «$\times$» и унарную операцию «$^{-1}$», а также константу «e» — «единицу группы». Логическая часть языка умалчивается как автоматически подразумеваемая операционная среда. К логической епархии относят и знак равенства. Но жесткого регламента нет. В качестве *языка примитивной арифметики* упоминают, как правило, $L_0 = \{+,\ \times,\ =,\ \exists\}$, подчеркивая ограниченный характер использования логики[13].

---

[10] Иначе говоря, *дизъюнкция* — это функция двух переменных, равная 1, если хотя бы одна переменная равна 1, и равная 0 в противном случае.

[11] *Конъюнкция* $x \wedge y$ равна 1, если $x = y = 1$, и — нулю в противном случае.

[12] С указанием их «n-арности», «n-местности».

[13] Разрешено употребление $\exists$, но не $\forall$ и $\neg$.

Таким образом, язык представляет собой *алфавит*[14] (набор символов) с «орфографией», каковая сводится к регламентации построения формул. *Правильно построенные формулы* (*ппф*) характеризуются соблюдением нескольких правил. Разрешаются равенства, $x = y$, $a = b$, n-местные отношения записываются в виде[15] $R(x_1, \dots, x_n)$, наконец, если A и B *пэпэфы*, то и

$$\neg A, \quad A \vee B, \quad A \wedge B, \quad A \to B, \quad \forall\, xA, \quad \exists\, xA$$

являются *пэпэфами*. Регламентированная запись функций и отношений (*предикатов*) на практике обычно либерализуется — вместо $+(x, y)$ или $< (x, y)$ пишут $x + y$, $x < y$.

Переменные в формуле типа $\forall\, x_3\ \exists\, x_7 \varphi(x_1, \dots, x_n)$, находящиеся под действием кванторов, называются *связанными*, остальные — *свободными*. Формулы, у которых все переменные *связаны*, считаются *замкнутыми* и называются *предложениями*, или *суждениями*.

• Константы и переменные называют *термами*. Если $t_1, \dots, t_n$ *термы*, а f — n-местная функция, то $f(t_1, \dots, t_n)$ — также *терм*. Иначе говоря, *термы* — это имена.

• Многоместные отношения $R(x_1, \dots, x_n)$ — это *предикаты*, R — *предикатный символ*. Примеры предикатов:

$$x_1 > x_2, \quad x_1 = \ln x_2, \quad x_1 + x_2 = x_3,$$

откуда видна, кстати, относительность понятий *предиката* и *функции*. Описание функции с помощью графика делает ее предикатом, а переход к характеристическим функциям отношений делает предикаты функциями. Во многих случаях предикатами удобнее считать именно *«характеристические функции отношений»*, чтобы не перегружать описания *оценками истинности*, т. е. не рассматривать одновременно и отношения, и их характеристические функции.

[14] Который помимо сигнатуры и логических обозначений может включать те или иные скобки и другие знаки для визуального удобства.

[15] Например, $R_{17}(a, b, c)$ может обозначать $a^b = c$.

Исчисление высказываний (ИВ) изучает функции $\varphi(p_1, \ldots, p_n)$, где переменные, как и сами функции, принимают одно из двух значений $\{1, 0\}$, равносильно: {*истина* (И), *ложь* (Л)}. За переменными, называемыми *пропозициональными*, стоят высказывания, в том числе в виде *отношений* (*предикатов*) типа $x > 2$, $x^y = z$, «x — простое число» и т. д. Характеристические функции этих отношений будут как раз *пропозициональными* переменными $p_1, \ldots, p_n, \ldots$, принимающими значения из $\{0, 1\}$. Пропозициональные переменные объединяются друг с другом с помощью логических связок[16] (1.1) в *формулы*, которыми выражается любая булева функция $\varphi : \{1, 0\}^n \to \{1, 0\}$, см. [3, т. 6].

1.4.1. *Множество формул Θ называется* ***совместным****, если при некоторых значениях переменных все формулы из Θ истинны. В случае одной формулы говорят о* ***выполнимости****, но о выполнимости говорят и в случае многих формул, подразумевая одновременную выполнимость.*

1.4.2. *Формула φ называется* ***тавтологией****, если при всех значениях переменных она истинна. Примеры тавтологий:*

$$\neg(p \vee q) \to (\neg p \wedge \neg q), \qquad (p \wedge q) \to q.$$

1.4.3. Выводом *в ИВ называется конечная последовательность формул, каждая из которых является либо аксиомой из* ***правил вывода***[17]*, либо формулой, получаемой из предыдущих в результате применения модус поненс. Последняя в такой последовательности формула называется* ***теоремой****.*

Исчисление предикатов (ИП) характеризуется допуском к использованию кванторов $\forall$, $\exists$ в *логике первого порядка*, где $\forall$ и $\exists$ всегда действуют на некотором данном множестве[18]. Рассматри-

[16] При этом последовательность выполнения операций определяется расстановкой скобок, что существенно.

[17] См. раздел 7 4.

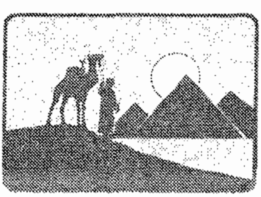
[18] Логики же более высоких порядков разрешают кванторам действовать на подмножествах X и на многоместных функциях, а также использовать кванторы по множествам функций и т. д. Подробное описание громоздко, да и здесь не к месту.

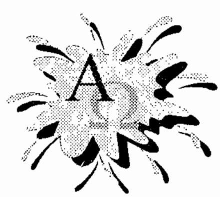
ваемые формулы предполагаются *правильно построенными* (*ппф*) и *замкнутыми* (находящимися под действием кванторов). Но замкнутыми только по переменным. Функциональные и предикатные символы остаются свободными, поскольку кванторам в *логике первого порядка* не разрешается действовать по функциям и предикатам. Поэтому формулы могут быть истинными или ложными в зависимости от интерпретации, в результате возникает понятие *общезначимой формулы*, о чем подробно сказано в разделе 7.4.

Стоит обратить внимание, что логика развивается двумя параллельными путями, *семантическим* и *синтаксическим*. В семантической колее символы обозначают реальные операции («или», «не», «для всех») и объекты (числа, множества). Синтаксическое рассмотрение предмета убирает какую бы то ни было интерпретацию. Знаки

$$\forall,\ \exists,\ \vee,\ \subset,\ \times,\ -$$

превращаются в буквы, за которыми нет никакого смыслового содержания. Поэтому действия, базировавшиеся в семантическом русле на понимании свойств операций, теперь должны регулироваться новыми механизмами, каковыми являются различные *правила вывода* и *аксиомы*, которые по указанной причине стараются записывать в строго регламентированной форме.





Глава 2

Кантор и бесконечность

Don't miss the boat!

Кое-кто думает, что «пенки уже сняты» и настало время мемуаров. Но с чем было связано теоретико-множественное потрясение XIX века? С неготовностью? Недопониманием? Или с приоткрытием спрятанной картины — мелькнувшей и ушедшей в подсознание. Завершилась ли та история? По-видимому, все только начинается.

Рисунок А. Фоменко

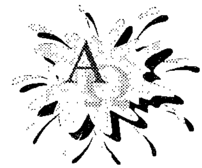
2.1. Откуда берутся множества

Еще раз о главном. Множества не бывают даны сами по себе [1], а появляются в результате конструирования с помощью предположений и постулатов. Изначально, конечно, от чего-то надо оттолкнуться, но потом идет чистое комбинирование. Поэтому, если не скользить по поверхности, то основное внимание надо уделять инструментам, каковые могут не обеспечивать требуемые свойства конечного продукта и даже вступать в противоречие друг с другом, явно или замаскированно.

Обратимся к примерам, не акцентируя пока внимания на инструментальной подоплеке.

[1] Хотя такая иллюзия иногда возникает.

1. Конечные множества, на первый взгляд, не вызывают затруднений. Но только на первый. Относительно беспроблемный вариант — перечислительный. Типа $S = \{1, 8, 3, 12\}$ или

$S = \Big\{$  ,  ,  $\Big\}$.

Но для формирования S обычно допускается *инструмент неявного задания*. Типа декларации свойств либо роли элементов S в каких-либо посторонних задачах, — все это с точки зрения житейской логики определяет S. Но как быть с конечным множеством S целочисленных решений некоторого «коварного» [3, т. 6] полиномиального уравнения

$$P(x) = 0,$$

где *принципиально* нет возможности ответить на вопрос о числе элементов S, и даже о пустоте S. Или как быть с множеством

$$S = \{R(4,6),\ R(5,6)\}, \quad R(k,l) \text{— \textit{числа Рамсея} [3, т. 10]},$$

состоящим всего из двух элементов, но для вычисления небольших чисел[2] $R(4,6)$, $R(5,6)$ не хватает вычислительных возможностей всей цивилизации, и никто не знает, из чего состоит множество S, ни дна ему ни покрышки.

2. Счетные множества охватывают натуральный ряд

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

и множества ему *эквивалентные*. Это шаг в бесконечность, влекущий за собой фундаментальные последствия.

2.1.1. Определение. *Множества X, Y считаются эквивалентными (равномощными), пишут $X \sim Y$, если между их элементами можно установить взаимно однозначное соответствие. Класс экви-*

[2] Известны оценки $35 \leqslant R(4,6) \leqslant 41$, $58 \leqslant R(5,6) \leqslant 87$.

валентности множества X называют его ***мощностью****, или* ***кардинальным числом****, и обозначают как* $|X|$.

Таким образом, множества, эквивалентные натуральному ряду, *счетны*. Стандартные фокусы «подключения» множеств к натуральному ряду хорошо известны.

Совокупности

$$1, 2, 3, \ 4, \ldots, n, \ldots$$

$$1, 4, 9, 16, \ldots, n^2, \ldots$$

эквивалентны в силу взаимно однозначного соответствия $\begin{matrix} n \\ \updownarrow \\ n^2 \end{matrix}$.

Множество целых чисел $\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$ счетно, ибо легко перечисляется после переформатирования:

$$\mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\}.$$

Двухиндексные множества $\{a_{ij}\}$ счетны, поскольку располагаются в виде бесконечной квадратной таблицы и нумеруются вдоль стрелочек,

$$\begin{pmatrix} a_{11} & \to & a_{12} & & a_{13} & \to & a_{14} & \cdots \\ & \swarrow & & \nearrow & & \swarrow & & \\ a_{21} & & a_{22} & & a_{23} & & a_{24} & \cdots \\ \downarrow & \nearrow & & \swarrow & & & & \\ a_{31} & & a_{32} & & a_{33} & & a_{34} & \cdots \\ & \swarrow & & & & & & \\ a_{41} & & a_{42} & & a_{43} & & a_{44} & \cdots \\ \downarrow & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{pmatrix}, \qquad (2.1)$$

в результате чего достигается взаимно однозначное соответствие с $\mathbb{N}$. Отсюда заодно ясно, что *счетная совокупность счетных множеств*[3] *— также счетное множество*[4]. Аналогичный трюк

[3] Например, строчек в таблице.

[4] Но тут не так все просто, см. доказательство утверждения 4.1.6.

работает при перечислении рациональных чисел[5] p/q, ра́вно как и при «усмирении» многоиндексных множеств.

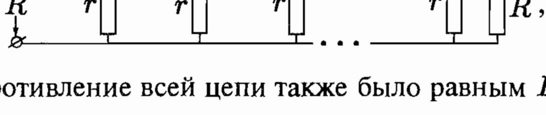
Счетная бесконечность при неаккуратном с ней обращении ведет к неприятностям[6]. Предусмотрительная позиция, казалось бы, должна состоять в интерпретации бесконечных множеств как *сколь угодно наращиваемых*. Типа ленты *машины Тьюринга* [3, т. 6]. Но теория множеств рассматривает бесконечность как **данность, состоявшийся факт** — и это порождает определенную головную боль. Счетное множество

$$S = \{s_1, s_2, \ldots s_n, \ldots\} \tag{2.2}$$

рассматривается не как разворачивающийся процесс, а как фактически существующая совокупность[7]. Эмоционально этому содействуют различные имиджевые конструкции. Например, отрезок $[0, 1]$ содержит все дроби p/q, $p < q$, — они уже тут, их не надо добавлять одну за другой. Но не надо забывать, что визуальный образ $[0, 1]$ — из другой геометрической реальности.

Как бы там ни было, но феномен осуществленной бесконечности чрезвычайно важен. Надлежащее понятие беспрестанно и эффективно работает во всех уголках виртуального мира. Особенно ярко это проявляется в математическом анализе.

Вот маленький пример из другой оперы. Необходимо так подобрать правое сопротивление R в электрической цепи .



(2.3)

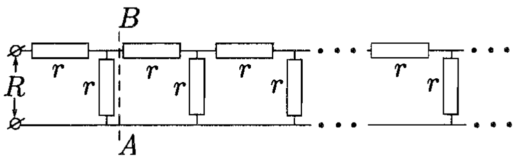
чтобы сопротивление всей цепи также было равным R.

[5] С поправкой на сократимость дробей. Ранее встречавшиеся числа $a_{pq} = p/q$ пропускаются.

[6] См., например, [3, тт. 1, 5, 6, 10, 12], а также [2].

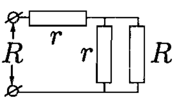
[7] При этом обычно говорят об *актуальной бесконечности*, что лингвистически абсурдно, и возникло, надо полагать, в результате неудачного перевода английского «actual», пребывающего в «ложных друзьях переводчика».

При большом числе звеньев решение задачи в лоб — весьма трудоемко. Выход из положения: заменяем правое R всей цепью (2.3), сопротивление которой по условию равно как раз R. В полученной цепи с удвоенным числом звеньев снова заменяем правое R всей цепью (2.3) и т. д. В результате получается бесконечная цепь[8)]



. (2.4)

Определение сопротивления цепи (2.4) представляется еще более сложной задачей, но тут как раз срабатывает состоявшаяся бесконечность. Цепь справа от сечения AB равносильна самой цепи (2.4). Но тогда исходная задача равносильна определению R в задаче



$$R = r + \frac{rR}{r+R} \quad \Rightarrow \quad R = \frac{1+\sqrt{5}}{2}r.$$

Континуум. Переход к рассмотрению действительных чисел

$$0{,}\alpha_1\alpha_2\ldots = \alpha_1 10^{-1} + \alpha_2 10^{-2} + \ldots \quad \text{на} \quad [0,1]$$

сталкивается с новым явлением. Множество таких чисел (*континуум*) оказывается *несчетным*. В предположении противного их можно было бы расположить в виде таблицы

$$\begin{array}{l} a_1 = 0,\ \alpha_{11}\ \alpha_{12}\ \alpha_{13}\ldots \\ a_2 = 0,\ \alpha_{21}\ \alpha_{22}\ \alpha_{23}\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots, \end{array} \tag{2.5}$$

но тогда любое число b с десятичной записью

$$b = 0{,}\beta_1\beta_2\ldots$$

8) По мере увеличения числа звеньев роль правого R стремится к нулю.

при условии $\beta_j \neq \alpha_{jj}$ для всех j — не входит в список (2.5), что дает противоречие[9].

Георг Кантор (1845–1918), возрастная динамика

Перечисленное уже позволяет обратить внимание на принципиальные трудности, которые могут препятствовать формированию непротиворечивой теории.

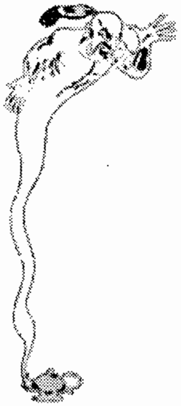
1) Благословив способы неявного задания множеств, мы не можем исключить малопривлекательные ситуации, в которых невозможно ответить на простейшие вопросы:

$$X = \varnothing? \quad X = Y? \quad X \subset Y? \quad X \cap Y \neq \varnothing?$$

Но запретить неявное описание X, Y — тоже плохо, иначе рухнет половина математики. И вопрос немыслимо решить раз и навсегда во всех контекстах. Приходится вечно лавировать.

2) Массу проблем порождает бесконечность. В упомянутых выше примерах счетных множеств соответствие с натуральным рядом (перечисление) было конструктивным. А может ли быть так, что необходимое соответствие есть, но его принципиально нельзя указать? Оказывается, да. Счетны: множество *общерекурсивных функций* [3, т. 6], множество истинных арифметических теорем, — но они неперечислимы (глава 6).

[9] Такой способ построения числа b называют *диагональным*. Чтобы обойти стороной проблему неоднозначной записи десятичной дроби, достаточно выбирать β_j не равными 0 и 9.



Как тогда быть? Принимая повышенные меры безопасности, мы сужаем полет мысли до сферы конструктивной математики, где почва уходит из-под ног. Ни равенство $a = b$, ни отношение $a < b$, — для конструктивных чисел в общем случае оказываются непроверяемы, а монотонная и ограниченная *последовательность Шпеккера* не сходится [3, т. 6]. В таких условиях конструктивностью приходится жертвовать, выпуская на волю джинна противоречий, — и тогда коромысло весов срывается в другую крайность. *Парадокс Банаха—Тарского*, разрывные линейные функции и другая чертовщина (глава 4) начинают подрывать психическое здоровье отзывчивой части населения.

3) Довольно много осложнений вертится вокруг континуума. Первым делом обращает внимание на себя тот факт, что иметь дело с бесконечными рядами

$$0{,}\alpha_1\alpha_2\ldots = \sum_{k=1}^{\infty} \frac{\alpha_k}{10^k}$$

в качестве элементов не только неудобно, но и проблематично, поскольку хотелось бы иметь дело с числами, которые можно складывать и умножать. Всмотревшись, приходится начинать не с суммирования рядов[10)], а с *сечений Дедекинда* (п. 10.1), выстраивая специальную теорию и не вполне осознавая поначалу, что, собственно, происходит. «Не вполне осознавая», потому что картина проясняется лишь тогда, когда нечто подобное делается совсем в других обстоятельствах. Когда пополняются, например, функциональные пространства. Или когда множество $\mathbb{Q}$ рациональных чисел пополняется в *p-адической норме*[11)], в результате

[10)] Каковое в отсутствие действительных чисел не имеет опоры.

[11)] Ремарка из [3, т. 14]: *в принципе работает обычная схема пополнения, но чучело итогового полного пространства $\mathbb{Q}_p$ совсем не напоминает $\mathbb{R}$. Конечно, есть норма, а значит, есть метрика, топология, непрерывность, — но нет покоя. Все по-другому... Где они эти $\mathbb{Q}_p$? Хотелось бы расположить их на вещественной прямой, но не тут-то было.*

чего становится ясно, что геометрический образ континуума $[0, 1]$ не более чем случайная декорация.

Еще одна популярная заноза — *парадокс Сколема* (п. 7.9). Парадокса, собственно, нет. Идея надуманного противоречия выглядит примерно так. Континуум получается тасованием счетного множества аксиом и правил — и потому счетен. Идея базируется на теореме *Лёвенгейма—Сколема*: «*Если счетная теория имеет модель, то она имеет также счетную модель*». Такие формулировки гипнотизируют. В итоге появляются перлы типа: соответствие $[0, 1]$ и $\mathbb{N}$ лежит в метатеории, где $[0, 1]$ можно «пересчитать». Конечно, оно так и есть, если думать о розыгрыше населения. Континуум является *счетной конструкцией*. Именно поэтому с ним можно работать, получая выводы за конечное число шагов. Другое дело вес, мощность конструируемой бесконечности. Тут уже зависит от аксиоматики. Рассматривается множество всех подмножеств $\mathbb{N}$, что в теории множеств допускается, — и несчетная совокупность готова. Тогда как сие «множество всех подмножеств» в принципе невозможно алгоритмически породить, даже как потенциальную субстанцию.

2.2. Феномен мощности

Всяк ныне знает, что теорию множеств создал *Георг Кантор*[12]. Связанная с этим революция и ее последствия подтверждают известный тезис «истина рождается как ересь и умирает как банальность». Главные идеи сегодня легко объяснить школьнику[13]. А «тогда» невозможно было объяснить никому. Интуиция противилась. Сейчас-то болезнь укоренилась, недоумение иссякло.

Теория развивалась в основном вокруг понятия *мощности*, — определение 2.1.1. Множества, между элементами которых можно установить взаимно однозначное соответствие, группируются в

[12] Родился 3 марта 1845 года в *России* (*Санкт-Петербург*), умер 6 июня 1918 года в *Германии*.

[13] Конечно, если не заострять. Что верно, надо признать, по любому поводу. В этом Мире ничего нельзя объяснить исчерпывающе. Как только начинаешь «всматриваться», объект расползается.

классы «равномощных» множеств. Конечные множества совпадают по мощности, если имеют одинаковое число элементов. С бесконечными множествами ситуация сложнее, но идеологически — вроде прозрачная. Тем не менее уже первые шаги обнаруживают разломы в миропонимании.

Особенно болезненной была историческая попытка установить, что отрезок $[0, 1]$ и квадрат $[0, 1] \times [0, 1]$ имеют разные *мощности*[14]. Оказалось — одинаковые.

◄ Точки квадрата $[0, 1] \times [0, 1]$ с координатами

$$x = 0{,}\alpha_1\alpha_2\ldots, \quad y = 0{,}\beta_1\beta_2\ldots \tag{2.6}$$

сопоставляются точкам отрезка $[0, 1]$

$$z = 0{,}\alpha_1\beta_1\alpha_2\beta_2\ldots\,. \;► \tag{2.7}$$

Вот, собственно, и все доказательство[15]. Но на эти две строчки (2.6), (2.7) у *Кантора* ушло *три года* (!), а круги по воде расходились еще дольше. При этом *Дедекинд* постепенно превратился в сторонника, а *Кронекер* канторовские построения воспринимал в штыки до конца жизни. Все это бывает интересно переварить заново. Даже не для того чтобы лучше почувствовать теорию множеств, а чтобы ощутить феномен столкновения нового со старым, привычного с непривычным, — что происходит ежесекундно в других сферах, но не всегда так показательно.

Кронекер
(1823–1891)

Дедекинд
(1831–1916)

[14] См. определение 2.1.1.

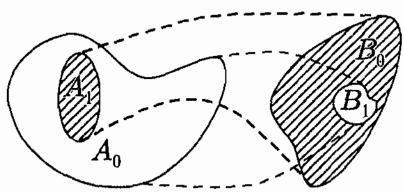
[15] Не считая мелких уточнений в связи с неоднозначностью десятичной записи чисел, см. далее.

Уже из простейшего (правда, шокирующего) примера (2.6), (2.7) видно, что устанавливать взаимно однозначное соответствие голыми руками бывает неудобно. Как во всяком деле, нужны вспомогательные инструменты. Иначе на пустяки уходит уйма энергии. В частности, указанное соответствие (2.7), строго говоря, взаимно однозначным не является из-за неоднозначной записи некоторых чисел типа $0{,}35999\ldots = 0{,}36000\ldots$ Обычно предпочтение отдается варианту с бесконечным числом нулей, но и это не спасает. Разные точки отрезка, например,

$$0{,}11; \quad 0{,}100909090\ldots; \quad 0{,}01909090\ldots,$$

переходят в одну и ту же точку квадрата $\{0{,}1;\, 0{,}1\}$. Взаимная однозначность легко достигается с помощью нижеследующей *теоремы Кантора—Бернштейна*.

2.2.1. Теорема. *Если A_0 равномощно подмножеству $B_1 \subset B_0$, а B_0 — подмножеству $A_1 \subset A_0$, то A_0 и B_0 — равномощны.*



Это удобный и эффективный инструмент, избавляющий от необходимости тратить силы на преодоление не относящихся к делу препятствий. Например, выше малой кровью достигнуто соответствие между квадратом и *частью* отрезка $[0, 1]$. Равномощность $[0, 1]$ подмножеству квадрата тем более очевидна. Теперь из факта 2.2.1 следует равномощность $[0, 1]$ и $[0, 1] \times [0, 1]$, и необходимость в указании конкретного соответствия отпадает.

◄ Теорема 2.2.1 вытекает из следующего результата, имеющего также самостоятельное значение.

2.2.2. Лемма. *Если $A_2 \subset A_1 \subset A_0$ и множества A_2 и A_0 равномощны, то все три множества равномощны.*

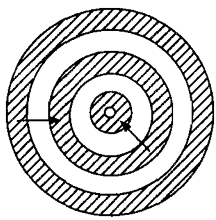
◀ Если $f : A_0 \to A_2$ взаимно однозначное преобразование, то, как легко видеть, $A_4 \subset A_3 \subset A_2 \subset A_1 \subset A_0$, где $A_3 = f(A_1)$, $A_4 = f(A_2)$. Продолжая индуктивный процесс $A_{k+2} = f(A_k)$, получаем цепочку

$$A_0 \supset A_1 \supset A_2 \supset A_3 \supset \dots .$$

Взаимно однозначное соответствие A_0 и A_1 обеспечивает преобразование

$$\psi(x) = \begin{cases} f(x), & \text{если} \quad x \in A_{2k} \setminus A_{2k+1}, \\ x, & \text{если} \quad x \in A_{2k+1} \setminus A_{2k+2} \quad \text{или} \quad x \in \bigcap\limits_k^{\infty} A_k, \end{cases}$$

при котором, символически рассуждая, каждый заштрихованный слой $A_{2k} \setminus A_{2k+1}$



переходит в следующий заштрихованный, а все незаштрихованные слои — остаются на месте. ▶

Вернемся теперь к теореме 2.2.1. Если

$$f : A_0 \to B_1 \quad \text{и} \quad g : B_0 \to A_1$$

соответствующие взаимно однозначные отображения, то gf устанавливает равномощность A_0 и $A_2 = g(f(A_0))$, и в цепочке $A_2 \subset A_1 \subset A_0$ остается доказать равномощность A_0 и $A_1 \sim B_0$, — что берет на себя лемма 2.2.2. ▶

2.3. Канторово множество и гипотеза континуума

Когда в поле зрения одновременно попадают $\mathbb{N}$ и $[0, 1]$, возникает вопрос о существовании множества, промежуточного по мощности. В поисках такого множества естественной выглядит попытка надлежащего усечения сегмента $[0, 1]$. Широкую известность получило *канторово множество* C, получаемое последовательным выбрасыванием третей из $[0, 1]$. Сначала отрезок $[0, 1]$ делится на три равные части, и средняя часть (*интервал*) удаляется. С каждой из оставшихся частей повторяется аналогичная операция — и так до бесконечности. В пределе от $[0, 1]$ почти ничего не остается, что и называется *канторовым множеством* C. Длина выброшенных третей равна

$$\frac{1}{3}\left(1+\frac{2}{3}+\left(\frac{2}{3}\right)^2+\ldots\right)=1,$$

т. е. «вся длина» выбрасывается, но C оказывается *равномощно континууму*, что опять-таки впечатляет.

◄ Концы выбрасываемых интервалов остаются в C, и называются точками *первого рода*. Их совокупность счетна, и они не исчерпывают C. Остальные точки в C называют *точками второго рода*, и, как нетрудно сообразить, это числа, в троичной записи которых не встречается единица, т. е. числа вида

$$\sum_{k=1}^{\infty}\frac{a_k}{3^k},$$

где a_k принимают значения 0 или 2. Последовательностей же $a_1, a_2, \ldots$, где a_k могут принимать два разных значения, как при двоичной записи числа, — несчетное количество. ►

В результате многих безуспешных попыток *Кантор* пришел к убеждению в справедливости следующего утверждения.

2.3.1. Гипотеза континуума (ГК). *Не существует множества, промежуточного по мощности между* $\mathbb{N}$ *и* $[0, 1]$, *т. е. вслед за счетным множеством сразу идет континуум.*

На решение проблемы ушла сотня лет. Итог оказался неожиданным. Выяснилось, что гипотезу с равным успехом можно принять или отвергнуть как аксиому.

Канторова лестница. Канторово множество служит источником построения многих аномалий. Пусть, например, функция

$$f:[0, 1]\to[0, 1]$$

на *замыкании* каждого выбрасываемого (в процессе построения канторова множества) интервала — принимает значение, равное середине этого интервала. Доопределение $f(x)$ в точках второго рода по непрерывности [16] дает *непрерывную* [17] *монотонную* функцию $f(x)$, *производная* которой *почти всюду равна нулю*, — тем не менее $f(0) = 0$, $f(1) = 1$. Другими словами, $f(x)$ почти нигде на $[0, 1]$ не растет, но успевает ощутимо вырасти на множестве нулевой меры. В результате

$$\int_0^1 f'(x)\,dx = 0,$$

но не

$$\int_0^1 f'(x)\,dx = f(1) - f(0) = 1.$$

2.4. Манипулирование бесконечностями

Отрезок $[0, 1]$ и другие числовые образования типа $[0, 1] \times [0, 1]$ упоминаются пока авансом, поскольку иррациональные числа надо сначала построить [18], что принципиально, хотя обычно недооценивается [19]. Поэтому об идеях *Кантора* более естественно говорить поначалу на «довещественно-числовом» уровне.

Вместо последовательности чисел (2.5) можно рассматривать последовательность последовательностей

$$\begin{array}{cccc} \alpha_{11}, & \alpha_{12}, & \alpha_{13}, & \dots \\ \alpha_{21}, & \alpha_{22}, & \alpha_{23}, & \dots \\ \multicolumn{4}{c}{\dots\dots\dots\dots\dots\dots,} \end{array} \tag{2.8}$$

[16] В точках второго рода $\tilde{x}$ полагается $f(\tilde{x}) = \lim f(x_k)$, где $x_k \to \tilde{x}$ и все x_k — точки первого рода.

[17] А значит, и равномерно непрерывную.

[18] См. раздел 10.1.

[19] Построить необходимо даже рациональные числа.

где α_{ij} принимают всевозможные значения из некоторого алфавита $\mathbb{A}$, и тогда $\beta_1, \beta_2, \ldots$, при условии $\forall\, j : \beta_j \neq \alpha_{jj}$ — не входит в список (2.8), откуда следует *несчетность всевозможных последовательностей* $A_i = \{\alpha_{ij}\}$, разумеется, если в алфавите $\mathbb{A}$ не менее двух символов[20].

2.4.1. Теорема. *Любое подмножество Y счетного множества X либо конечно, либо счетно.*

◄ Удалим из $X = \{x_1, x_2, \ldots\}$ те x_i, которые не принадлежат Y, сохраняя порядок остающихся. Все. ►

2.4.2. *Множество* ***конечных*** *подмножеств натурального ряда счетно.*

◄ Пусть p_r обозначает r-е простое число. Всякому подмножеству

$$\{n_1, \ldots, n_k\} \subset \mathbb{N}$$

поставим в соответствие натуральное число $p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}$. ►

2.4.3. *Множество* ***всех*** *подмножеств натурального ряда несчетно.*

◄ В предположении противного все подмножества $\mathbb{N}$ можно перенумеровать, $S_1, S_2, \ldots, S_k, \ldots$, и пусть D обозначает множество таких j, что $j \notin S_j$. В силу $D \subset \mathbb{N}$ множество D обязано совпадать с некоторым S_m. Но тогда, если $m \notin S_m$, то $m \in D$, т. е. $m \in S_m$. Если же $m \in S_m$, то $m \notin D$, т. е. $m \notin S_m$. В любом случае — противоречие. ►

Вот еще несколько стандартных фактов, на которые можно смотреть как на задачи для обозрения или как на упражнения для разминки.

2.4.4. *Декартово произведение конечного числа счетных множеств счетно.*

2.4.5. *Мощность бесконечного множества не меняется при добавлении к нему счетного или конечного множества.*

[20] При этом числовая специфика — типа неоднозначной записи чисел — не мешает видеть главное.

2.4.6. *Мощность несчетного множества не меняется при удалении из него счетного или конечного множества.*

2.4.7. *Декартово произведение счетной совокупности счетных*[21] *множеств имеет мощность континуума.*

2.4.8. *Декартово произведение конечной или счетной совокупности множеств мощности континуума имеет мощность континуума.*

2.4.9. Теорема Кантора. *Мощность множества 2^X всех подмножеств множества X строго больше мощности самого X.*

◄ Очевидно, $|2^X| \geqslant |X|$, и надо лишь исключить равенство. Пусть

$$f : X \to 2^X$$

— взаимно однозначное соответствие между X и 2^X. Тогда получается противоречие, потому что множество

$$Y = \{x \in X : x \notin f(x)\} \subset 2^X$$

не имеет прообраза. Действительно, если предположить $Y = f(y)$, то либо

$$y \in Y \to y \notin f(y) = Y,$$

либо

$$y \notin Y = f(y) \to y \in Y. \ ►$$

Мощность конечного множества из n элементов полагается равной n. *Мощность счетного множества* обозначается как $\aleph_0$ — читается «*алеф нуль*». Из п. 2.4.9 вытекает существование бесконечной цепочки возрастающих мощностей

$$\aleph_0, 2^{\aleph_0}, 2^{2^{\aleph_0}}, \dots . \qquad (2.9)$$

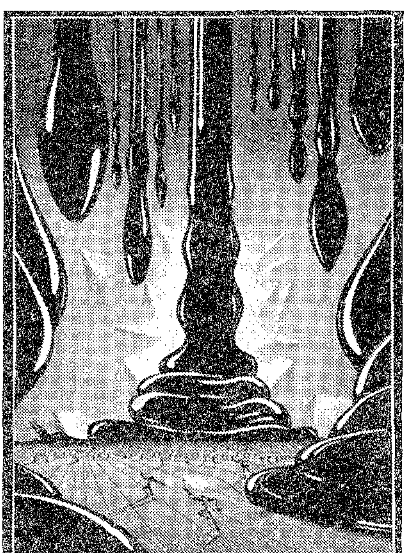
Существуют ли мощности в промежутках между элементами (2.9) — нерешенный вопрос.

[21] Или конечных, но содержащих не менее двух элементов каждое.

2.5. Реализованная бесконечность

Бесконечна ли Вселенная, и если — да, то как это может быть. А если — нет, то что там за пределами? Испепеляющее жжение этого вопроса шокирует в раннем возрасте, когда проблемы Поднебесной воспринимаются нутром, а не умом. Потом пронизывающий зов бесконечности мало-помалу глохнет под напором ухищрений, спасительных для психического здоровья. И, обжигаясь о реальность, человек бежит в придуманный мир ментальных условностей.

Но хорошо спрятаться от проблемы все равно не удается. В мире идей бесконечность является в другом облике. В каком смысле существует натуральный ряд $\mathbb{N}$? Как разворачивающийся процесс или как завершившийся? Числа из $\mathbb{N}$ потенциально можно построить или они уже есть в наличии? На таком этапе размышлений проблема отдает схоластикой. Не все ли равно, казалось бы. Понимай как хочешь. Последствий-то никаких.



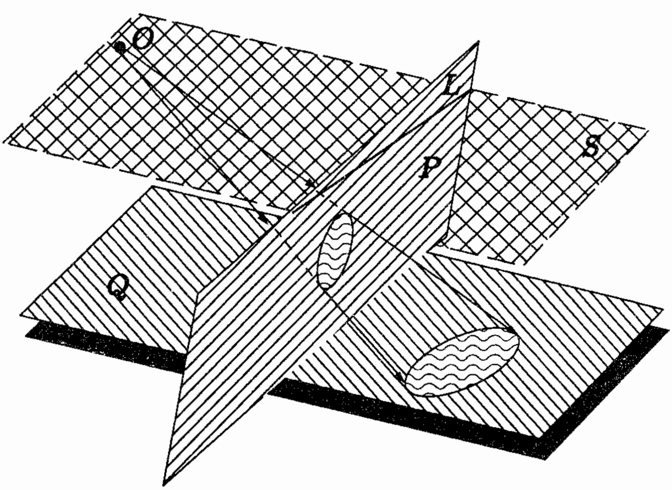
Рисунки А. Фоменко

Последствия тем не менее — феноменальные. «Как лодку назовешь, так она и поплывет». Какой ответ выберешь — на таком дилижансе и поедешь. В альтернативе получаются две разные математики, колоссально разнящиеся по содержанию. Одна — конструктивная, не допускающая осуществления бесконечности во всей ее необъятности. Другая — обычная, до некоторой степени всеядная.

Ощутить пропасть между ними не так просто, потому что глубина различия на поверхности почти незаметна, а докапываться в суете будней некогда. Поэтому продвигаться к разделяющей бездне лучше всего шаг за шагом на примерах.

• Если отрицать возможность окончательно сформировавшейся бесконечности, то цепочка 2.4 не имеет права существовать (виртуально, гипотетически), и задачу 2.3 придется решать другим способом.

• В *проективной геометрии* [3, тт. 8, 13] плоскость дополняется фикцией — *бесконечно удаленной прямой*, и это спасает научную дисциплину. Суть дела заключается в следующем. При *центральном проектировании* плоскости $\boldsymbol{P}$ в плоскость $\boldsymbol{Q}$ из точки O, лежащей вне $\boldsymbol{P}$ и $\boldsymbol{Q}$, точки $A \in \boldsymbol{P}$ переходят в точки $A' \in \boldsymbol{Q}$.



Механизм дает сбой на точках $\boldsymbol{P}$, лежащих в плоскости $\boldsymbol{S}$, проходящей через O и параллельной $\boldsymbol{Q}$, — они никуда не проектируются, уходят в бесконечность[22]. И только пополнение плоскостей *бесконечно удаленными прямыми* консолидирует ситуацию, определяя *проективные преобразования* как преобразования проективной плоскости, переводящие любую прямую в прямую. Концы сводятся с концами, и теория, замыкаясь в целостный феномен, начинает эффективно работать.

• Нечто подобное происходит в матанализе, где иррациональные числа суть состоявшиеся бесконечности, без которых все «стоит на месте». Последовательностям некуда сходиться, пределы не существуют, производных нет, интегралов тоже, ну и вообще. Это, конечно, галопом по Европам. Чтобы оценить степень катастрофы, надо останавливаться на частностях и каждый раз даваться диву, что отнимает время, но углубляет миропонимание[23].

Перечисленное относится к аргументам «за». Но есть и «против», особенно у интуиции. Скажем, когда ограниченное множество увеличивается в результате его поворота «как твердого тела», это в общем-то не лезет ни в какие ворота. Однако:

2.5.1. Химера. *Пусть Ω — конечное или счетное множество точек на окружности C. Тогда $C \setminus \Omega$ можно разбить на два непересекающихся множества A и B, и после поворота B на некоторый угол — из непересекающихся A и повернутого $\theta(B)$ — сложить полноценную окружность C.*

◄ В силу счетности Ω найдется поворот θ (вокруг центра C) такой, что $\Omega \cap \theta(\Omega) = \varnothing$. Полагая

$$B = \bigcup_{k=1}^{\infty} \theta^k(\Omega), \qquad A = C \setminus (\Omega \cup B),$$

имеем $A \cup \theta^{-1}(B) = C$, поскольку $\theta^{-1}(B) = \bigcup\limits_{k=0}^{\infty} \theta^k(\Omega) = \Omega \cup B$. ►

Вот другой мираж более высокого порядка.

2.5.2. «Парадокс». *Окружность $C \subset \mathbb{R}^2$ допускает разбиение на счетное число множеств $B_1, B_2, \ldots$, из которых поворотами B_j можно составить две окружности C.*

[22] Соответственно прямые, лежащие в $\boldsymbol{P}$ и пересекающиеся в некоторой точке прямой $\boldsymbol{L} = \boldsymbol{P} \cap \boldsymbol{S}$, переходят в параллельные прямые на плоскости $\boldsymbol{Q}$, а параллельные на $\boldsymbol{P}$ — в пересекающиеся прямые плоскости $\boldsymbol{Q}$.

[23] Не только и не столько по части вещественных чисел.

◀ Пусть f обозначает поворот на иррациональный (по числу оборотов) угол α, f^{-1} — поворот на угол «минус α». Точки x, y окружности C назовем *эквивалентными*, если $f^k x = y$ при некотором целом k, положительном или отрицательном. Тем самым C распадается на классы эквивалентных точек.

В каждом таком классе выберем по одному элементу[24], из которых образуем множество Z, и рассмотрим множества

$$Z^k = f^k Z.$$

Очевидно, $\bigcup\limits_k Z^k = C$, причем любое Z^p из Z^q получается поворотом Z^q, «как твердого тела», на угол $(p-q)\alpha$. Поэтому, если семейство множеств $\{Z^k\}$ разбито изначально на две бесконечных совокупности $\{Z^{\mu_k}\}$, $\{Z^{\nu_k}\}$, — то из каждой такой совокупности можно опять сложить C, потому что любое множество Z^{γ_k}, где γ обозначает либо μ, либо ν, переводится в Z^k поворотом на угол $(k-\gamma_k)\alpha$. Следовательно, из каждого подмножества

$$\bigcup_k Z^{\gamma_k} \subset C \; (\neq C)$$

передвижением Z^{γ_k}, «как твердых тел», можно снова составить C. ▶

«Мошенничество» 2.5.2 можно поднять на еще бóльшую высоту, вплоть до *феномена Банаха—Тарского* 4.3.1. Принципиальный шаг в соответствующем направлении дает препарирование группы $\boldsymbol{G}$ вращений в $\mathbb{R}^3$ с двумя образующими f и g. Повороты f и g происходят вокруг разных осей на иррациональные, по числу оборотов, углы α и β. Собственно, от $\boldsymbol{G}$ требуется лишь, чтобы она была *свободной группой*[25].

Очевидно,

$$\boldsymbol{G} = \{e\} \cup G(f) \cup G(f^{-1}) \cup G(g) \cup G(g^{-1}),$$

где e — единица группы, а $G(q)$ обозначает ***всевозможные последовательности поворотов, начинающихся с поворота q***.

Возможны также представления

$$\boldsymbol{G} = fG(f^{-1}) \cup G(f) \quad \textit{либо} \quad \boldsymbol{G} = gG(g^{-1}) \cup G(g), \tag{2.10}$$

[24] Тут мы используем *аксиому выбора*, см. главу 4.

[25] Элементами *свободной группы* являются всевозможные слова из букв *алфавита* $\mathbb{A}$, *не содержащие рядом стоящих обратных символов* f и f^{-1}. Произведение определяется как простое слияние слов, $abc * ab^{-1} = abcab^{-1}$, с учетом возможных сокращений, $abc^{-1} * cb^{-1}a = abc^{-1}cb^{-1}a = aa$.

где $fG(f^{-1})$ — множество произведений поворотов из $G(f^{-1})$ на f слева[26]. Возникает фокус типа 2.5.2, но уже с «разрезанием» $\boldsymbol{G}$ на конечное число частей, и **без использования аксиомы выбора**:

2.5.3. *Группа $\boldsymbol{G}$ может быть разрезана на четыре части*

$$G(f), \quad G(f^{-1}), \quad G(g), \quad G(g^{-1}), \tag{2.11}$$

и их поворотами (2.10) *— удвоена.*

От поворотов легко перейти к орбитам на сфере $S \subset \mathbb{R}^3$. Точки $x, y \in S$ считаются принадлежащими одной орбите в томм случае, когда x переводится в y некоторым поворотом $h \in \boldsymbol{G}$. Рассмотрим *правильную* орбиту

$$O_x = \{y: \quad y = hx, h \in \boldsymbol{G}\}, \tag{2.12}$$

на которой каждая точка достигается из любой данной — единственным образом. Существование правильных орбит устанавливается совсем просто.

◄ Каждому повороту $h \in \boldsymbol{G}$ отвечают точки S, попадающие на ось вращения f или g и остающиеся некоторое время неподвижными, — что нарушает единственность. Множество Ω таких точек счетно, в силу счетности $\boldsymbol{G}$. Поэтому любая орбита, начинающаяся в точке $x \in S \setminus \Omega$, правильна. ►

2.5.4. Теорема. *Правильная орбита* (2.12) *может быть разбита на четыре множества A, B, C, D, из которых поворотами можно сложить две орбиты*:

$$A \cup fB = O_x, \quad C \cup gD = O_x.$$

◄ Достаточно взять

$$A = G(f)x, \quad B = G(f^{-1})x, \quad C = G(g)x, \quad D = G(g^{-1})x,$$

и сослаться на п. 2.5.3. ►

---

[26] Здесь подразумевается, что $fG(f^{-1})$ состоит из слов вида $ff^{-1}\ldots$, где «...» — что угодно, в том числе e, но только не последовательность поворотов, начинающаяся с f. Поэтому $fG(f^{-1}) \cup G(f) = \boldsymbol{G}$. Что касается единицы группы, то ее можно добавить, например, в $G(f)$, но тогда f^{-1} надо убрать из $G(f^{-1})$, чтобы не дублировать e в $fG(f^{-1})$.

Сюрприз 2.5.4 представляет собой упрощенный и менее эффектный вариант *парадокса Банаха—Тарского* 4.3.1, потому что орбита вместо шара выглядит несколько эфемерно. Но сей *«парадокс»* зато *не опирается на аксиому выбора*, и это весьма примечательное обстоятельство, из которого видно, что состоявшаяся бесконечность способна заводить в такие дебри виртуального мироустройства, что почва уходит из-под ног.

2.6. Губительна ли наивность

Эту главу было трудно писать, поскольку местами приходилось изображать недоумение в контексте педагогической лжи, и разыгрывать смирение в замешательстве перед безответными вопросами. Таковой была *наивная теория множеств Кантора*, построенная на смеси здравого смысла и мистической тяги к бесконечности. *«Наивная»* в смысле неочерченности и неопределенности по части неоговоренности средств и непомерности целей.

В следующей главе фундаментально повисшие здесь вопросы, типа «откуда берутся множества» и «существует ли натуральный ряд», исчезают. Аксиоматизация, правда, избавляет от головной боли, но не от душевных мук. Теория, построенная на формальных основаниях, обретает стройность и дает казенные ответы на азбучные вопросы, а дисгармонию ретуширует. Противоречия уходят вглубь, и до них уже не так легко добраться. Это типичный сценарий, ибо *теорема Гёделя о неполноте* 6.4.2 не оставляет надежд. Поэтому если наивная теория хлопочет о прояснении ситуации, то этажом выше все ясно — вопросы остаются безответными, но по более глубоким причинам.

Глава 3

Аксиоматика Цермело—Френкеля

ZFC-система занимает в виртуальном мире намного больше места, чем египетские пирамиды на Земле.

Теория множеств становится интересной задним числом. Когда выясняется, что предмет изучения — не множества, а инструменты. Не итог, а процесс. Допущения, жонглирование, — вот что образует центральный механизм. За конечный результат ответственны аксиоматика и логика — с них-то и надо бы начинать. Но в реальности ими приходится заканчивать, потому что картина проясняется только к концу.

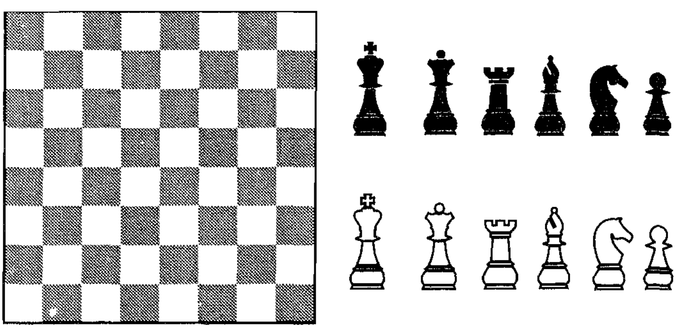
3.1. Отступление

Когда речь заходит о вещах, близких к основаниям математики, реальные потребности уходят вроде бы за горизонт. Но это та же история, что и собирание марок, спичечных коробков, игра в домино, увлечение поэзией, музыкой, живописью. Утилитарная надобность вроде бы нулевая, а вдумаешься, так ничего более важного нет. Математика в этом ряду вполне может стоять на первом месте. Потому что в первую очередь — это не инструмент решения повседневных задач, а фундамент психологической надстройки. Теоремы *Гёделя* или аксиомы *Пеано* — напрямую никому не нужны. Но от знакомства с подобными вещами зависит ви́денье Мира, круг общения, манеры поведения, успехи и неудачи в любых начинаниях. Соприкосновение с корнями теории множеств опосредованно влияет на стиль мышления и образ жизни, на выбор друзей, жены, страны. «I am a part of everything that I have read», — говорил *Теодор Рузвельт*.

Так что к математике, как и вообще к жизни, имеет смысл подходить с иррациональных позиций. Нет ничего полезнее бесполезных вещей. Но влипать тоже не стоит, чтобы не увязнуть. Поэтому дальнейший текст ориентирован на умеренное проникновение в суть дела.

3.2. Проблема аксиоматизации вообще

На аксиоматизацию полезно взглянуть вообще, как можно шире, — осознавая, что речь идет о задании некоторой игры. Обдумывание удобно начать с чего-нибудь за пределами математики. Например, с шахмат, где описание начинается с таких понятий, как доска, король, ферзь, ход, позиция и т. д. Затем наступает черед регламентации правил игры. При этом ясно, что обычное представление о шахматах



совершенно необязательно. Игровое поле и фигуры могут выглядеть иначе, и даже быть просто символами, e2–e4, Kg8–f6. «Аксиоматизация» шахмат ныне доведена до синтаксического уровня, о чем свидетельствует успешная игра компьютеров.

Доведение любой проблематики до синтаксиса является идеальным вариантом аксиоматизации любой дисциплины и перевода семантики на уровень программирования. Пока же хоть что-то остается в руках человека, от смысловой интерпретации очень трудно избавиться. В результате многое ускользает от формализации, и гарантировать, что теория стоит на каких-нибудь трех китах, удается с натяжкой [1].

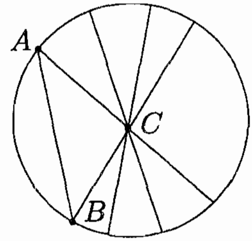
Дополнительное освещение проблематика аксиоматизации получает при переходе к геометрии *Евклида*. К игре, которая более двух тысяч лет считалась образцовой теорией, построенной на дедуктивных началах. Безмятежное существование продолжалось до тех пор, пока оную геометрию не стали компьютеризировать. Программирование выявило пробелы в аксиоматике. Вдруг обнаружилось, что без визуальных представлений о точках и прямых «чего-то не хватает». Компьютеру потребовались дополнительные указания и уточнения. Например, разъяснения, что такое «между». Дополнительные постулаты, попросту говоря. Таким образом выяснилось, что на пяти стерильных постулатах *Евклида* геометрию не построишь. Здравый смысл в той или иной форме просачивается в рассуждения, и процесс формализации таких ингредиентов растягивается на века. Программы, доказывающие геометрические теоремы, ныне есть, но в какой мере они урезают геометрию *Евклида*, не вполне ясно.

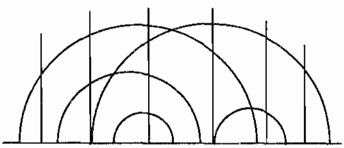
Геометрия Лобачевского привносит в тему новые краски. История хорошо известна. Многовековая эпопея освобождения геометрии *Евклида* от пятого постулата (Е5) «Через точку, лежащую вне прямой, проходит единственная прямая, не пересекающая исходную» закончилась построением новой геометрии с заменой (Е5) аксиомой (Л5) «Через точку, лежащую вне прямой, проходит по крайней мере две прямые, не пересекающие исходную». При этом Лобачевский действовал «синтаксически», манипулируя с постулатами чисто формально, без какого бы то ни было визуального сопровождения, ибо никто в те времена не мог себе представить, как Л5 может реализоваться.

---

[1] Напомним, синтаксическая точка зрения убирает смысловую интерпретацию. Знаки $\forall$, $\exists$, $\in$ — превращаются в буквы. Преобразования и выводы, базирующиеся в семантическом русле на понимании операций, теперь регулируются только грамматикой, построенной на *правилах вывода* и *аксиомах*.

Бельтрами впоследствии показал, что новая геометрия выполняется на поверхностях постоянной отрицательной кривизны. Еще более эффектна *модель Клейна*, в которой: плоскость — внутренность круга, прямые — хорды. Через точку C проходит целый пучок хорд, не пересекающих AB (рисунок справа). Вот такая модель *геометрии Лобачевского*.





Другой вариант реализации *геометрии Лобачевского — модель Пуанкаре*, в которой «плоскостью» служит открытая полуплоскость, «прямыми» — полуокружности, а также вертикальные полупрямые, как полуокружности бесконечного радиуса.

Обе модели, произрастающие из единого корня, как нельзя лучше характеризуют проблему взаимоотношения чисто логической аксиоматики и возможности ее наполнения каким-либо содержанием. Демонстрация на примерах позволяет ощутить, в чем суть и какие у нее (у сути) бывают лица. Есть даже целая научная дисциплина — *теория моделей* (глава 7), — направленная в основном на изучение логических схем и аксиоматик.

3.3. Система ZFC

Френкель (1891–1965)

Соседство философии с теорией множеств подталкивало первооткрывателей к принятию экстренных мер демаркационного толка[2)]. Наибольшую известность в этом отношении получила *аксиоматика Цермело—Френкеля*, называемая обычно системой **ZF** или **ZFC**, где **C** подчеркивает присутствие в системе *аксиомы выбора*.

[2)] Что касается Кантора, то соседство с философией его воодушевляло.

Ведущая роль в формировании системы **ZF** принадлежит *Цермело*, портрет которого расположен в окрестности *теоремы* 4.1.4.

Исходные неопределяемые понятия в **ZFC** — это «множество» и отношение $\in$ «быть элементом»[3]. К языку добавляются логические связки и кванторы

$\neg$	*отрицание «не»*
$\vee$	*или (дизъюнкция)*
$\wedge$	*и (конъюнкция)*
$\to$	*следует*
$\leftrightarrow$	*в томм случае, когда*
$\forall$	*для всех*
$\exists$	*существует*

, (3.1)

с помощью которых строятся *предикаты* на базе двух элементарных отношений: $X \in Y$ и $U = V$. Ничто другое в принципе не допускается, но используются скобки[4] и некоторые сокращения типа $X \neq Y$, $X \notin Y$, $X \subset Y$:

$X \neq Y$	$\neg(X = Y)$
$X \notin Y$	$\neg(X \in Y)$
$X \subset Y$	$\forall Z : Z \in X \to Z \in Y$

. (3.2)

В качестве сокращений используются также $\cap$, $\cup$, $\setminus$, Δ, и другие общепринятые символы, каковые могут быть расшифрованы с помощью «первичных» обозначений.

Скажем, $Z = X \cup Y$ означает $\forall U \in Z \leftrightarrow (U \in X) \vee (U \in Y)$.

Иногда о множествах говорят как о последовательностях или функциях, что с точностью до изоморфизма является вопросом терминологии. *Функция* из $\mathbb{R}$ в $\mathbb{R}$, например, это множество упорядоченных пар действительных чисел (график функции). А *действительное число* — это множество эквивалентных фундаментальных последовательностей.

---

[3] Напомним, что запись $X \in Y$ означает: множество X является *элементом* Y. Поэтому, например, $X = \{2, 3\}$ не является элементом $Y = \{2, 3, 4\}$, хотя $X \subset Y$, но является элементом множества $\{\{2, 3\}, 3, 4\}$.

[4] Для однозначного прочтения формул.

Наивная точка зрения состоит во взгляде на множества как на совокупности элементов, каковые могут быть объектами любой природы, в том числе множествами[5]. Новые множества из уже существующих получаются неким комбинированием, которое нуждается в сдерживающих началах во избежание противоречий. Напомним классический *парадокс Рассела*. Пусть S есть множество, элементами которого являются все такие множества X, что X не является элементом X. Тогда

$$\forall X : X \in S \leftrightarrow X \notin X, \tag{3.3}$$

в том числе для $X = S$, что дает противоречие $S \in S \leftrightarrow S \notin S$.

Тут, конечно, есть резон вспомнить еще о неприятностях, связанных с использованием кванторов. Например,

$$\forall X \varphi(X) \to \varphi(Y) \tag{3.4}$$

представляется очевидным фактом: «если утверждение $\varphi(X)$ справедливо при любом аргументе, то в $\varphi(X)$ можно подставить $X = Y$». Но в случае

$$\varphi(X) = \exists Y : Y \neq X$$

подстановка в (3.4),

$$\forall X \, \exists Y : Y \neq X \to \exists Y : Y \neq Y,$$

приводит к нелепости. Поэтому логика уделяет кванторам особое внимание, более всего — их взаимодействию.

Аксиоматика **ZFC** базируется на следующих постулатах[6]:

Z1. *Аксиома объемности: множества равны в томм случае, когда состоят из одних и тех же элементов.*

Такого сорта назидания новичок воспринимает с улыбкой, думая в лучшем случае: «зачем ломиться

[5] В **ZFC** элементами могут быть только множества, см. далее. В другой системе **ZFA** допускаются элементы, не являющиеся множествами, каковые называются *атомами*, или *праэлементами*.

[6] Система **ZFC** допускает некоторые модификации, поскольку не все аксиомы независимы. Поэтому обсуждаемый ниже список аксиом несколько отличается от приведенного в [3, т. 6].

в открытую дверь». И тогда возникают пояснения насчет «важности и нужности **Z1**». Это нередко ухудшает ситуацию, потому что всякое смысловое разъяснение привносит дополнительные краски, маскирующие суть, которая в очищенном виде сводится к грамматике:

$$\forall X : (X \in Y \leftrightarrow X \in Z) \to (Y = Z).$$

Все превращается в символы — и двусмысленностям нет места.

Z2. *Аксиома существования пустого множества* $\varnothing = \{\}$:

$$X = \varnothing \quad \leftrightarrow \quad \neg\exists\, Y : Y \in X.$$

Факт существования $\varnothing$ важен, например, в ситуации, когда в процессе преобразований некоторое множество может в принципе «опустеть», что сразу не ясно, и тогда без **Z2** механизм доказательства перестает работать.

Но роль пустого множества в ZFC более грандиозна, $\varnothing$ — единственный первичный элемент, с помощью которого можно строить «любые» множества, комбинируя шаги[7]:

$$\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}, \ldots, \tag{3.5}$$

и применяя далее разрешенные аксиоматикой операции.

Глядя на (3.5), можно подумать, что с помощью $\varnothing$ и фигурных скобок образуются максимум счетные множества. Однако другие аксиомы позволяют «многократно уходить в бесконечность», образуя множества типа

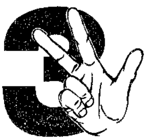
$$\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \ldots\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}, \ldots\}, \ldots, \tag{3.6}$$

и это уводит сколь угодно далеко в «несчетный мир».

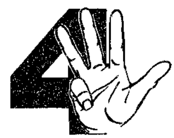
Что касается натурального ряда и других «стандартных» множеств, то они рассматриваются в привычном виде, каковому каждый раз отвечает эквивалент из ассортимента (3.6). Но сказанное

[7] Обратим внимание, что $\varnothing$ — множество, не имеющее элементов; $\{\varnothing\}$ — множество, единственным элементом которого является $\varnothing$.

не означает, что множества вообще могут состоять из произвольных элементов. Такое послабление разрушает теорию. Тем не менее существует аксиоматическая система **ZFA**, в которой элементами могут быть *атомы*, или *праэлементы*, — но там требуются другие сдерживающие начала.

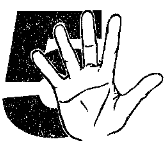


Z3. *Аксиома пары: каковы бы ни были X и Y, существует множество Z, содержащее X и Y.*



Z4. *Аксиома объединения: для любого X существует множество, содержащее элементы элементов X и только их.* Синтаксически это выглядит так:

$$\forall X\ \exists Y\ \forall Z : \big(Z \in Y \leftrightarrow \exists T : (Z \in T \in X)\big).$$



Z5. *Аксиома бесконечности: существует бесконечное множество*, что синтаксически уточняется следующим образом:

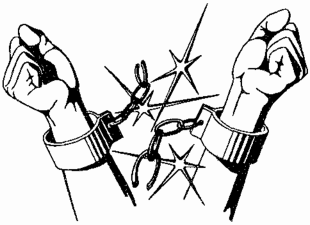
$$\exists X : \big[(\varnothing \in X) \wedge \forall Y : (Y \in X \to Y \cup \{Y\} \in X)\big]. \qquad (3.7)$$

В переводе на русский язык (3.7) означает существование множества X, которому принадлежит $\varnothing$ и вместе с каждым $Y \in X$ в X входит и $Y \cup \{Y\}$.

Здесь, собственно, собака и зарыта. Плоды фантазий объявляются реальностью, и *состоявшаяся бесконечность*[8] обретает гражданство.

На формулировке **Z5** особенно хорошо заметна роль синтаксиса. Словесная декларация существования бесконечного множества дает такую свободу толкования, что с подобной аксиоматикой далеко не уедешь.

[8] Напоминаем, мы всячески избегаем употребления неудачного термина *«актуальная бесконечность»*.



Z6. *Аксиома подстановки: каковы бы ни были X и Y, для любой формулы $\varphi(U,V)$ (подразумеваются формулы языка первого порядка в сигнатуре $\{\in,=\}$) существует множество*

$$Z=\{T\in X:\varphi(T,Y)\},$$

содержащее все $T\in X$, обладающие свойством $\varphi(T,Y)$. По сути **Z6** *является* ***схемой аксиом***.

Z6 подвержена некоторым вариациям, как содержательным, так и терминологическим. Ее называют также *аксиомой свертывания* или *аксиомой выделения*. Аксиома **Z6** допускает рассмотрение только таких определяемых совокупностей, которые содержатся в некотором множестве, — и это главное, на что здесь надо обратить внимание[9].

Множество решений диофантова уравнения $P(x)=0$ заведомо является подмножеством множества $\mathbb{N}\times\ldots\times\mathbb{N}$, и потому имеет право на существование, хотя о его свойствах может быть ничего не известно, см. раздел 2.1.

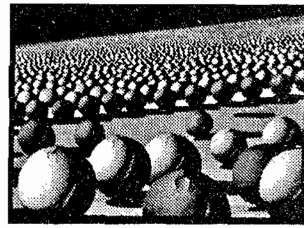
Z7. *Аксиома степени: для любого X существует множество 2^X всех подмножеств X*. Синтаксически это оформляется следующим образом:

$$\forall X\,\exists Y\,\forall Z:(Z\in Y\leftrightarrow Z\subset X).$$

Это весьма «скользкая» аксиома, интуитивно прозрачная в относительно простых ситуациях, но заводящая в тупики за привычным горизонтом, см. хотя бы раздел 8.4.

[9] Источником **Z6** послужили затруднения, возникавшие в наивной теории множеств из-за того, что множеством считалась любая определяемая совокупность.

Z8. *Аксиома выбора* **AC**[10]. Утверждает, что *для каждого множества X существует функция выбора на X, т. е. функция f, сопоставляющая всякому подмножеству $Y \in X$ элемент $f(Y) \in Y$*, см. главу 4.

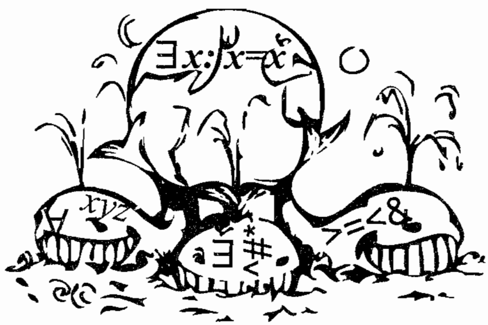


Z9. *Аксиома фундирования* постулирует, что *не существует бесконечных убывающих цепей,*

$$X_1 \ni X_2 \ni \ldots .$$

Альтернативой является *аксиома регулярности*, утверждающая существование в каждом непустом множестве элемента, не содержащего других элементов этого множества.

В тайниках **ZFC** есть масса неисследованных закоулков. При серьезных намерениях взаимодействие и роль аксиом **Z1–Z9** нуждаются в постепенном и скрупулезном освоении. Мы здесь ограничиваемся взглядом издалека.



Комплект **Z1–Z9** уникален как системно, так и частностями. Особенно широко известны «аномальные свойства» *аксиомы*

[10] По первым буквам «*axiom of choice*».

выбора. На первый взгляд, **Z8** естественна и не обещает неожиданностей. Однако с ее помощью строится *неизмеримое по Лебегу множество Витали*, а шар разбивается на конечное число частей, которые после «механического передвижения» образуют два шара такого же размера, см. главу 4.

Не менее каверзна аксиома **Z5**, признающая по сути натуральный ряд $\mathbb{N}$ как свершившийся факт. Не как наращиваемую сущность, а как готовую неприятность — и окаянная вседозволенность *состоявшейся бесконечности* тут как тут. Надежды, что для исполненной бесконечности требуется хотя бы кошелек конечного объема типа $[0, 1]$, тут не имеют оснований.

В более ясном толковании нуждается *аксиома фундирования*[11] **Z9**, которая почти без потерь может быть исключена из списка. Конечно, она блокирует *парадокс Рассела*, но с этим справляются и другие аксиомы. Главная роль **Z9** в основном философская, обеспечивающая взгляд на мир множеств как на *универсум фон Неймана*, иерархически вырастающий из «ничего», т. е. из пустого множества $\varnothing$.

Заметим, что в **Z9** речь идет о цепях, убывающих не по включению множеств. Запись $X \in Y$ не означает $X \subset Y$. В $X \in Y$ подразумевается, что X — элемент множества Y. У натурального ряда $\mathbb{N}$, например, никакое подмножество не является элементом $\mathbb{N}$. Поэтому все цепи в $\mathbb{N}$ обрываются на втором шаге, $k \in \mathbb{N}$ — и все[12]. Но возможны множества иного сорта, скажем,

$$\{1,\ 2,\ \{2, 4, \{3, 8\}\},\ \{137\},\ \{3\},\ 3,\ \ldots\}.$$

Здесь цепи длиннее, но не могут быть бесконечными, в силу **Z9**.

---

[11] Введена *Бернайсом* и *Гёделем* в 1941 году, заменила аксиому регулярности *фон Неймана* (1925).

[12] Правда, оставаясь в рамках **ZF**, приходится пользоваться изоморфным представлением натуральных чисел,

$$\varnothing \leftrightarrow 0, \{\varnothing\} \leftrightarrow 1, \{\varnothing, \{\varnothing\}\} \leftrightarrow 2, \ldots .$$

При таком понимании $\mathbb{N}$ убывающие цепи могут быть сколь угодно длинными, но любая из них — конечна.

Следствия **ZFC** простираются очень далеко, образуя «вблизи» общепринятые нормы теории множеств, которые мы привыкли воспринимать как нечто само собой разумеющееся. Например:

3.3.1. *Если X и Y — множества, то*

$$X \cap Y, \quad X \cup Y, \quad \{X\}, \quad \{X, Y\}$$

также множества.

Помимо $\{X, Y\}$ иногда возникает необходимость в определении *упорядоченной пары* множеств $\langle X, Y\rangle$, где X идет первым номером, и $\langle X, Y\rangle = \langle U, V\rangle$ в томм случае, когда $X = U$, $Y = V$. В рамки **ZFC** такая дефиниция не помещается. Но язык **ZFC** позволяет все же определить *упорядоченную пару* как

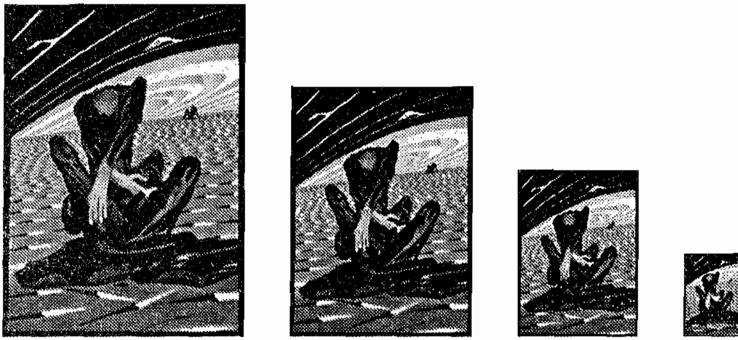
$$\langle X, Y\rangle = \{\{X\}, \{X, Y\}\}. \tag{3.8}$$

• Варианты $\langle X, Y\rangle = \{X, Y\}$, $\langle X, Y\rangle = \{X, \{X, Y\}\}$, — не годятся. **(?)**

Конструкция (3.8) возникает лишь в связи с потребностями «говорить на языке **ZFC**». Обычная практика пролегает вдали от таких формальностей. Скажем, *декартово произведение* $X \times Y$ определяется как совокупность всех *упорядоченных пар* $\langle x, y\rangle$ таких, что $x \in X$, $y \in Y$. При этом никто не вспоминает об устройстве (3.8), довольствуясь представлением $\langle x, y\rangle = \{x, y\}$ с оговоркой, что x стоит на первом месте.

Широко используются также множества, состоящие из чисел, символов, функций и других неправомерных в **ZFC** элементов. Но беда тут небольшая, потому что эти множества изоморфны легальным в **ZFC** множествам *универсума фон Неймана*, получаемым из элементов (3.5) с помощью инструментов **Z1–Z9**.

Заметим, что пассивное созерцание аксиом **ZFC** мало что дает и едва ли целесообразно само по себе, ибо равносильно лицезрению неработающего двигателя или даже его чертежей. Тут надо постепенно «въехать в тему», понаблюдать динамику, следствия; приблизиться к ядру противоречий и ощутить загадку.



Рисунки А. Фоменко

Что же до периферии теории множеств, так она рассеяна по многим территориям и хорошо известна всем, кто изучал анализ и родственные дисциплины. Так что постижение теоретико-множественных премудростей при аппаратно-математической грамотности не имеет особого смысла, если устремления ограничены приземленными потребностями. Для изучения «глубин» необходимо хроническое стремление разобраться в том, без чего можно обойтись. Однако обойтись можно «без всего».

3.4. Взаимодействие с логикой

Упоминание логики вскользь в рамках **ZFC** создает впечатление, что логика тут находится в тени примерно как в обычной математике. Совершенно «не так». В обычных математических дисциплинах *логический уровень сложности крайне низок*. Используются примитивные конструкции вроде «упал — отжался». Довольно короткие комбинации из ассортимента (3.1), и никакого сколько-нибудь длительного жонглирования.

Другое дело — до чего матлогика может довести сама по себе. «До чего» в принципе. До каких крайностей можно дойти при отсутствии сдерживающих факторов. Именно на такие вопросы приходится отвечать, рассматривая потенциальные возможности разрешенных инструментов в аксиоматизации. Тут «краеугольная» проблематика вынуждена иметь дело с логикой не как с подсобной грамматикой умозаключений, а как с источником опасностей при безудержном использовании инструмента.

3.5. Натуральный ряд и арифметика Пеано

Арифметика Пеано представляет собой шедевр в смысле минимизации посылок. *Аксиоматика Пеано* сводит арифметическую систему $\{\mathbb{N}, +, \times\}$ к алгебре с одной *операцией счета* σ, называемой также *функцией следования*, $\sigma : \mathbb{N} \to \mathbb{N}$, и удовлетворяющей трем *аксиомам Пеано*[13]:

A1 $\sigma(m) = \sigma(n) \to m = n$.

A2 $\forall n \in \mathbb{N} : \sigma(n) \neq 1$.

A3 Если 1 обладает свойством $\mathcal{P}$, т. е. $\mathcal{P}(1) = 1$ и $\mathcal{P}(n) = 1$ влечет за собой $\mathcal{P}(\sigma(n)) = 1$, то свойством $\mathcal{P}$ обладает любое n.

Разумеется, предпринимая в арифметике ту или иную акцию, нет необходимости каждый раз стартовать с крохотной площадки **A1–A3**. Все уже «выведенное» можно использовать в качестве готовых инструментов. В [3, т. 6] показано, например, как с помощью **A1–A3** вводятся арифметические действия.

Аксиома **A3** часто формулируется в более общем виде:

A3′ Если $1 \in Q \subset \mathbb{N}$, где Q — произвольное подмножество $\mathbb{N}$, и «$n \in Q \to \sigma(n) \in Q$», то $Q = \mathbb{N}$.

Разница между **A3** и **A3′** разительна. В первом случае дело приходится иметь со счетным множеством подмножеств $\mathbb{N}$, в варианте **A3′** — с континуальным. При этом **A3′** постулирует больше, чем арифметика может проглотить, потому что утверждений и доказательств (а значит, и подмножеств $Q \subset \mathbb{N}$, которые имеют шанс попасть в поле зрения) — счетное число[14].

---

[13] Точнее, *аксиоматическая система Пеано* есть **A1–A3** плюс стандартные «логические аксиомы».

[14] Потому что подмножества Q *конструктивно выделяются* только с помощью перечислимых предикатов.

Немаловажно отметить, что арифметика может быть погружена в систему **ZFC**. Для этого в рамках **ZFC** надо построить натуральный ряд $\mathbb{N}$ и ввести аналог *функции следования*. Делается это так. Нулю сопоставляется пустое множество $\varnothing$; 1 отождествляется с $\{0\}$, 2 с $\{0, 1\}$ и т. д. При этом переход к следующему натуральному числу осуществляется с помощью операции

$$\sigma(X) = X \cup \{X\}. \tag{3.9}$$

В результате арифметические аксиомы Пеано становятся теоремами системы **ZFC**. В том числе матиндукция — ибо **А3** является частным случаем трансфинитной индукции, каковая в **ZFC** не постулируется, а доказывается, см. п. 4.2.1.

Аксиоматика Пеано, разумеется, не есть инструмент привычной арифметики. Это зародыш, из которого остальное вырастает. Как бы ДНК арифметики, каковая в своих фенотипических проявлениях опирается на более адекватный инструментарий. Например, на язык

$$L = \{+,\ \times,\ =,\ \exists\ ,\ \forall\,\}, \tag{3.10}$$

который возникает при соединении **А1–А3** с *логикой первого порядка*. Чрезвычайно интересен и важен усеченный *язык примитивной арифметики*

$$L_0 = \{+,\ \times,\ =,\ \exists\,\}, \tag{3.11}$$

в котором исключена математическая индукция, и ничего нельзя доказать, можно только проверить разрешимость полиномиального уравнения (перебором). Иначе говоря, все *верные* утверждения $\exists\, xP(x) = 0$, и только они, в L_0 доказываются.

В то же время язык L_0, как *язык диофантовых уравнений*, оказывается исключительно богат по своим возможностям, и позволяет описывать любые алгоритмически выразимые свойства чисел, множеств и других умопостигаемых объектов. Вот как это выглядит в простейших ситуациях.

- Множество A пар $\{a_1, a_2\}$, у которых a_2 делится на a_1,

$$A \leftrightarrow \exists\, x : a_1 x = a_2 \leftrightarrow P(a, x) = a_1 x - a_2 = 0.$$

- Множество A упорядоченных пар $\{a_1 < a_2\}$,

$$A \leftrightarrow \exists\, x : a_1 + x = a_2 \leftrightarrow P(a,x) = x + a_1 - a_2 = 0.$$

- Множество $\{a \neq 2^n\} \leftrightarrow \exists\, x_1\ \exists\, x_2 : a = x_1(2x_2 + 1)$.

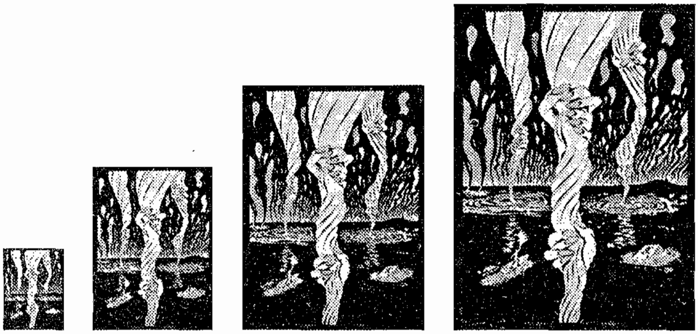
Аналогичным образом любая «вычислимая» задача сводится к разрешимости уравнения $P(a,x) = 0$, где $a = \{a_1, \ldots, a_k\}$, $x = \{x_1, \ldots, x_n\}$. В результате множества целых чисел или векторов a, для которых справедливо $\exists\, x : P(a,x) = 0$, т. е. диофантов полином $P(a,x)$ имеет корни, — оказываются единственно алгоритмически осмысливаемыми множествами, что лежит в недрах *десятой проблемы Гильберта* (глава 6, см. также [3, т. 6]).

3.6. Универсумы фон Неймана и Гёделя

Вернемся к общей аксиоматике теории множеств. Оглядываясь ретроспективно на **ZFC**, нетрудно угадать индуктивный путь развития системы. Изначально всеохватывающая точка зрения на множества как на произвольные совокупности любых элементов регулярно демонстрировала свою неадекватность, и шаг за шагом подталкивала к принятию регламента. Рамки поиска формата естественно группировались вокруг простой идеи — фиксировать совокупность разрешенных элементов и оговорить правила построения более сложных множеств из более простых.

«Правила» постепенно консолидировались в альянс **Z1–Z9**. Что же касается «разрешенных элементов», оказалось возможным обойтись вообще без них, постулировав существование пустого множества, — и тем самым обеспечивая, с точностью до изоморфизма, законность работы с разнообразными множествами, возникающими на практике.

При этом, однако, был упущен механизм вырастания сложного из простого. Правила правилами, но каков тот океан множеств, который зиждется на аксиоматике? Есть ли у него берега и нет ли закупоренных темниц? Здесь определенный интерес представляют различные *модели теории множеств*, которые укладываются

$\varnothing$ 

Рисунки А. Фоменко

в рамки **ZF** или **ZFC** и как-то организуют процесс образования новых множеств, уменьшая широту замаха. На этом пути выделяется модель *фон Неймана*.

Об **универсуме фон Неймана** V уже говорилось в форме (3.6), не очень удобной для восприятия. Построение *универсума* V отправляется от пустого множества $\varnothing$ и далее последовательно применяется *операция степени* — образования множества всех подмножеств уже построенных множеств. Начальный отрезок такого построения выглядит так:

$$V_0 = \varnothing, \quad V_1 = 2^{V_0}, \quad V_2 = 2^{V_1}, \quad \dots . \tag{3.12}$$

По «завершении» счетного процесса (3.12) делается следующий *трансфинитный* шаг и т. д. Весь процесс единообразно описывается трансфинитной рекурсией: для следующего *порядкового числа* (*ординала*)[15] $\alpha + 1$ множество $V_{\alpha+1}$ определяется как 2^{V_α}, а для *предельных ординалов* α как

$$V_\alpha = \bigcup\{V_\beta : \beta < \alpha\} \tag{3.13}$$

Универсум V (но это уже не множество в рамках **ZF**) определяется как объединение всех V_α,

$$V = \bigcup_\alpha V_\alpha.$$

[15] Ординалы рассматриваются в главе 5.

Построенная совокупность (класс) V, как оказывается[16], исчерпывает все допустимые в **ZF** множества, т. е. множества вида (3.6). Предмет для доказательства здесь заключается в том, что **ZF** допускает и другие способы образования новых множеств из старых (взятие пересечений, например), но описанный механизм взятия всех подмножеств из уже «готовых» множеств перекрывает все остальное, что и приходится доказывать. А предполагать приходится непротиворечивость **ZF** — иначе построению грош цена (см. главу 6).

Фон Нейман
(1903–1957)

Универсум Гёделя L (или *конструктивный универсум*, constructible universe) представляет собой класс множеств, конструируемых поэтапно[17] из множеств, построенных ранее, т. е. формулы и кванторы могут быть обращены лишь к уже сконструированным множествам[18].

Все происходит по аналогии с построением V, но вместо 2^X используется усеченная операция $\mathrm{Def}(X)$, производящая множество подмножеств X, выводимых в **ZF**, *но только с параметрами из* X. Схема «выращивания» L аналогична (3.12), (3.13),

$$L_0 = \varnothing, \quad L_{\alpha+1} = \mathrm{Def}(L_\alpha),$$

$L_\alpha = \bigcup\{L_\beta : \beta < \alpha\}$ для *предельных ординалов* α, наконец,

$$L = \bigcup_\alpha L_\alpha.$$

При этом каждый α-шаг получения множества подмножеств L_α может быть развернут в трансфинитную последовательность получения подмножеств L_α. В результате ***все*** множества из L вы-

[16] Это не очень сложная теорема, но немного скучная.

[17] Но не алгоритмически в смысле [3, т. 6].

[18] Если $\varphi(Z, X)$ логическая формула, то совокупность множеств Z, при которых $\exists X : \varphi(Z, X)$ истинна, зависит очевидным образом от того, в каких границах подразумевается $\exists X$.

страиваются в трансфинитную последовательность. Иначе говоря, *все* множества из L оказываются вполне упорядочены, и тогда любому $X \in L$ можно сопоставить наименьший элемент X, т. е. в L существует по крайней мере одна функция выбора, что влечет за собой справедливость следующего утверждения.

3.6.1. Теорема. *В универсуме Гёделя* $\mathbf{L}$ *аксиома выбора выполняется автоматически.*

Это означает, что **AC** не противоречит **ZF**. Точнее говоря, если система **ZF** непротиворечива[19], то и **ZFC** непротиворечива, т. е. **AC** можно безбоязненно присоединять к **ZF**.

Сказанное вытекает из теоремы 3.6.1, потому что L является моделью[20] **ZF**. И если бы **AC** противоречила **ZF**, то в любой модели **ZF** **AC** не могла бы выполняться. Кстати говоря,

3.6.2. *в универсуме Гёделя* L *справедлива* **ГК**[21],

и потому *гипотеза континуума* не противоречит аксиоматике **ZF**, разумеется, в предположении непротиворечивости **ZF**. Следовательно, **ГК** можно добавить к **ZF** как аксиому.

Коэн (1963) к вышесказанному добавил противоположное: к системе **ZF** в качестве аксиом можно добавить *отрицания* (!) **AC** и **ГК**. Вот точная формулировка его результатов.

3.6.3. Теорема. *Если теория* **ZF** *непротиворечива, то аксиома выбора не является теоремой теории* **ZF**.

3.6.4. Теорема. *Если теория* **ZF** *непротиворечива, то гипотеза континуума не является теоремой теории* **ZFC**.

---

[19] О чем мы можем только догадываться.

[20] Чтобы убедиться в этом, достаточно удостовериться в справедливости всех аксиом **ZF** в L, что сводится в основном к тавтологии.

[21] Результат в принципе прозрачен, хотя рутина, как всегда, неизбежна, см. [19, ч. II, гл. 5]. В связи с максимально экономичным ходом построения множеств в L для любого *кардинала* ξ *кардинал* 2^{ξ} имеет минимально возможное значение. Поэтому в L, в частности, $2^{\aleph_0} = \aleph_1$, см. также п. 8.3.2.

Глава 4

Аксиома выбора

Мир устроен так,
что удивляться заранее — не получается.

Всякое исследование должно проходить под творческим надзором смотрящего, способного «в случае чего» переосмыслить задачу и направить усилия в другое русло. Но также способного держать курс и не паниковать по любому поводу, ибо ложь и правда все равно неотделимы.

4.1. Концепция Всевидящего Ока

Формулировка *аксиомы выбора* **AC** (раздел 3.3) подвержена некоторым модификациям. Популярен следующий вариант.

4.1.1. Аксиома выбора. *В любом семействе* Φ *непустых множеств существует функция выбора* f, *ставящая в соответствие каждому* $X \in \Phi$ *элемент* $f(X) \in X$.

Существенно, что выбрать по одному элементу можно одновременно, а не «по очереди», т. е. существует функция выбора как *состоявшаяся бесконечность*.

Параметрическая разновидность 4.1.1:

4.1.2. Аксиома выбора. *В любом семействе*

$$\Phi = \{X_\alpha : \alpha \in \mathcal{A}\}$$

непустых множеств существует функция выбора $f(X_\alpha) \in X_\alpha$.

Интересно, что 4.1.2 равносильно ***непустоте прямого произведения***

$$\prod_{\alpha \in \mathcal{A}} X_\alpha, \tag{4.1}$$

ибо всякий элемент

$$\prod_{\alpha \in \mathcal{A}} X_\alpha,$$

если таковой имеется, представляет собой график некоторой *функции выбора*. Допустить, что прямое произведение (4.1) непустых множеств оказывается пустым — представляется абсурдным. Под этим углом зрения аксиома 4.1.2 выглядит особенно естественной. Но в этом, собственно, и заключается искусство софистики.

AC — действительно аксиома, в рамках **ZF** ее нельзя ни доказать, ни опровергнуть (разделы 3.6, 8.5, 8.7). Поэтому вопрос о ее правдоподобии лежит за пределами **ZF**. И в условиях независимости лучше говорить о ее согласовании с периферией нашего мировоззрения, каковое, вообще говоря, иллюзорно и зыбко.

Ослабленный вариант 4.1.2 до уровня $\mathcal{A} = \mathbb{N}$ называют *счетной аксиомой выбора*.

Вот еще одна разновидность формулировки аксиомы выбора.

4.1.3. Аксиома выбора. *Если $f : X \to Y$ — сюръективное*[1] *отображение, то существует подмножество $Z \subset X$, пересекающееся с каждым слоем*

$$f^{-1}(y) = \{x : f(x) = y\} \tag{4.2}$$

ровно по одному элементу[2].

[1] *Сюръективным* называют «отображение на», у которого все *слои* (4.2) непусты, т. е. уравнение $f(x) = y$ разрешимо при любом $y \in Y$.

[2] Иначе говоря, существует сужение $f|_Z$, являющееся *биекцией*, т. е. сюръективным взаимно однозначным отображением $f|_Z : Z \to Y$.

Известно довольно много утверждений, эквивалентных *аксиоме выбора*. Среди них наиболее популярны:

4.1.4. Теорема Цермело. *Всякое множество X можно вполне упорядочить, т. е. ввести такое отношение порядка, при котором у любого подмножества $A \subset X$ будет наименьший элемент*[3] $x^0 \in A$.

Цермело (1871–1953)

Напомним, что *наименьший элемент* в множестве A — это элемент $x^0 \in A$, меньший любого другого: $x^0 \leqslant x$, если $x \in A$. А *минимальный* (*максимальный*) *элемент* — это такой $x^* \in A$, что в A нет элемента меньшего (большего) x^*.

4.1.5. Лемма Цорна. *Если в частично упорядоченном множестве X любое частично упорядоченное подмножество ограничено снизу, то в X существует минимальный элемент x^*.*

Цорн (1906–1993)

Разумеется в утверждениях 4.1.4, 4.1.5 с равным успехом можно говорить о «наибольшем» и «максимальном» элементе, поскольку упорядочение типа $1, 2, \ldots$ всегда можно «перевернуть»: $\ldots, 2, 1$. Но тогда надо будет переопределять *полную упорядоченность*.

Использование **АС** в математических дисциплинах происходит повсеместно и, как правило, неосознанно. Каждый раз как только что-либо допускается по поводу бесконечных множеств, в замаскированной глубине обычно возникает аксиома выбора, без которой «рассыпается половина математики». Возьмем простейший инцидент.

---

[3] Сделать это конструктивно в общем случае невозможно. Никому еще не удалось вполне упорядочить отрезок $[0, 1]$, у которого при обычном отношении порядка $\geqslant$ у интервалов $(a, b) \subset [0, 1]$ нет наименьших элементов.

4.1.6. *Счетное семейство счетных множеств — счетно.*

◄ Факт 4.1.6 без AC недоказуем. Причем это не сразу бросается в глаза. По первому впечатлению схема доказательства (2.1),

$$\begin{array}{cccccccccc}
A_1 & \Rightarrow & a_{11} & \rightarrow & a_{12} & & a_{13} & \rightarrow & a_{14} & \dots \\
 & & & \swarrow & & \nearrow & & \swarrow & & \\
A_2 & \Rightarrow & a_{21} & & a_{22} & & a_{23} & & a_{24} & \dots \\
 & & \downarrow & \nearrow & & \swarrow & & & & \\
A_3 & \Rightarrow & a_{31} & & a_{32} & & a_{33} & & a_{34} & \dots \\
 & & & \swarrow & & & & & & \\
A_4 & \Rightarrow & a_{41} & & a_{42} & & a_{43} & & a_{44} & \dots \\
\vdots & & \downarrow & \dots & \dots & \dots & \dots & \dots & \dots & \dots
\end{array}, \qquad (4.3)$$

дает нужный результат без каких бы то ни было предположений. Но без AC не удается фиксировать таблицу (4.3), потому что из множества возможных нумераций *каждой* последовательности[4] A_i требуется выбрать *каждый раз* конкретную нумерацию, для чего нужна опора на аксиому выбора.

Другое дело, можно надеяться выйти из положения окольным путем. Однако никакая другая схема не работает, хотя это устанавливается уже не так просто, — но устанавливается. ►

Одного этого примера достаточно, чтобы оценить масштабы инфицированности математики. Исключение аксиомы выбора изымает из математического арсенала массу удобных и при-

Рисунки А. Фоменко

[4] Наличие таких нумераций гарантирует *счетность* последовательности.

вычных инструментов. Например, эквивалентность (ε, δ)-определения непрерывности определению с помощью сходимости последовательностей. Нелегитимны становятся: счетная аддитивность *меры Лебега*, существование базиса у любого векторного пространства и многое другое.

Как доказать, что объединение X счетного семейства множеств $X_j \subset [0, 1]$, $j = 1, 2, \ldots$, имеет меру нуль, если каждое X_j имеет меру нуль? Каждое X_j покрывается счетной системой интервалов суммарной длины, меньшей $\varepsilon/2^j$. В результате X оказывается покрытым системой интервалов суммарной длины, меньшей ε. Рассуждение, понятно, рассыпается, если не существует функции выбора, ставящей в соответствие каждому X_j подходящую систему интервалов. Вот такой бюрократизм.

4.2. Теорема Цермело и трансфинитная индукция

АС имеет много лиц. Одно из них — *теорема Цермело* 4.1.4.

Ядро доказательства *теоремы Цермело* образует простая идея. Если f — функция выбора на X, то процесс

$$x_0 = f(X), \quad x_1 = f(X - x_0), \quad x_2 = f(X - \{x_0, \quad x_1\}), \quad \ldots$$

дает полное упорядочение X. Слабым звеном здесь выглядит преодоление барьеров бесконечности. Первый такой барьер возникает по «завершении» построения счетного множества точек

$$x_0, x_1, x_2, \ldots .$$

Если X несчетно, приходится делать следующий шаг,

$$x_\omega = f(X - \{x_0, x_1, x_2, \ldots\}),$$

затем

$$x_{\omega+1} = f(X - \{x_0, x_1, x_2, \ldots, x_\omega\}),$$

и так далее, до исчерпания X. При этом «количество» шагов может быть сколь угодно велико по мощности. Последнее обстоятельство вызывает опасение, не застопорится ли процесс.

Однако в условиях аксиоматики, в которой бесконечности «могут быть пройдены до конца», трудно представить, как процесс может остановиться посередине[5].

Возможность полного упорядочения любого множества, играет принципиальную роль по разным причинам. В первую очередь, она исключает существование несоизмеримых мощностей.

Мощности множеств X, Y считаются равными, пишут $|X| = |Y|$, в томм случае, когда существует взаимно однозначное соответствие между X и Y; и $|X|$ полагается больше $|Y|$, пишут $|X| > |Y|$, в томм случае, когда существует взаимно однозначное соответствие между X и частью Y; соответственно определяется $|X| < |Y|$. Гипотетически можно было бы предположить существование множеств, имеющих несравнимые мощности. Но *теорема Цермело* как раз исключает такую возможность. Подробности в главе 5.

Помимо этого, полная упорядоченность дает основу для *трансфинитной индукции*, что для матанализа принципиально важно, ибо ограничение счетности шагов в обычной индукции не позволяет работать в океане континуальных наслоений. В трансфинитной же индукции общее число шагов может быть сколь угодно большим по мощности, что позволяет преодолевать многократные уходы индуктивного построения в бесконечность.

4.2.1. Трансфинитная индукция. *Пусть утверждение T справедливо для первого элемента вполне упорядоченного множества X и для всякого элемента $a \in X$, если оно справедливо для любого $x < a$. Тогда утверждение T справедливо для любого элемента множества X.*

◄ В противном случае существует подмножество $Z \subset X$ элементов X, для которых T не имеет места. Множество Z, как подмножество вполне упорядоченного множества X, имеет наименьший элемент $a \in Z$. Для всех

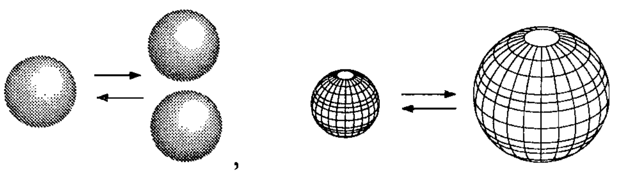
[5] Формальное доказательство обычно наполняется некоторым количеством деталей, чтобы труднее было возразить и проще — согласиться.

$x < a$ утверждение T справедливо, но тогда оно обязано быть справедливым и для a, откуда $a \notin Z$, что приводит к противоречию. ►

4.3. Парадокс Банаха—Тарского

Невинная с виду аксиома выбора знаменита «невероятными» следствиями. Вплоть до паранойи, как поначалу кажется.

4.3.1. Феномен Банаха—Тарского. *Шар $B \subset \mathbb{R}^3$ допускает разбиение на конечное число непересекающихся множеств $B_1, \dots, B_k$, из которых можно составить передвижением B_j, как твердых тел (перенос плюс поворот), либо два шара того же радиуса, либо шар удвоенного радиуса.*



Выглядит шокирующе, но в **ZFC** — это *теорема*[6].

И все-таки казус 4.3.1 — не катастрофа. Передвижение точек $x \in [0, 1]$ в точки $y = 2x$ тоже ведь преобразует $[0, 1]$ в отрезок $[0, 2]$. В *теореме* 4.3.1 это умопомрачительно обыгрывается.

Иногда для усиления эффекта говорят о возможности подходящего разрезания B на куски B_j, но это уже метафора. Для трезвой оценки результата существенно доказательство, без которого не видны причины, каковые весьма прозаичны. К тому же, в парадоксе помимо *аксиомы выбора* в большей степени виновата *«актуальная бесконечность»* (**Z5**).

О результатах типа 4.3.1 удобнее говорить, опираясь на понятие *изометричной разложимости*.

---

[6] *Banach S. and Tarski A.* // Found. Math. 1924. **6**. 244.

4.3.2. Определение. *Пусть* $\boldsymbol{G}$ — *группа изометрий на множестве* X. *Если существуют* $f_1, \dots, f_k \in \boldsymbol{G}$ *и разбиение* X *на конечное число непересекающихся множеств* $A_1, \dots, A_k$, *такие что* $f_1(A_1), \dots, f_k(A_k)$ *также не пересекаются и*

$$\bigcup_j f_j(A_j) = Y,$$

то X *и* Y *называют* ***изометрично разложимыми***, i***-разложимыми*** *либо* i***-эквивалентными***, $X \overset{i}{\sim} Y$.

Нетрудно убедиться, что «$\overset{i}{\sim}$» является отношением эквивалентности. *Парадокс Банаха—Тарского* может быть сформулирован как i*-эквивалентность* одного шара $B \subset \mathbb{R}^3$ и двух шаров. Кстати, если X i*-эквивалентно* множеству Y, состоящему из двух дубликатов X, то говорят, что X *парадоксально*, или *парадоксально разложимо*.

4.3.3. Лемма. *Если* $X_2 \subset X_1 \subset X_0$ *и множества* X_2 *и* X_0 *изометрично разложимы, то все три множества изометрично разложимы*[7].

◄ Пусть i*-разложимость* X_0 и X_2 обеспечивается разбиением X_0 на непересекающиеся множества $B_1, \dots, B_k$ и изометричными преобразованиями $f_j : B_j \to X_2$ с непересекающимися $f_1(B_1), \dots, f_k(B_k)$, и $\bigcup_j f_j(B_j) = X_2$.

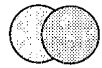
Та же конструкция $X_0 \supset X_1 \supset X_2 \supset X_3 \supset \dots$, что и в п. 2.2.2, приводит к кусочной изометрии

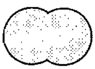
$$\psi(x) = \begin{cases} f_j(x), & \text{если} \quad x \in B_j \cap (X_{2k} \setminus X_{2k+1}), \\ x, & \text{если} \quad x \in X_{2k+1} \setminus X_{2k+2} \quad \text{или} \quad x \in \bigcap\limits_k^{\infty} X_k. \end{cases}$$ ►

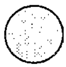
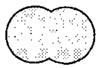
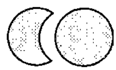
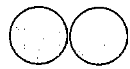
4.3.4. Следствие.

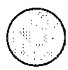
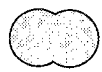
$$A_0 \overset{i}{\sim} B_1 \subset B_0, \quad B_0 \overset{i}{\sim} A_1 \subset A_0 \quad \Rightarrow \quad A_0 \overset{i}{\sim} B_0.$$

[7] Результат перекликается с леммой 2.2.2.

Результаты 4.3.3, 4.3.4 позволяют достаточно вольно обращаться с множествами — объединяя, вычитая, пересекая, вращая и передвигая их, — без потери свойства парадоксальной разложимости. Два шара, получившиеся из одного в *теореме Банаха—Тарского*, можно надвинуть друг на друга[8], ,

и объединить, , потому что

 $\subset$  $=$  $\subset$ ,

и по лемме 4.3.3 выходит  $\overset{i}{\sim}$  .

Поэтому шар B *i-эквивалентен* объединению любого числа шаров B, как угодно расположенных. А поскольку объединением большого числа шаров можно накрыть любое ограниченное множество X, внутри которого, если есть внутренняя точка, можно поместить достаточно малый шарик B, — получается, *лемма* 4.3.3,

$$B \subset X \subset nB, \quad B \overset{i}{\sim} nB \quad \Rightarrow \quad X \overset{i}{\sim} B,$$

что в принципе сразу доказывает следующие два факта, обобщающих *теорему* 4.3.1.

4.3.5. Теорема. *Любое множество $X \subset \mathbb{R}^3$, имеющее внутренние точки — парадоксально разложимо.*

4.3.6. Теорема. *Любые множества $X, Y \subset \mathbb{R}^3$, имеющие внутренние точки, — i-эквивалентны.*

Перейдем теперь к доказательству теоремы 4.3.1.

◄ Рассмотрим орбиты на сфере S. Напомним, точки $x, y \in S$ считаются принадлежащими одной орбите в томм случае, когда x переводится в y некоторым поворотом S. На каждой орбите, лежащей в S, выберем по одному элементу (*аксиома выбора*), и образуем из этих элементов множество $Z \subset S$. Если бы любая точка y любой орбиты достигалась единственным способом из подходящей

[8] Картинки плоские, но размерность подразумевается не менее трех.

точки $x \in Z$ — умножением x на поворот $h \in G$, — парадоксальное разбиение группы (2.11) порождало бы, в силу $\bigcup_{h\in G} hZ = S$, парадоксальное разбиение сферы S. Но тут имеется небольшая загвоздка. Каждому повороту $h \in G$ отвечают точки S, попадающие на ось вращения f или g и остающиеся некоторое время неподвижными, — что нарушает единственность. Множество Ω таких точек счетно, в силу счетности G. Исключая их из рассмотрения, имеем парадоксальное разбиение множества $S - \Omega = S \setminus \Omega$.

Покажем, что $S - \Omega \overset{i}{\sim} S$.

◁ Действительно, поскольку Ω счетно, найдется поворот σ, такой что $\Omega \cap \sigma(\Omega) = \varnothing$. Но тогда $\Theta = \bigcup_{k=1}^{\infty} \sigma^k(\Omega) \subset S - \Omega$. В результате $S - \Omega$ и S *i-эквивалентны*, поскольку $S - \Omega = \Theta + \overline{\Theta}$, а $\sigma^{-1}(\Theta) + \overline{\Theta} = S$, ибо

$$\sigma^{-1}(\Theta) = \bigcup_{k=0}^{\infty} \sigma^k(\Omega) = \Theta + \Omega. \quad \triangleright$$

Таким образом, $S - \Omega \overset{i}{\sim} S$, т. е. сфера *парадоксальна*. Отсюда сразу следует *парадоксальность* шара с выколотым центром[9]. Центр O легко подключается с помощью трюка из п. 2.5.1. Берем любую окружность $C \subset B$, проходящую через точку O, и ссылаясь на п. 2.5.1, замечаем $C - O \overset{i}{\sim} C$. ▶

Дополнительными ухищрениями можно добиться минимизации числа подмножеств $B_1, \ldots, B_k$ — и обойтись пятью, но это уже технический вопрос, не добавляющий философского содержания. Более принципиален частный результат 2.5.4, показывающий, что участие *аксиомы выбора* в *парадоксе Банаха—Тарского* малозначительно. Для существования *парадоксально разложимых* множеств главную роль играет актуальная бесконечность. При этом парадоксальные множества получаются конструктивно, ра́вно как и само разложение. Аксиома выбора лишь наводит лоск, включая в разряд парадоксальных наглядные множества типа шара.

Прототипом теоремы 4.3.1 послужил следующий результат[10].

[9] Парадоксальное разбиение сферы S, ограничивающей B, порождает разбиение лучей, выходящих из центра.

[10] *Hausdorff F.* // Math. Ann. 1914. **75**.

4.3.7. Парадокс Хаусдорфа. *Сфера в* $\mathbb{R}^3$ *после исключения счетного множества* Ω *может быть разбита на три конгруэнтных*[11] *множества* A, B, C, *таких что* $B \cup C$ *также конгруэнтно любому из* A, B, C.

Доказательство развивается тем же путем[12]. Но заключительного аккорда не хватает. Капля дегтя Ω портит результат. В итоге удваивается каждое множество A, B, C, — но разбивается все же не изящная сфера S, а кот в мешке $S \setminus \Omega$.

4.4. Вопросы правдоподобия

AC, как наиболее «жгучая» аксиома, слишком долго была в фокусе внимания, в связи с чем по отношению к сопутствующей проблематике накопилась эмоциональная усталость, и ажиотаж вокруг — несколько спал. Но «чудеса из окружения» остаются тем не менее животрепещущими, особенно при первом знакомстве, и заслуживают осмысления. К *парадоксу Банаха—Тарского* тут можно добавить *базисы Гамеля* (раздел 5.6) с огромной вереницей «неприятных» следствий.

Принципиальное отличие *аксиомы выбора* от остальных аксиом **ZF** заключается в ее неконструктивности. Вообще говоря,

Банах (1892–1945)

Тарский (1901–1983)

[11] Множества *конгруэнтны*, если совмещаются движением.

[12] Рассматривается частный случай двух трехмерных поворотов на углы π и $2\pi/3$ вокруг перпендикулярных осей.

неконструктивные явления допустимы, и во многих ситуациях не вызывают возражений. Вот простейший пример.

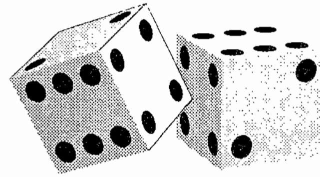
4.4.1. Задача. *Существуют ли иррациональные числа a и b, такие что a^b рационально?*

◀ Существуют. Неконструктивное доказательство таково. $\sqrt{2}^{\sqrt{2}}$ либо рационально, либо иррационально. В первом случае вопрос решен; во втором случае можно взять $a = \sqrt{2}^{\sqrt{2}}$, $b = \sqrt{2}$, и тогда $a^b = 2$. ▶

Конкретные a и b не указаны, но положительное решение задачи невзыскательному населению представляется удовлетворительным. Однако это задача иной природы — альтернативы подготовлены теорией вещественных чисел. Что касается **AC**, там картина иная. Без **AC**, например, невозможно утверждать существование *неизмеримых по Лебегу множеств*. И тут неконструктивность **AC** создает впечатление, что аксиома выбора ничего конкретного в проблему «измеримости» не вносит, кроме голословного заявления о возможных аномалиях. Хуже того, подспудно кажется, что неизмеримые множества либо существуют, либо нет, независимо от **AC**. И «если не существуют», то аксиому, получается, даже принимать нельзя. Либо можно — в силу как раз ее неконструктивности, но тогда мы попадаем в ситуацию, «когда ложь так же хороша, как правда», см. раздел 6.10.

Что же насчет правдоподобия **AC**, вопрос плохо поставлен, ибо проблема лежит в другой плоскости. Особенно если учесть независимость **AC** от **ZF** (см. разделы 3.6, 8.5, 8.7). Система **ZF** допускает, хотя это и противоречит интуиции, как принятие аксиомы выбора, так и ее отрицания. Сама по себе аксиома кажется правдоподобной, но это лишь стандартный путь заблуждения, ведущего иногда чудесным образом к открытию, — когда мы делаем общие выводы из наблюдения двух-трех примеров.

Поэтому о правдоподобии **AC** имеет смысл говорить лишь оценивая следствия принятия аксиомы. Да и то с поправкой на привычку интуиции делать выводы в неведомых ей областях.



Все «интуитивно неприятные» следствия **AC** на самом деле не так страшны и по большому счету не мешают привычному развитию математики. А отсутствие аксиомы выбора, кстати, также приводит к «интуитивно неприятным» последствиям, типа представления континуума в виде объединения счетного семейства счетных множеств. Не говоря о том, что без **AC** разваливается половина математики.

4.5. Аксиома детерминированности

Как бы там ни было, но *аксиома выбора* остается источником беспокойства и колоброжения. Среди многочисленных попыток модификации **AC** или ее замены особое место занимает *аксиома детерминированности*, декларирующая существование выигрывающей стратегии у одного из игроков в следующей игре G_X.

Пусть X — некоторое множество бесконечных последовательностей натуральных чисел. Игроки A и B последовательно выбирают числа $n_k \in \mathbb{N}$; A выбирает n_k для нечетных k, B — для четных, и если

$$\{n_1, n_2, n_3, \ldots\} \in X,$$

то выигрывает A, в противном случае — B. Игра G_X, ра́вно как и множество X, считается *детерминированной*, если один из игроков имеет выигрывающую стратегию.

4.5.1. Аксиома детерминированности AD. *Каково бы ни было множество X бесконечных последовательностей натуральных чисел, игра G_X детерминирована.*

Мы здесь избегаем подробностей, потому что говорим об аксиоме 4.5.1 не ради нее самой, а для прорисовки границ и среды, в которой находится система **ZF**. Детали можно найти в [9].

Детерминированными заведомо являются все конечные множества X и все — счетные. Сюда можно кое-что добавить. Например, детерминированность любых открытых множеств из *бэровского пространства*, т. е. пространства $\mathcal{N}$ всех бесконечных последовательностей натуральных чисел[13].

Рисунки А. Фоменко

С помощью аксиомы выбора существование недетерминированного множества X устанавливается, но без **AC** построить недетерминированное множество никому не удавалось, откуда делается бездоказательный пока вывод о непротиворечивости **AD** и **ZF**, разумеется, в предположении непротиворечивости **ZF**.

На вид **AD** несколько вычурна и несолидна, чтобы войти в круг аксиом **ZF**. Но тут виновата формулировка. В другой редакции, например, **AD** принимает вид вполне респектабельного обобщения на бесконечнокванторные формулы *закона исключенного третьего*, см. [9]. Кроме того, **AD** влечет за собой справедливость *счетной аксиомы выбора*, и тем самым «оставляет на месте» значительную часть наиболее употребительных математических результатов типа *счетной аддитивности меры Лебега*. Поэтому при замене **AC** на **AD** не все теряется.

[13] Топология *бэровского пространства* определяется системой бэровских интервалов — множеств $\mathcal{N}_\alpha$, в которые помимо последовательности α входят последовательности β, имеющие с α общее начало любой конечной длины.

В то же время присоединение **AD** к **ZF** дает массу благоприятных следствий. Вот, например, кое-что из списка удобных воздействий на континуум.

4.5.2. *В присутствии* **AD** *любое подмножество* $[0, 1]$:

- *измеримо по Лебегу*;
- *обладает свойством Бэра*;

а каждое несчетное множество содержит совершенное подмножество.

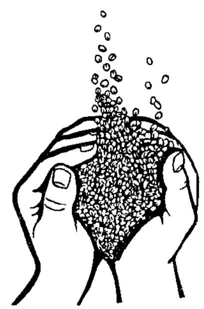
Таким образом, **AD** на фоне **AC** имеет серьезные конкурентные преимущества. Но топологи всегда будут голосовать против, потому что без **AC** половина их штата останется без работы.

Глава 5

Ординалы и кардиналы

Keep your eyes on the stars,
and your feet on the ground.

Theodore Roosevelt



Начало пути к дальней цели всегда уныло и безотрадно. Цель не видна, призрачна. Ландшафт противный — скука, рутина. Что для чего — не ясно. Да и нет уверенности, что имеет смысл идти в такую даль. Причем неясно «в какую».

5.1. Статус-кво

Широко известными до сих пор остаются лишь первые шаги *Кантора* в изучении бесконечности. Счетность, континуум, равномощность отрезка и квадрата, — вот стандартный набор явлений, расширяющих кругозор в области абстрагирования. Дальше дело идет туго. Навороты типа *кардинальной арифметики* воспринимаются большей частью как путь в никуда, что отчасти подтверждается практикой. Ибо потребности функционального анализа исчерпываются, как правило, *леммой Цорна*. Спрос на *трансфинитную индукцию* и *ординалы* особенно не ощущается. Да его и нет, если говорить о повседневных нуждах. Однако в наивысших математических достижениях «заумные» теоретико-множественные инструменты работают весьма эффективно. А уж опосредованное их присутствие обнаруживается повсюду, если присмотреться.

5.2. Кардинальная арифметика

О понятии *мощности множества* и его простейших свойствах уже говорилось в разделе 2.4, см. также определение 2.1.1.

Мощности, являющиеся классами эквивалентности множеств, называют также *кардинальными числами*, что несколько мистифицирует суть, но простительно из-за параллелей. Во-первых, мощности естественным образом линейно упорядочиваются [1], как обыкновенные числа. Во-вторых, для мощностей вводятся операции сложения и умножения, хотя тут аналогия уже хромает.

Сумма мощностей множеств X и Y определяется как мощность объединения $X \cup Y$, если $X \cap Y$ пусто, либо как мощность объединения непересекающихся эквивалентов [2] X, Y.

Произведение мощностей X и Y определяется как мощность декартова произведения $X \times Y$.

Наконец, *возведение в степень мощностей*, $|X|^{|Y|}$, определяется как мощность множества всех функций [3] $f : Y \to X$.

Кардинальная арифметика в свете данных определений напоминает обычную арифметику. Легко проверяется, что введенные сложение и умножение обладают коммутативностью, ассоциативностью и обычной для арифметики чисел дистрибутивностью, а возведение в степень также укладывается внешне в привычные рамки:

$$\left(|X|^{|Y|}\right)^{|Z|} = |X|^{|Y|\cdot|Z|}, \qquad \left(|X|\cdot|Y|\right)^{|Z|} = |X|^{|Z|}\cdot|Y|^{|Z|},$$
$$|X|^{|Y|+|Z|} = |X|^{|Y|}\cdot|X|^{|Z|}.$$

---

[1] Мощности множеств X, Y равны, $|X| = |Y|$, в томм случае, когда существует взаимно однозначное соответствие между X и Y; и $|X| > |Y|$, в томм случае, когда существует взаимно однозначное соответствие между X и частью Y; $|X| < |Y|$ определяется как $|Y| > |X|$.

[2] Например, $X \times \{1\}$ и $Y \times \{2\}$.

[3] Если множества X и Y конечны и содержат x и y элементов, соответственно, то $|X|^{|Y|}$ содержит x^y элементов. (?)

При этом *кардинальная арифметика* применительно к конечным множествам совпадает с арифметикой обычных чисел, но в целом — пестрит сюрпризами. Например[4],

$$\aleph_0 + n = \aleph_0, \quad \aleph_0 + \aleph_0 = \aleph_0, \quad \aleph_0 \times \aleph_0 = \aleph_0.$$

Многие соотношения между мощностями довольно легко устанавливаются с помощью арифметических выкладок вкупе с опорными фактами типа $\aleph_0 < \mathbf{c}$ ($\mathbf{c}$ — *мощность континуума*) или теорем 2.2.1, 2.4.9. Выкладка

$$\mathbf{c} \cdot \mathbf{c} = 2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0 + \aleph_0} = 2^{\aleph_0} = \mathbf{c}$$

означает равномощность прямой и плоскости. В том же ключе:

$$\mathbf{c}^{\aleph_0} = \left(2^{\aleph_0}\right)^{\aleph_0} = 2^{\aleph_0 + \aleph_0} = 2^{\aleph_0} = \mathbf{c},$$

а с учетом монотонности возведения в степень,

$$\mathbf{c} = 2^{\aleph_0} \leqslant {\aleph_0}^{\aleph_0} \leqslant \mathbf{c}^{\aleph_0} = \mathbf{c},$$

получается ${\aleph_0}^{\aleph_0} = \mathbf{c}$.

Но не все так просто. Кое-что не доказывается бесхитростными манипуляциями. Неясно, например, существует ли следующее после $\aleph_0$ кардинальное число $\aleph_1$? Оказывается, существует, но обоснование сопряжено с некоторой морокой[5]. *Гипотеза континуума*, кстати, заключена в предположении $\mathbf{c} = \aleph_1$. Недостаток аппаратных средств испытывают и другие довольно простые факты. Скажем, для бесконечных множеств

$$|X| + |Y| = |X| \cdot |Y| = \max\left(|X|, |Y|\right),$$

что легко проверяется на примерах, но в общем виде сразу не поддается обоснованию.

---

[4] Напомним, *мощность конечного множества* из n элементов полагается равной n. *Мощность счетного множества* обозначается как $\aleph_0$ (*алеф нуль*), *мощность континуума* — $\mathbf{c}$.

[5] См. следующий раздел.

5.3. Ординалы

Если с самого начала ориентироваться только на вполне упорядоченные множества, то можно многого добиться, не опираясь на аксиому выбора, а заодно и рассмотреть за ширмой понятия «мощности» более детальную картину. Соответствующий путь в общих чертах выглядит примерно так.

Линейно упорядоченные множества X, Y называются *подобными*, если существует взаимно однозначное соответствие f между X и Y, сохраняющее порядок,

$$a > b \leftrightarrow f(a) \succ f(b), \tag{5.1}$$

где $a, b \in X$; $>$, $\succ$ — отношения порядка в X, Y соответственно[6].

О двух *подобных* вполне упорядоченных множествах X, Y говорят, что они имеют одинаковый *порядковый тип*, или одинаковое *порядковое число*, и пишут

$$\|X\| = \|Y\|.$$

Порядковые числа конечных множеств отождествляются с натуральными числами.

Таким образом, *порядковые типы* — это классы эквивалентности, задаваемой отношением подобия. Их (классы) еще называют *трансфинитными числами*, или *ординалами*. Для них вводится отношение порядка:

$\|X\| > \|Y\|$ в томм случае, когда существует взаимно однозначное соответствие между Y и частью X. То есть ранжирование ординалов происходит по аналогии с мощностями, но с помощью более тонкого инструмента: вместо эквивалентности (взаимно однозначного соответствия) используется подобие, требующее дополнительно сохранения порядка (5.1).

Всякий элемент a вполне упорядоченного множества X определяет *начальный интервал* X как совокупность элементов $x < a$.

---

[6] Подобие уравнивает в правах не только множества, но и отношения порядка.

Очевидно, порядковые числа меньшие ξ взаимно однозначно отвечают *начальным интервалам* любого множества Z, имеющего порядковый тип ξ. Поэтому в качестве стандартного представителя *порядкового числа* ξ можно принять множество

$$\xi = \{\eta : \eta < \xi\}. \tag{5.2}$$

В результате каждый ординал оказывается множеством всех меньших ординалов. И если ординал определить именно так (через указанный выбор (5.2) стандартных множеств), то ***совокупность всех ординалов сама оказывается вполне упорядоченной (по включению),*** что вскрывает некоторые подспудные механизмы теории мощностей.

ДНК

Ординал $\omega = \{1, 2, \ldots\}$ является в то же время и порядковым числом множества всех натуральных чисел. Целесообразность фиксации стандартных множеств в порядковых типах понятна, ибо хочется иметь дело с множествами, а не классами эквивалентности. Но определять стандарты «сверху» неудобно, потому что тогда приходится танцевать от «множества всех вполне упорядоченных множеств», что недопустимо[7]. Идея (5.2) фиксации стандартных множеств «снизу» принадлежит *фон Нейману.*

Итак, ординалы, как множества всех меньших ординалов, могут быть развернуты в *трансфинитную последовательность*

$$1, 2, \ldots, \omega, \ldots, \tag{5.3}$$

[7] К любому вполне упорядоченному множеству можно добавить новый элемент, больший всех предыдущих, — поэтому «множество» всех ординалов, само по себе вполне упорядоченное, не существует, что называют *парадоксом Бурали—Форте.* О совокупности всех ординалов говорят как о *классе.*

каковую часто расписывают более подробно:

$$1,\ 2,\ \ldots,\ \omega,\ \omega+1,\ \omega+2,\ \ldots,\ \omega+\omega,\ \ldots,\ \omega+\omega+\omega,\ \ldots.$$

5.3.1. *Здесь перечисление исходного вполне упорядоченного множества X идет вначале счетным образом, и если на $1, 2, \ldots$ процесс не заканчивается, то в $X - \{1, 2, \ldots\}$ берется наименьший элемент, обозначаемый ω, и процедура счета продолжается: $\omega+1, \omega+2, \ldots$, где $\omega+k$ — порядковый тип множества $\{1, 2, \ldots, 1, 2, \ldots k.\}$. Если при бесконечном продолжении списка исчерпания X не происходит, то в*

$$X - \{1,\ 2,\ \ldots,\ \omega,\ \omega+1,\ \omega+2,\ \ldots\}$$

берется наименьший элемент, обозначаемый $\omega+\omega = \omega\cdot 2$, и процесс идет далее. На этом пути появляются элементы $\omega \cdot k$ вместе с $\omega \cdot k + l$. Если и они не исчерпывают X, берется наименьший из оставшихся элемент ω^2, и перечисление идет по опорным вехам $\omega^k + \ldots$. Затем возникает ω^ω и т. д.

5.3.2. *Ординал, не имеющий предыдущего ординала* (*см. п.* 1.3.5), *называется* ***предельным.***

Таковым является, например, ординал ω и вообще любой ординал в ряду ординалов, перед которым стоит «уходящее в бесконечность» многоточие.

Слева от любого $\xi \geqslant \omega$ имеется бесконечно много ординалов, но *бесконечные строго убывающие последовательности ординалов невозможны* (теорема 1.3.4). Природа феномена заключена в том, что, шагая влево от ω, приходится переступать через бесконечность, попадая на конкретное n.

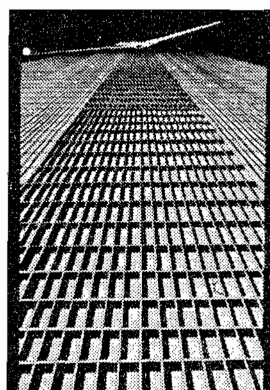
Каждому ординалу (порядковому числу) отвечает определенная мощность, поэтому из линейной упорядоченности порядковых чисел вытекает сравнимость мощностей любых двух *вполне упорядоченных* множеств — и сей вывод не опирается на аксиому выбора **AC**. Зато в сфере действия **AC** с учетом *теоремы Цермело* сравнимыми по мощности оказываются все множества, а не только вполне упорядоченные[8)].

Далее. Наименьший среди ординалов одинаковой мощности называется *кардиналом*. Кардиналами, в частности, являются все натуральные числа, счетный ординал ω — ему отвечает мощность $\aleph_0$, первый несчетный ординал ω_1 мощности $\aleph_1$ и т. д.[9)] В результате кардиналы выстраиваются в ряд алефов

$$\aleph_0, \aleph_1, \ldots, \aleph_\xi, \ldots . \tag{5.4}$$

Теорема Цермело гарантирует, что все множества могут быть вполне упорядочены, и потому все мощности входят в последовательность (5.4). В частности, мощность континуума $\mathfrak{c} = 2^{\aleph_0}$ присутствует в (5.4), но с каким $\aleph_\xi$ совпадает — принципиально не ясно. *Гипотеза континуума* $\mathfrak{c} = \aleph_1$, как оказалось, в рамках аксиоматики **ZFC** не решается, ни в ту ни в другую сторону, см. главу 7.

Описанная выше картина обычно излагается подробнее. Но рутина не способствует освоению предмета, хотя перемалывание



Рисунки А. Фоменко

[8)] Потому что любое множество оказывается эквивалентно какому-то вполне упорядоченному.

[9)] Существование следующего после $\aleph_0$ кардинального числа $\aleph_1$ вытекает, таким образом, из полной упорядоченности ординалов. У совокупности несчетных ординалов существует наименьший, его мощность и есть $\aleph_1$.

частностей иногда воспринимается как апогей учебного процесса. Понимание необходимости закрыть глаза на детали и всмотреться в каркас приходит потом. Отвлечься от мелочовки полезно и на первом этапе изучения предмета, чтобы двигаться затем в подходящем умонастроении. Так или иначе, но с подробностями «ординально-кардинальных» виражей можно ознакомиться по любому учебнику. В то же время надо иметь в виду, что сказанного выше достаточно для самостоятельного восполнения кажущихся пробелов изложения, а окаянные ординалы едва ли потребуются в жизни, если Господь не распорядится иначе. Но как бы там ни было, форточку в поле ординальной арифметики желательно держать открытой.

5.4. Ординальная арифметика

Арифметика ординалов иногда оказывается полезной.

Для *вполне упорядоченных множеств* X, Y сумма $X+Y$ определяется как *объединение* непересекающихся копий X, Y, в котором элементы X предшествуют элементам Y, а в произведении $X \cdot Y$ пары элементов сравниваются справа налево, сначала по Y-компоненте, а случае совпадения — по X-компоненте.

Обе операции ассоциативны, но не коммутативны: $\omega+k \neq \omega$, тогда как $k+\omega=\omega$. Аналогично: $\omega \cdot k \neq \omega$, но $k \cdot \omega = \omega$.

5.4.1. *Сумма $X+Y$ и произведение $X \cdot Y$ строго возрастают при возрастании второго аргумента, и нестрого — при возрастании первого.* $\triangleleft$

Возведение в степень для порядковых чисел определяется рекурсивно:

$$\alpha^0 = 1,$$

$$\alpha^{\xi+1} = \alpha^{\xi} \cdot \alpha,$$

$$\alpha^{\beta} = \sup\{\alpha^{\xi} : \xi < \beta\},$$

если β — *предельный ординал.*

Что касается сравнения ординалов, то здесь все достаточно просто, хотя местами громоздко. Опираться полезно на стандартную модель, которая, собственно, уже описывалась в п. 5.3.1.

Возрастающая (по включению) последовательность ординалов «с нуля» строится как «луч» в универсуме V по правилу

$$X_{k+1} = \sigma(X_k), \tag{5.5}$$

где $\sigma(X) = X \cup \{X\}$, что в начале пути дает «натуральный ряд»:

$$\varnothing,\ \{\varnothing\},\ \{\varnothing, \{\varnothing\}\},\ \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\},\ \dots . \tag{5.6}$$

Но механизма (5.5) не хватает, чтобы перепрыгнуть через многоточие и уйти в бесконечность. Поэтому совершается предельный переход

$$\{\varnothing,\ \{\varnothing\},\ \{\varnothing, \{\varnothing\}\},\ \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\},\ \dots\} = \omega, \tag{5.7}$$

далее снова включается итерирование (5.5), и так до нового многоточия и т. д.

Современное определение ординала с самого начала опирается на универсальное линейное упорядочение по «включению» $\in$. *Ординалом* называют *транзитивное множество*[10], все элементы которого *транзитивны*[11].

Картина (5.5)–(5.7), разумеется, более удобна в обозначениях п. 5.3.1, и если ее иметь перед глазами, то сравнивать между собой ординалы довольно легко. Вот два простых упражнения.

- Ординал

$$\sum_{k=0}^{k=N} \alpha^k \cdot \beta_k,$$

[10] Множество X называется *транзитивным*, если из $Z \in Y \in X$ следует $Z \in X$, т. е. если элементы элементов X являются элементами X. Множество $\{\{1,2\},\{2,3\}\}$ — не транзитивно, а $\{\{1,2\},\{2,3\},1,2,3\}$ — транзитивно.

[11] Разнообразие определений несколько смазывает картину, но причины многообразия очевидны. *Ординалы* — это классы подобных вполне упорядоченных множеств. Чтобы не носить за собой «классы», выбирают по стандартному представителю. Различие «стандартов» порождает разнообразие определений ординала.

где все $\beta_k < \alpha$, убывает, если ***лексикографически*** убывает набор (кортеж) ординалов

$$\{\beta_N, \beta_{N-1}, \ldots, \beta_1, \beta_0\},$$

т. е. убывает какой-то b_j, а слева от него все по-прежнему. Справа — как угодно, при условии[12] $\beta_k < \alpha$. **(?)**

- Если $\xi < \alpha \cdot \beta$, то $\xi = \alpha \cdot \rho + \tau$, где $\tau < \alpha$ и $\rho < \beta$. **(?)**

В заключение темы имеет смысл «пробежаться по опорным точкам».

- Любые два ординала либо совпадают, либо один принадлежит другому.
- Ординалы, за исключением $\alpha = \varnothing$, бывают двух видов: либо $\sigma(\alpha)$, либо предельные ординалы $\beta = \bigcup\limits_{\alpha<\beta} \alpha$.
- За любым ординалом α непосредственно следует $\sigma(\alpha)$, но любой предельный ординал не имеет непосредственного предшественника.
- Совокупность всех ординалов не является множеством.

5.5. Лемма Цорна и как она работает

Для приложений *лемма Цорна* 4.1.5[13] более удобна в эквивалентной формулировке, опирающейся на понятие *цепи*.

Если $\leqslant$ задает *частичный порядок* на X, то любое подмножество $Y \subset X$, *линейно упорядоченное* отношением $\leqslant$, называется *цепью* в X.

5.5.1. Лемма Цорна. *Если каждая цепь $Y \subset X$ имеет верхнюю грань в X, то в X существует хотя бы один максимальный элемент x^*, т. е. в X нет элементов $z > x^*$.*

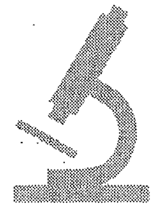
---

[12] Речь идет как бы о позиционной записи ординалов.

[13] *Если в частично упорядоченном множестве X любое частично упорядоченное подмножество ограничено снизу, то в X существует хотя бы один минимальный элемент x^** (п. 4.1.5).

◀ Возьмем любую цепь P:

$$x_0 \leqslant x_1 \leqslant x_2 \leqslant \ldots . \qquad (5.8)$$



Если ее верхняя грань максимальна в X — задача решена. Если нет — в множестве $\Gamma = \{z : z > x, x \in P\}$ строгих верхних границ фиксируем наименьший элемент в смысле *полной упорядоченности Цермело*[14], и добавим его к (5.8). Получится новая цепь, к ней применим тот же трюк и т. д. Вплоть до полного исчерпания Γ, если в середине пути не встретится требуемый максимальный элемент. ▶

Из приведенного доказательства видно, что *лемма Цорна* следует из *теоремы Цермело*, которая, в свою очередь, следует из *аксиомы выбора*. Чтобы замкнуть круг, убедимся в справедливости импликации:

5.5.2. *Лемма Цорна* → AC.

◀ На семействе $\Phi = \{X_\alpha : \alpha \in \mathcal{A}\}$ непустых множеств рассмотрим совокупность $\mathcal{P}$ всех частичных функций выбора $f(X_\alpha) \in X_\alpha$, определенных на непустых множествах $\Phi' \subset \Phi$. Считаем $f < g$, если f есть сужение g на более узкую область определения. При такой полуупорядоченности всякая цепь $\mathcal{Q} \subset \mathcal{P}$ имеет верхнюю грань. Следовательно, по *лемме Цорна* существует максимальная частичная функция выбора.

Такая функция должна быть определена на всем семействе Φ, иначе ее можно было бы продолжить на более широкое подмножество, поскольку любую частичную функцию выбора можно доопределить по крайней мере в одной точке вне $\mathrm{Dom}(f)$. ▶

Схема использования *леммы Цорна* в обосновании п. 5.5.2 универсальна и широко применяется. Рассмотрим классическое доказательство *теоремы Хана—Банаха*: «*Всякий линейный ограниченный функционал φ, определенный на линейном многообразии E_0 линейного нормированного пространства E, можно продолжить на все пространство, не увеличивая нормы φ*».

◀ Сначала устанавливается [3, т. 5], что любой функционал, определенный на области $\mathrm{Dom}(\varphi) \neq E$, можно приемлемо доопределить хотя бы в одной точке

[14] При полной упорядоченности наименьший элемент всегда есть у *любого* множества.

$z \notin \mathrm{Dom}(\varphi)$. Далее рассматриваются всевозможные продолжения функционалов, полуупорядоченных по включению областей определения. В совокупности таких продолжений любое упорядоченное подмножество ограничено сверху функционалом, определенным на объединении областей определения. Условия *леммы Цорна* выполнены — максимальный элемент существует, и он представляет искомый функционал φ^* — иначе φ^* можно было бы доопределить еще в одной точке, как отмечалось вначале. ►

Другой характерный пример: *существование базиса в любом линейном пространстве* E. Доказательство опять-таки упирается в ту же проблему. Если множество B линейно независимых векторов — не базис, то к нему всегда можно добавить какой-нибудь вектор $x \notin B$, не являющийся линейной комбинацией векторов из B. Вводя для линейно независимых множество полуупорядоченность $B_1 \leqslant B_2$, если $B_1 \subset B_2$, сводим задачу к существованию максимального элемента.

Абстрактно возникает прежняя ситуация. Размерность любого «небазиса» B можно увеличить на единичку, но как исчерпать все E, особенно в случае большой мощности? Тут *лемма Цорна* и спасает. И она работает внешне одинаково во многих сценариях. Вот примеры ее следствий.

- *Каждая булева алгебра имеет простой идеал*[15] [3, т. 8].
- *Если каждое конечное подмножество некоторого множества предложений* Σ *имеет модель, то* Σ *само имеет модель* (*теорема* 7.8.2).
- *Полуось* $(0, \infty)$ *может быть представлена в виде объединения двух непересекающихся множеств* X *и* Y, *замкнутых по сложе. лю.* **(?)**

Космическая роль последнего примера менее значительна. Для применения *леммы Цорна* здесь требуется малая толика изобретательности.

◄ Рассмотрим на $(0, \infty)$ множество пар (X, Y), где X, Y не пересекаются и каждое замкнуто по сложению[16]. Такое множество заведомо непусто. Такова, например, пара $X = \mathbb{Q}$, $Y = \sqrt{3} \cdot \mathbb{Q}$.

[15] *Теорема Тарского.*

[16] Замкнутость (инвариантность) X по сложению означает $x + y \in X$, если $x, y \in X$ Но тогда, понятно, из $x, y \in X$ следует также $\alpha x + \beta y \in X$ для любых натуральных α и β.

Подготавливая почву для применения *леммы Цорна*, необходимо сделать две вещи: ввести подходящий частичный порядок — здесь годится

$$(X, Y) < (X', Y') \quad \leftrightarrow \quad X \subset X',\ Y \subset Y',$$

и установить возможность расширения хотя бы одного из множеств X, Y, если $X \cup Y \neq (0, \infty)$. Тут надо слегка повозиться.

Итак, пусть X, Y замкнуты по сложению и $X \cup Y \neq (0, \infty)$. Присоединение точки $z \notin X \cup Y$ к X и замыкание по сложению раздувает X, добавляя элементы $\gamma z + x$ при всех $x \in X$ и натуральных γ. Если такое увеличение X не налезает на Y (не пересекается с Y), задача решена: X можно расширить. Если нет, то при некоторых $x^* \in X$ и $\alpha \in \mathbb{N}$ точка $\alpha z + x$ попадет в Y.

Если и Y нельзя расширить с помощью z, то, аналогично, при некоторых $y^* \in Y$ и $\beta \in \mathbb{N}$ точка $\beta z + y^*$ должна попасть в X. Иначе говоря,

$$\alpha z + x^* \in Y, \quad \beta z + y^* \in X \quad (x^* \in X, y^* \in Y),$$

откуда $\beta\alpha z + \beta x^* \in Y$ и $\beta\alpha z + \alpha y^* \in X$, но тогда элемент $\beta\alpha z + \beta x^* + \alpha y^*$ принадлежит одновременчо и X, и Y, что противоречит пустоте $X \cap Y$. ▶

В том же духе устанавливается следующий факт:

• ***Всякий частичный порядок может быть продолжен до линейного порядка на том же множестве.*** **(?)**

5.6. Базисы Гамеля

Базисы Гамеля — еще одно виртуальное чудо, базирующееся на *аксиоме выбора*. Неожиданность феномена — в непривычности с точки зрения каких-нибудь банаховых пространств [3, т. 5].

Итак, множество[17)] $H \subset \mathbb{R}$ называется *рационально независимым*, если для любого ***конечного*** набора ненулевых элементов $e_1, \ldots, e_n \subset H$ и любых рациональных чисел $r_1, \ldots, r_n$ сумма

$$\sum_{j=1}^{n} r_j e_j$$

обращается в нуль в томм случае, когда все r_j равны нулю. Например, множество $\{1, \sqrt{2}\}$ рационально независимо.

[17)] Из дальнейшего ясно, что выбор в качестве игрового поля действительной прямой $\mathbb{R}$ необязателен.

Легко видеть, что объединение рационально независимых множеств любой цепи (по вложению) — также рационально независимое множество. Поэтому из леммы Цорна вытекает *существование на $\mathbb{R}$ максимальных рационально независимых множеств*, каковые и называют *базисами Гамеля*.

Если H — *базис Гамеля*, то всякое ненулевое число x можно единственным образом представить в виде

$$x = \sum_{j<n} x_j e_j, \tag{5.9}$$

где $\{x_j : j < n\}$ — конечный набор рациональных коэффициентов, координат «вектора» x. В противном случае множество $H \cup \{x\}$ было бы рационально независимо вопреки максимальности H. А если бы у $x \neq 0$ было два представления

$$x = \sum_{e_j \in E} x_j e_j = \sum_{e_j \in E'} x'_j e_j,$$

где E, E' — конечные подмножества H, то множество $E \cap E'$, а значит и H, было бы рационально зависимо вразрез с определением *базиса Гамеля*.

Вот некоторые легко устанавливаемые факты.

- *Любой базис Гамеля имеет мощность* $\mathbf{c}$.
- *Существуют везде плотные и нигде не плотные базисы Гамеля.*
- *Измеримые базисы Гамеля имеют нулевую меру Лебега.*
- *Любое рационально независимое множество содержится в некотором базисе Гамеля.*

Таким образом, описанный инструмент превращает вещественную прямую в бесконечномерное пространство (!) с диковинными базисами, в которых любое число $x \in \mathbb{R} \setminus \{0\}$ имеет лишь ***конечное*** число ненулевых координат (!).

Феномен наличия *базисов Гамеля* знаменит парадоксальными на вид следствиями.

• Оказывается, существуют ***разрывные аддитивные функции*** $\varphi : \mathbb{R} \to \mathbb{R}$, характеризуемые условием

$$\varphi(x + y) = \varphi(x) + \varphi(y). \tag{5.10}$$

◄ Возьмем некоторое рационально независимое множество $\{e_1, \ldots, e_n\}$, и пусть $H \supset \{e_1, \ldots, e_n\}$ — *базис Гамеля*. Функция

$$\varphi(x) = x_1, \tag{5.11}$$

где x_1 — e_1-координата числа x в базисе H, удовлетворяет (5.10). ►

Помимо (5.11) аддитивными будут также функции

$$\varphi(x) = \sum_j \alpha_j x_j, \tag{5.12}$$

где суммирование идет по какому-нибудь конечному множеству индексов.

• Функции (5.11) и (5.12) неограниченны на любом сегменте, а их графики всюду плотны в $\mathbb{R}^2$. **(?)**

Все это странно выглядит на фоне обычного определения линейной функции с помощью характеристического свойства (5.10) при дополнительном требовании непрерывности $\varphi(\cdot)$. В этом случае решение $\varphi(x) = kx$ функционального уравнения (5.10) получается совсем просто:

◄ Из (5.10) следует $\varphi(px) = p\varphi(x)$ для любого целого p. Поэтому

$$\varphi\left(\frac{z}{p}\right) = \frac{1}{p}\varphi(z),$$

что получается в результате замены $z = px$. Это дает

$$\varphi\left(\frac{p}{q}z\right) = \frac{p}{q}\varphi(z),$$

т. е. $\varphi(x) = kx$, $k = \varphi(1)$, для всех рациональных x. Окончательный вывод о неизбежности $\varphi(x) = kx$ делается на основе предположения о непрерывности φ. ►

Пренебрежение непрерывностью извлекает на свет *«разрывные линейные функции»* (5.12).

• Функция $I(x) \equiv x$ может быть представлена как сумма двух периодических функций.

◄ Пусть $\{a, b\}$ рационально независимое двухэлементное множество, и $H \supset \{a, b\}$ — *базис Гамеля*. Любое число имеет разложение

$$x = x_a \cdot a + x_b \cdot b + \psi(x),$$

где у остатка $\psi(x)$ координаты при a и b нулевые. Поэтому

$$I(x) = f(x) + g(x),$$

где $f(x) = x_a \cdot a$ имеет период b, а $g(x) = x_b \cdot b + \psi(x)$ — период a. ►

Список интуитивных казусов подобного рода довольно велик.

• Существует такое множество $X \subset \mathbb{R}$, что *для любого* действительного x только конечное число множеств среди

$$X, \quad X + x, \quad X + 2x, \quad X + 3x, \quad \ldots$$

отличаются друг от друга.

• Существует такое множество $X \subset \mathbb{R}$, что *для любого* действительного $x \neq 0$ либо $X \subset X + x$, либо $X + x \subset X$, но $X + x \neq X$.

• $\mathbb{R} \setminus \{0\}$ является объединением счетного числа *базисов Гамеля* в томм случае, когда справедлива *гипотеза континуума*.

Однако *базисы Гамеля* являются не только источником экзотики. В [3, т. 1] описано, например, совсем короткое (благодаря использованию *базисов Гамеля*) решение *третьей проблемы Гильберта*[18], центральная идея которого заключена в приписывании любому многограннику M псевдовеса

$$p(M) = \sum_i l_i \varphi(\lambda_i),$$

[18] Равновеликие многоугольники равносоставлены, т. е. один из них можно разрезать на меньшие многоугольники и сложить другой. Равносоставлены ли равновеликие многогранники? В этом вопросе и заключалась *третья проблема Гильберта*, которую отрицательно решил М. Дэн в 1900 году.

где суммирование идет по всем ребрам длины l_i, λ_i — двугранный угол при i-м ребре, а φ — как раз «дикая» функция типа (5.11). Элементарные соображения показывают, что псевдовес куба отличается от псевдовеса тетраэдра, в то время как разрезание многогранника и перестановка частей не меняют псевдовеса, см. [3, т. 1, глава 8].

5 7. Теорема Гудстейна

Речь далее идет о сходимости итерационных процессов на поле $\mathbb{N}$, каковая легко устанавливается в $\mathbf{ZF}$, но не в *арифметике Пеано*. Таинственно известна на этом поприще *теорема Гудстейна*, утверждающая сходимость к нулю следующей процедуры.

Число n *дотошно записывается*[19] по основанию 2, затем 2 меняется на 3, полученное число уменьшается на единицу и *дотошно записывается* по основанию 3. Далее 3 меняется на основание 4, полученное число уменьшается на единицу и т. д.

5.7.1. Теорема. *При любом начальном n описанный* **процесс Гудстейна** *приходит в нуль за конечное число шагов $G(n) < \infty$.*

Вот несколько сверхъестественное, но очень простое доказательство. ◄ В *дотошной записи* любого натурального m по любому основанию k заменим k *ординалом* ω. В результате каждому m в дотошной записи по основанию k сопоставляется ординал[20]. При этом операция замены основания k не меняет

---

[19] *Дотошная запись* n по основанию k означает запись n в k-ичной системе

$$n = \sum a_i k^{b_i}$$

с последующей перезаписью всех показателей $b_i > k$ снова в k-ичной системе и т д. — до исчерпания показателей, превосходящих k. Например, $35 = 2^5 + 2 + 1 = 2^{2^2+1} + 2 + 1$.

[20] Например, $35_2 = 2^{2^2+1} + 2 + 1 \to \omega^{\omega^\omega+1} + \omega + 1$. Надо лишь помнить, что коэффициенты в ординальных полиномах необходимо писать справа, что связано со спецификой умножения ординалов,

$$\sum a_i k^{b_i} \quad \to \quad \sum \omega^{b_i} \cdot a_i .$$

соответствующего ординала, а вот вычитание единицы в *процессе Гудстейна* с последующей перезаписью полученного числа в той же системе — уменьшает «контролирующий» ординал. Поэтому числовому *процессу Гудстейна* отвечает убывающая последовательность ординалов, которая не может бесконечно убывать, ибо совокупность ординалов *вполне упорядочена*. Таким образом, процесс рано или поздно должен остановиться в нуле, когда вычесть единицу невозможно. ►

Прежде чем говорить о возможности или невозможности поставить это «потустороннее» рассуждение на рельсы обыкновенной арифметики, имеет смысл понаблюдать за процессом.

Начнем с $n = 2^2 = 4$. На следующем шаге имеем

$$3^3 - 1 = 26 = 2 \cdot 3^2 + 2 \cdot 3 + 2$$

Далее

$$\begin{aligned} 2 \cdot 4^2 + 2 \cdot 4 + 2 - 1 &= 41, \\ 2 \cdot 5^2 + 2 \cdot 5 + 1 - 1 &= 60, \\ 2 \cdot 6^2 + 2 \cdot 6 - 1 = 2 \cdot 6^2 + 6 + 5 &= 83, \\ 2 \cdot 7^2 + 7 + 5 - 1 &= 109, \end{aligned}$$

....

Числа в правом столбце неспешно растут, однако до умопомрачительных значений. Затем начинается падение (в час по чайной ложке — по 1 за шаг) и процесс скатывается в нуль через

$$G(4) = 3\left(2^{402653211} - 1\right) \text{ шагов. (!)}$$

О необычайности *процесса Гудстейна* свидетельствует стартовый взлет с заурядных n. Скажем, для $n = 21 = 2^{2^2} + 2^2 + 1$ подъем траектории долгое время идет при доминирующей роли слагаемого x^{x^x}, где x основание. Уже за первые два шага процедура взмывает в невидимую высь:

$$3^{3^3} + 3^3 = 7625597485014,$$

$$4^{4^4} + 4^4 - 1 = 4^{4^4} + 3 \cdot 4^3 + 3 \cdot 4^2 + 3 \cdot 4 + 3 > 2,5 \cdot 10^{154}.$$

На седьмом шаге ($x = 9$) возникает число большее $10^{350\,000\,000}$. Затем обилие цифр становится просто чудовищным. А потом ведь спускаться каждый раз надо будет всего лишь по единичке. Но даже этих $10^{350\,000\,000}$ шагов хватило бы, чтобы исходить Галактику вдоль и поперек.

От гигантских чисел, возникающих на ровном месте, конечно, дух захватывает, но подобные явления не новы. «Скандально известны» *функция Аккермана* [3, т. 6], трудоемкость определения *чисел Рамсея* [3, т. 10] и ряд других конструкций. Но *процесс Гудстейна* легко может выйти на первое место после небольшой модификации. Из доказательства теоремы 5.7.1 ясно, что *основание* каждый раз можно увеличивать не на единицу, а как угодно — сходимость к нулю не пострадает. Поэтому выбирать *основание* можно, например, итерируя *функцию Аккермана* — $A^k(2)$, где k — номер шага. Сходимость остается, но длина траектории зашкаливает, даже в масштабах Вселенной.

Теорема 5.7.1 [21] довольно проста и вовсе не обязана опираться на «сверхъестественные» *ординалы*. Вместо ω ставим букву x и переходим к рассмотрению полиномов, правда, многоэтажных. Далее «лексикографически» их упорядочиваем — и никаких проблем, если под рукой имеется *лемма Цорна* или *теорема* 1.3.4, что в данном случае одно и то же.

Суть дела легче всего пояснить на упрощенном варианте процесса. На k-м шаге число n записывается по некоторому основанию x_k, из него вычитается 1, полученное число снова переписывается в x_k-ичной системе, после чего x_k заменяется бо́льшим основанием x_{k+1} и т. д. Все то же самое, но без «дотошной записи» [22]. При этом ясно, что число в x_k-ичной записи

$$a_1 x_k^m + a_2 x_k^{m-1} + \ldots + a_m x_k + a_{m+1} \tag{5.13}$$

после вычитания 1 переходит в число, у которого в той же системе записи некоторый коэффициент a_i меньше на единицу, слева от a_i коэффициенты те же самые, а справа как-то меняются — неважно как. И если следить только за набором коэффициентов

$$\{a_1, a_2, \ldots, a_m, a_{m+1}\}, \tag{5.14}$$

т. е. за цифровой записью чисел, то при лексикографической упорядоченности векторов (5.14) они будут строго убывать на траекториях, независимо от чехарды *оснований*.

О полиномах (5.13), кстати, можно забыть и перейти к другой интерпретации. Скажем, (5.14) — деньги на счету фирмы в разных валютах, ранжированных

---

[21] *Goodstein R.* On the restricted ordinal theorem // The Journal of Symbolic Logic. 1944. 9 (2). 33–41.

[22] Каковая наводит тень на плетень, порождая многоэтажность типа x^{x^x}, и ретушируя тривиальную подоплеку.

по какому-то принципу. Фирма ежемесячно вносит абонентскую плату в любой на выбор валюте, а придурковатый банк ей за это каждый раз дает кредит в любом размере, но в меньшей по рангу валюте. Фирма, понятное дело, рано или поздно разорится, теоретически. Но практически банк прогорит раньше — будь они неладны *ординалы*.

Теорема Гудстейна стала знаменита по причине своей недоказуемости[23] в *арифметике Пеано* и тривиальности в **ZF**. Вся мощь **ZF** тут, разумеется, не нужна. Поэтому иногда говорят о доказуемости теоремы 5.7.1 в *арифметике второго порядка*, в которой допускается рассмотрение бесконечных множеств натуральных чисел и которая по сути представляет собой элементарный анализ, включающий непрерывные функции, вещественные числа, борелевские множества, счетные ординалы.

[23] Каковая более-менее ясна, но аккуратно была установлена в 1982 году (*Kirby L.*, *Paris J.* Accessible independence results for Peano arithmetic // Bull. London Math. Society. 1982. **14**: 285–293.

Глава 6

Вычислимость и доказуемость

Соприкоснувшись с вещью,
не прикрепляйся к ней.

Будда

Фиксируя взгляд на звездах, стоять приходится на земле. Так и **ZFC**, устремленная за горизонт, нуждается в реальной стартовой площадке и сдерживающих началах, работающих не только в потусторонних областях неизмеримых кардиналов и состоявшихся бесконечностей, но и здесь, в плену ограниченных фантазий.

6.1. Вычислимые функции

Русло **ZFC** во многом определяется из-за кулис *логикой первого порядка*. Но в изложении отправляться удобнее от вычислимых функций. Механизмы взаимодействия аксиом, разрешимость, доказуемость, истинность и противоречивость, — все это наглядно раскрывается в контексте алгоритмической работы с числовыми множествами. Соответствующая тематика довольно подробно и с доказательствами (вплоть до решения 10-*й проблемы Гильберта*) рассматривается в [3, т. 6], коротко и с другими акцентами — в [3, т. 10, 14], адаптированно к целям данного тома — в данной главе.

6.1.1. Определение. *Целочисленную функцию $f(n)$ целочисленного аргумента*[1] *называют вычислимой, если существует алгоритм, вычисляющий значения $f(n)$, но необязательно приводящий к результату.*

Алгоритм отождествляется с программой работы компьютера, представляющей собой запись *процесса вычислений* на некотором языке в некотором алфавите $\mathbb{A}$,

$$P = a_1 a_2 \dots a_N, \quad \text{все} \quad a_j \in \mathbb{A}. \tag{6.1}$$

Программа применяется к различным *входным словам*. Если входные и выходные данные кодируются числами, программа определяет *вычислимую функцию*.

В математической логике *теоремы полноты* как раз означают, что все выводимое *логически* выводится *синтаксически*, т. е. может быть адекватно описано на некотором языке программирования.

Многочисленные попытки определения вычислимой функции шли разными путями. *Тьюринг* (1936) ввел функции, вычислимые конечной машиной, известной ныне как *машина Тьюринга*. Примерно в то же время *Гёдель*, *Эрбран*, *Клини* ввели *рекурсивные функции*. Затем *Чёрч*, *Пост*, *Марков* — выделяли иные классы функций. Но все пути, как выяснилось, приводят к одному и тому же классу вычислимых функций.

Большинство населения чувствует возможность вычисления на компьютере всякой всячины, от бухгалтерских задач до распознавания речи и управления видео. Несколько меньшая часть людской массы понимает, как все это программируется и вкладывается в машину, а там по готовым рецептам предписания дезинтегрируются в машинные коды, и любая сложная задача рассыпается на простые арифметические и логические операции. Поэтому неудивительно, что все теоретически решаемые проблемы могут быть в принципе решены даже на архаичных счётах [4].

---

[1] Аргумент может быть векторным, $n = \{n_1, \dots, n_k\}$. Функцию в этом случае называют *k-местной*. *Включение запятых в алфавит с последующей перекодировкой цифрами позволяет все функции считать одноместными.*

Так что примитивизм *машины Тьюринга* — не такой уж сюрприз, хотя и нуждается в проработке деталей [3, т. 6].

Запись программы вычислений в виде (6.1) позволяет *все вычислимые функции перенумеровать*,

$$f_1(x), \dots, f_n(x), \dots . \tag{6.2}$$

Сначала перечисляются все программы из одной буквы, потом из двух, потом из трех и т. д.[2)]

6.1.2. Теорема. *Любая попытка ввести понятие вычислимой функции $f(n)$ так, чтобы она была определена при любом n,* — **обречена на провал**.

◀ С помощью нумерации (6.2) определим функцию

$$g(n) = f_n(n) + 1.$$

Она не вычислима, так как при $n = 1$ отличается от f_1, при $n = 2$ — от f_2, и т. д. С другой стороны, она вычислима в любом разумном смысле, поскольку к вычисляемому значению $f_n(n)$ всегда можно прибавить 1. ▶

Что касается существования *невычислимых функций*, то это ясно из того, что различных функций $f(n)$ имеется континуум, а вычислимых — счетное число (6.2). Конкретно указать невычислимую функцию тоже просто. Очевидно,

$$h(n) = \begin{cases} f_n(n) + 1, & \textit{если значение } f_n(n) \textit{ определено}, \\ 0, & \textit{если значение } f_n(n) \textit{ не определено} \end{cases} \tag{6.3}$$

невычислима. Для доказательства предположим противное, т. е. $h(n) = f_p(n)$ при некотором p. Но этого не может быть, так как $h(p) \neq f_p(p)$, если значение $f_p(p)$ определено, и $h(p)$ определено, если $f_p(p)$ не определено.

[2)] Нумеруются таким образом не функции, а программы, в результате чего каждая функция в перечислении (6.2) получает бесконечное множество номеров. Можно было бы, конечно, оставить в лексиконе только алгоритмы, но тогда в простых ситуациях типа $f(n) = n(n+1)/2$ пришлось бы говорить о конкретных программах.

6.2. Перечислимые и разрешимые множества

Множество ***перечислимо***, если существует *эффективная процедура*[3] порождения его элементов. Элементы перечислимого множества эффективно нумеруются — в порядке появления.

На практике часто используют эквивалентную дефиницию:

6.2.1. Определение. *Множество X перечислимо, если представляет собой область значений либо область определения вычислимой функции.*

◄ Это не сразу увязывается с предыдущим. Если X — область значений $f(n)$, то как порождать элементы? Процедура, похоже, «зависнет» на первом же n, при котором значение $f(n)$ не определено. Тем не менее пусть $P(n, m)$ обозначает реализацию m шагов работы программы по вычислению значения $f(n)$. Пары чисел (n, m) упорядочиваются стандартным образом (нумеруются вдоль стрелочек):

$$\left(\begin{array}{cccccccc}
(1,1) & \to & (1,2) & & (1,3) & \to & (1,4) & \dots \\
 & \swarrow & & \nearrow & & \swarrow & & \\
(2,1) & & (2,2) & & (2,3) & & (2,4) & \dots \\
\downarrow & \nearrow & & \swarrow & & & & \\
(3,1) & & (3,2) & & (3,3) & & (3,4) & \dots \\
 & \swarrow & & & & & & \\
(4,1) & & (4,2) & & (4,3) & & (4,4) & \dots \\
\downarrow & \dots & \dots & \dots & \dots & \dots & \dots & \dots
\end{array}\right), \qquad (6.4)$$

после чего программе дается возможность последовательно работать по m шагов, вычисляя $f(n)$, в избранном порядке. Понятно, все значения $f(n)$ будут рано или поздно перечислены.

В пояснении нуждается также другой момент. Определение содержит по сути в себе теорему: *область значений любой вычислимой функции всегда есть область определения другой вычислимой функции, и наоборот.* Устанавливается это с помощью той же процедуры $P(n, m)$, вычисляющей $f(n)$ на протяжении m шагов. Если вычисление $P(n, m)$ приводит к определенному результату, n объявляется значением функции $g(k)$, где k — номер пары (n, m). В результате область определения f становится областью значений g. Обратный трюк еще проще. ►

[3] Под *эффективной процедурой* подразумевается *эффективный алгоритм*, всегда дающий результат.

Множество называется ***разрешимым***, если существует *эффективная процедура* для выяснения принадлежности любого n этому множеству. Понятно, что множество X разрешимо, если его характеристическая функция,

$$\theta_X(x) = \begin{cases} 1, & \textit{если } x \in X; \\ 0, & \textit{в противном случае}, \end{cases} \tag{6.5}$$

вычислима.

6.2.2. Теорема Поста. *Для разрешимости X необходимо и достаточно, чтобы X и его дополнение $\overline{X}$ были перечислимы.*

◄ *Необходимость.* Если программа P определяет, принадлежит n множеству X или нет, то ее последовательная работа на $n = 1, 2, \dots$ разбивает натуральный ряд на два списка X и $\overline{X}$.

Достаточность. Если P перечисляет X, а Q — $\overline{X}$, то попеременная работа программ P и Q рано или поздно любое n внесет в один из списков X или $\overline{X}$, что дает разрешающий алгоритм. ►

6.2.3. Теорема. *Существует перечислимое, но неразрешимое множество положительных целых чисел.*

◄ Пусть $S_1, S_2, \dots$ — эффективное перечисление всех перечислимых множеств[4]. Заметим, если бы все S_n были разрешимы, то и все дополнения $\overline{S_n}$ входили бы в перечисление $S_1, S_2, \dots$ (теорема 6.2.2).

Образуем перечислимое множество D из тех номеров n, которые принадлежат S_n. Непустота D при любой организации перечисления $\{S_n\}$ следует хотя бы из того, что $S_q = \mathbb{N}$ при каком-то q. Очевидно, $n \in D$ равносильно любому из эквивалентных условий

$$n \in D \cap S_n \quad \leftrightarrow \quad n \in D \cup S_n.$$

Поэтому в случае $D = \overline{S_k}$ номеру k «некуда деваться». Если $k \in S_k$, то $k \in \overline{S_k} \cap S_k = \varnothing$, либо $k \notin S_k$, но тогда $k \notin \overline{S_k} \cup S_k = \mathbb{N}$. Это означает, что D не совпадает ни с одним $\overline{S_n}$, а значит (теорема 6.2.2) неразрешимо. ►

[4] Существование перечисления перечислимых множеств следует из наличия перечисления (6.2) вычислимых функций, области значений которых и являются множествами $S_1, S_2, \dots$.

Доказательство коротко, но отчасти головоломно, пожалуй. Теорема 6.2.3 — главный результат теории алгоритмов, от которого круги по воде расходятся очень далеко. Многочисленные «неразрешимости», в том числе знаменитые *теоремы Гёделя*, являются вариациями феномена 6.2.3.

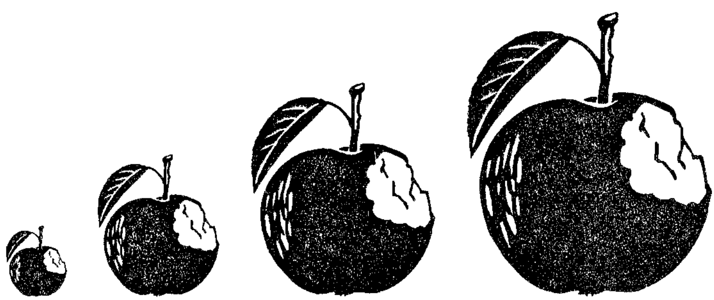
Аналогом разрешимого множества является понятие *эффективно вычислимой функции* $f(n)$, вычислимой, по определению, при любом n. В теории рекурсивных функций — это так называемые *общерекурсивные функции*.

6.2.4. Теорема. *Множество эффективно вычислимых функций неперечислимо — не может быть эффективно пронумеровано*[5].

◄ В данном случае работает та же конструкция, что и в доказательстве теоремы 6.1.2. Если существует нумерация f_n, то функция $g(n) = f_n(n) + 1$ заведомо эффективно вычислима, но не присутствует в списке $\{f_n\}$. ►

• Существуют вычислимые нигде не определенные функции. (?)

• Множество вычислимых функций, определенных хотя бы при одном n, перечислимо. (?)

$\varnothing$ 

6.3. Диофантовы множества

Диофантовы множества возникли и устоялись в контексте решения 10-*й проблемы Гильберта* о распознавании неразрешимых диофантовых уравнений.

[5] Соответственно множество разрешимых множеств неперечислимо.

Пусть $p(z_1, \ldots, z_n)$ — полином с целыми коэффициентами [6]. *Диофантовы уравнения*

$$p(z_1, \ldots, z_n) = 0 \qquad (6.6)$$

подразумевают решение в целых числах.

Часть переменных в (6.6) выделим в качестве параметров, и перепишем уравнение в виде

$$p(a, x) = 0, \qquad (6.7)$$

где $a = \{a_1, \ldots, a_k\}$ — векторный параметр, $x = \{x_1, \ldots, x_m\}$ — аргумент, причем все $a_i, x_j \in \mathbb{N}$.

6.3.1. Определение. *Множество A положительных векторов*

$$a = \{a_1, \ldots, a_k\}$$

называется диофантовым, если при любом $a \in A$ и только при $a \in A$ уравнение (6.7) *разрешимо в целых положительных $x_1, \ldots, x_m$.*

Требование положительности переменных, вообще говоря, не принципиально и связано с техническими причинами. Отрицательные коэффициенты полинома $p(a, x)$ при этом не исключены, например,

$$p(a, x) = x^2 - ax - 1, \quad p(a, x) = x_1^2 - x_1 x_2 - a_1 x_2 + a_2 x_1 x_2^7.$$

В тех случаях, когда, имея уравнение $p(a, x) = 0$ неразрешимое в целых положительных числах, необходимо указать уравнение неразрешимое в

$$\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\},$$

выручает известная *теорема Лагранжа*: *каждое целое положительное число является суммой четырех квадратов*. Поэтому замена $p(a, x) = 0$ на

$$p(a, 1 + p^2 + q^2 + r^2 + s^2) = 0$$

дает «то что надо». В случае $x = \{x_1, \ldots, x_m\}$ теорема Лагранжа применяется к каждому x_j отдельно.

Совсем просто дефиниция 6.3.1 трансформируется в интуитивно более ясную формулировку.

---

[6] Например, $p(z_1, z_2) = z_1^5 - 4z_1 z_2^3 + 32$.

6.3.2. Лемма. *Множество $A \subset \mathbb{N}$ диофантово в томм случае, когда оно является множеством положительных значений некоторого полинома $P(x_1, \ldots, x_k)$.*

◀ Действительно, если A — множество положительных значений полинома $P(x_1, \ldots, x_k)$, то уравнение

$$p(a, x_1, \ldots, x_k) = a - P(x_1, \ldots, x_k) = 0$$

определяет A как — диофантово.

Обратно. Пусть A — множество тех a, при которых

$$Q(a, x_1, \ldots, x_l) = 0$$

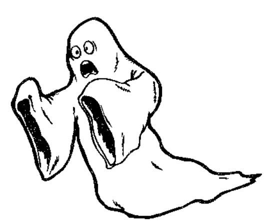
разрешимо. Тогда A — множество положительных значений полинома

$$a[1 - Q^2(a, x_1, \ldots, x_l)]. \quad ▶$$

На вид определение 6.3.1 весьма специфично, и кажется маловероятным, что диофантовыми будут сколько-нибудь интересные множества иной природы. Скажем, множество простых чисел или чисел, встречающихся в десятичной записи числа π. И до того как *Матиясевич* поставил в решении *десятой проблемы Гильберта* последнюю точку [14], мало кто на вопрос: «диофантово ли множество простых чисел?» — ответил бы: «да». Оказалось же, что:

6.3.3. Теорема. *Диофантовость множества равносильна перечислимости.*

Это был шок. Выяснилось, что существует полином, множество положительных значений которого в точности совпадает с множеством простых чисел[7].



Из теоремы 6.3.3 сразу следует отрицательное решение *десятой проблемы Гильберта*, ибо простой перевод на диофантов язык *теоремы* 6.2.3 приводит к следующему результату.

[7] Более того, его можно конкретно указать, см. [3, т. 6], где рассматриваемая здесь тематика достаточно подробно освещена.

6.3.4. Теорема. *Существует такой полином $P(x_1, \ldots, x_k)$, что разрешимость уравнения*

$$P(x_1, \ldots, x_k) - y = 0 \tag{6.8}$$

по $x_1, \ldots, x_k$ при некоторых положительных y — алгоритмически непроверяема.

Вот конкретная недоказуемая арифметическая формула:

$$\exists\, n, y\ \forall\, x_1, \ldots, x_k : U(n, y, x_1, \ldots, x_k) \neq 0, \tag{6.9}$$

где U — универсальный полином (см. далее).

Для перечислимых множеств, имеющих осмысленное описание[8] алгоритмического толка, всегда можно указать соответствующую программу вычислений. Точно так же можно указать соответствующий полином. Надлежащая техника описана в [3, т. 13].

6.4. Неполнота арифметики

Проблема доказуемости заключается в существовании *алгоритма*, ведущего от исходных посылок к заключениям (теоремам) и ограниченного в средствах использованием аксиом и правил вывода. Поскольку *доказательства*, как цепочки рассуждений, конечны, — все они, а значит, и теоремы — могут быть эффективно пересчитаны, т. е. алгоритмически пронумерованы.

6.4.1. Теорема. *Какова бы ни была непротиворечивая теория*[9], *содержащая арифметику, существует не имеющий положительных корней полином $Q(x_1, \ldots, x_k)$, отсутствие у которого целых положительных корней недоказуемо.*

◄ *Доказательство.* Пусть алгоритм $\mathscr{A}_1$ перечисляет разрешимые уравнения $P(x_1, \ldots, x_k) = 0$. Неперечисленными остаются утверждения

$$\forall\, x_1, \ldots, x_k : P(x_1, \ldots, x_k) \neq 0. \tag{6.10}$$

[8] Например, переборно-поисковое.

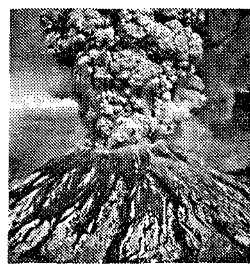
[9] *Теория T* называется *непротиворечивой*, если в T не могут быть доказаны две противоположные теоремы: A и «не A» (что обозначают как $\neg A$).

Если допустить, что при некоторой непротиворечивой системе аксиом все факты вида (6.10) доказуемы, это будет означать существование алгоритма $\mathscr{A}_2$, перечисляющего теоремы (6.10), т. е. перечисляющего дополнение к множеству $\mathbb{P}$ полиномов, перечисляемых алгоритмом $\mathscr{A}_1$. Отсюда по *теореме* 6.2.2 будет следовать разрешимость множества $\mathbb{P}$, что вступает в противоречие с отрицательным решением *десятой проблемы Гильберта*. ▶

Утверждение 6.4.1 представляет собой по сути усиление *теоремы Гёделя о неполноте*:

6.4.2. Теорема. *В любой непротиворечивой теории, содержащей арифметику, существует такое утверждение A, что ни A, ни его отрицание $(\neg A)$ — недоказуемы*[10].

Пируэт «ни A, ни $\neg A$» связан здесь с *неформализуемостью истины* в более-менее сложных теориях, в том числе — в арифметике[11]. Интуитивно желаема ведь формулировка о недоказуемости истинной теоремы. Но откуда ее взять, пока нет доказательства. Хитрость «ни A, ни $\neg A$» позволяет выйти из порочного круга, ибо по крайней мере одно из A и $\neg A$ истинно. Обратим внимание, что *теорема* 6.4.1 обходится без этой уловки.



6.5. Феномен неаксиоматизируемости

Одно из преимуществ *теоремы* 6.4.1 перед теоремой 6.4.2 состоит в возможности обойти стороной дебри математической логики. Об арифметике надо лишь знать, что ее язык достаточен для опи-

[10] ZFC включает в себя арифметику.

[11] В доказательстве *теоремы* 6.4.1 мы рассматривали пары

$$\exists\, x : P(x) = 0 \quad \text{и} \quad \forall\, x : P(x) \neq 0, \quad x = \{x_1, \ldots, x_n\},$$

в качестве A и $\neg A$.

сания диофантовых уравнений. Какова в точности аксиоматика рассматриваемой теории, даже не важно. Потому что результат 6.4.1 имеет абсолютный характер, утверждая недоказуемость как отсутствие *какого бы то ни было* алгоритма, устанавливающего истинную теорему $\forall\, xQ(x) \neq 0$, а не только алгоритма, стесненного выбором дозволенных аксиом и правил. И если бы существовала аксиоматика, в которой «все» доказывалось бы, существовал бы и надлежащий алгоритм, ибо в совокупности всех алгоритмов есть алгоритмы, реализующие поиск при любой мыслимой системе аксиом [12]. Поэтому:

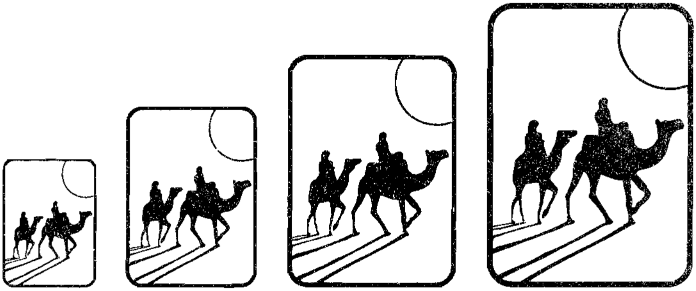
6.5.1. Теорема. *Арифметика неаксиоматизируема, даже при включении в систему бесконечного, но конструктивно (перечислимо) задаваемого множества аксиом.*

Именно по этой причине факт наличия недоказуемых истин на арифметическом поле сводится к существованию «абсолютно» неразрешимых множеств, что дает возможность обходиться без всех этих хлопот логико-языкового толка. Если бы решение вопроса зависело от аксиоматики, пришлось бы выделять алгоритмы, использующие только разрешенные средства. И тогда не избежать головной боли, связанной с необходимостью проникновения в логику и аксиоматику. Такая необходимость возникает при изучении конечно-аксиоматизируемых теорий [3, т. 6] либо даже арифметики, но при фокусировании интереса на узких подклассах теорем.

Следует заметить, что под арифметикой обычно подразумевается *арифметика Пеано*. Но есть еще *арифметика второго порядка*, приближающаяся к системе **ZFC**, а есть и *примитивная арифметика* **PA** на базе языка $L_0 = \{+,\ \times,\ =,\ \exists\,\}$, позволяющего лишь делать высказывания $\exists\, x : p(a, x) = 0$, но не

$$\forall\, x : p(a, x) \neq 0 \quad \text{или} \quad \neg\exists\, x : p(a, x) = 0.$$

[12] Как в списке *всех* текстов есть все ненаписанные пока романы.

$\varnothing$ 

Понятно, что такая арифметика непротиворечива, в смысле доказуемости всех истинных утверждений $\exists\, x : p(a, x) = 0$ (последовательной проверкой) и невозможности проверить — ложные. Но как только к L_0 добавляется $\forall$ либо $\neg$ — теория прыгает в другую крайность.

6.6. Непротиворечивость аксиоматики

Непротиворечивость аксиоматики внутри теории, как правило, недоказуема.

6.6.1. Вторая теорема Гёделя[13]**.** *Если теория T непротиворечива и содержит в себе арифметику, то непротиворечивость T недоказуема в T.*

Разумеется, *вторая теорема Гёделя* не исключает возможности решения проблемы за счет погружения теории в более вместительную систему. *Генцен*, например, установил непротиворечивость арифметики при опоре на *трансфинитную индукцию*, что представляет определенный интерес, ибо показывает ту «малость», каковой не хватает, чтобы свести концы с концами. Но гарантировать непротиворечивость *расширенной аксиоматики* опять-таки нельзя в силу *теоремы* 6.6.1, и необходим следующий акт расширения. Путь ведет в «никуда», и в этом смысле *проблема непротиворечивости* не имеет абсолютного решения.

[13] Набросок короткого доказательства есть в [3, т. 6].

Проблема решается для достаточно примитивных теорий. А в случае противоречивой аксиоматики может решаться сама собой из-за «короткого замыкания». Если же предположить непротиворечивость исходной системы, то не очень ясно, как можно *безопасно* добавлять новые аксиомы. Отталкиваясь, скажем, от любой стартовой совокупности, можно утверждать существование недоказуемой истины

$$\forall\, x > 0 : P(x) \neq 0. \tag{6.11}$$

Но конкретно указать полином $P(x)$ принципиально нельзя, иначе возникает противоречие с недоказуемостью (6.11). Поэтому здесь возможны лишь подозрения в правильности (6.11), и включение оной «истины» в аксиоматику чревато неприятностями. Интересно, что вместо (6.11) с действительно неразрешимым полиномом в аксиоматику может быть добавлено ложное утверждение «$\exists\, x > 0 : P(x) = 0$», причем *без ущерба для арифметики*. Как бы дико это ни казалось, но опровергнуть декларацию разрешимости неразрешимого полинома — принципиально невозможно. В результате в теории возникнет множество следствий *непроверяемой лжи* «$\exists\, x > 0 : P(x) = 0$», каковое не будет приходить в соприкосновение с теоремами обычной арифметики. Поэтому не из всякой лжи выводится что угодно, как иногда считается. Иная ложь *Всевидящего Ока* так же хороша, как правда.

6.7. Проблема арифметичности

Та простота, с которой выше была рассмотрена гёделевская тематика, существенно опирается на решение *десятой проблемы Гильберта* [14]. При этом кажется, что вполне можно было обойтись без диофантовых ухищрений, опираясь на *теорему* о существовании перечислимого, но неразрешимого множества. Вот как могло бы выглядеть доказательство *теоремы Гёделя* 6.4.2.

◄ *Перечислимое по определению множество S значений вычислимой функции $f(x)$ разрешимо, если существует алгоритм, определяющий по любому $y \in \mathbb{N}$, имеет решение уравнение $f(x) = y$ или нет.*

[14] Аппаратно несложное, но весьма трудоемкое [3, т. 6, гл. 5].

Из существования перечислимого, но неразрешимого множества (*теорема* 6.2.3) *вытекает, что последняя задача при некоторой функции* $f(x)$ *и некотором* y — *алгоритмически неразрешима. Это означает* **недоказуемость** *неразрешимости уравнения* $f(x) = y$ *при некоторых* y. ▶

На первый взгляд не очень ясно, чем это хуже. Вроде ничем. Худо-бедно обнаруживается недоказуемая теорема

$$\exists\, y \forall\, x : f(x) \neq y. \tag{6.12}$$

Но $f(x) = y$ вместо $P(x) = y$, вообще говоря, выбивает арифметическую почву из-под ног. За $f(x)$ стоит ведь какой-то алгоритм. Где гарантия, что он имеет арифметическую природу? Конечно, спасает теорема 6.3.3, но это сказка про белого бычка — опять всплывает диофантова кухня, без которой мы хотели обойтись. Как иначе показать, что (6.12) имеет арифметический характер? Оказывается, это длинная песня, связанная с регламентацией языка и привлечением математической логики. Таким образом, вычислимые функции вместо полиномов — возможны, но там приходится изгонять дьявола, прячущегося в деталях, что опять-таки по большому счету уводит в диофантовы дебри [15].

Конечно, любой опытный программист интуитивно чувствует арифметичность всего, что алгоритмизуемо. Но интуиция всегда опирается на небольшой круг примеров, попадающих в ее поле зрения. Кует обобщения, так сказать, из дырки от бублика. Но как быть с вычислениями, использующими сколь угодно длинные циклы? Там прямолинейное описание подходящих последовательностей связано с неограниченным количеством кванторов существования, что неарифметично. И едва ли интуиция чувствует, что любая сколь угодно длинная последовательность

$$\{x_1, \ldots, x_N\}$$

может быть закодирована всего тремя числами, см. [3, т. 6], что существенно для *арифметичности*.

[15] Хотя и не так далеко, как при решении 10-*й проблемы Гильберта*, поскольку надо лишь установить «полиномиальность» вычислимых функций, но не стоит обратная задача об исчерпании полиномами всех алгоритмов.

6.8. Универсальные функции

Эффективная нумерация (6.2) вычислимых функций $f_n(x)$ позволяет считать двуместную функцию

$$U(n, x) = f_n(x) \tag{6.13}$$

универсальной. Но здесь, вообще говоря, есть проблема, ибо поднятие индекса в данном случае не сводится к орфографии, а означает, что функция $U(n, x)$ *вычислима* теми же средствами, что и сами функции $f_n(x)$. Поэтому за внешней картиной (6.13) стоит некая внутренняя эквилибристика.

Машины Тьюринга, например, упорядочиваются, $M_1, M_2, \ldots$, после чего конструируется универсальная машина U, по номеру восстанавливающая и воспроизводящая работу M_j.

В рамках диофантовой тематики по эффективному перечислению всех перечислимых множеств $S_1, S_2, \ldots$ — строится универсальный полином

$$U(n; x_1, \ldots, x_k),$$

множество положительных значений которого при фиксированном n совпадает с S_n,

$$s \in S_n \leftrightarrow \exists\,(x_1, \ldots, x_k) : s = U(n; x_1, \ldots, x_k) > 0.$$

При этом обнаруживается сюрприз. Для всякого полинома

$$P(z_1, \ldots, z_N)$$

любой размерности и любой степени существует полином

$$U_n(x_1, \ldots, x_k)$$

фиксированной размерности и фиксированной степени, множество положительных значений которого в точности совпадает с множеством положительных значений полинома $P(z_1, \ldots, z_N)$.

Для алгоритмического подхода (6.1) естественна универсальная функция, нумерующая программы вычисления — по их длине.

Разумеется, способов нумерации программ — бесконечно много. Но иметь дело желательно с эффективно вычислимыми.

6.8.1. Определение. *Нумерация и функция $U(n, x)$ называются **гёделевскими**, если существует всюду определенная вычислимая функция $s(n)$, такая что для любой двуместной функции $f(n, x)$ справедливо*

$$f(n, x) = U(s(n), x).$$

Понятно, что:

6.8.2. Лемма. *Упорядочение программ вычисления по их длине дает гёделевскую нумерацию.*

Проблема останова. Функция $g(n) = U(n, n)+1$ не может быть **везде** доопределена, иначе ее доопределение $g^*(n)$ не будет входить в перечисление[16] (6.2). Разумеется, область определения некоторых вычислимых функций может быть расширена, иногда — вплоть до $\mathbb{N}$. Но пример функции $g(n)$ показывает справедливость следующего принципиального факта. *Среди вычислимых — существуют функции, область определения которых не может быть расширена до* $\mathbb{N}$.

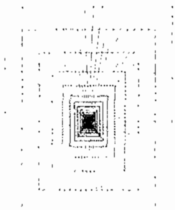
Одно из возможных следствий[17] — *неразрешимость проблемы останова.* Если бы существовал алгоритм, дающий ответ на вопрос, определено ли значение $f(n)$ для любых $f \in \mathbb{F}$ и $n \in \mathbb{N}$, то $f(n)$ всегда можно было бы всюду доопределить.

6.9. Теорема Райса

Бесконечный список алгоритмически неразрешимых проблем укладывается в общую формулировку:

[16] Будет отличаться от $f_n(x)$ в точке $x = n$ — из-за прибавления единицы, если значение $f_n(n)$ определено, либо из-за определенности значения $g^*(n)$ в случае неопределенности $f_n(n) =?$.

[17] Другое следствие — неразрешимость области определения функции $u(n)$. В противном случае $u(n)$ могла бы быть доопределена. В результате получается еще один пример перечислимого, но неразрешимого множества. Конструкция на данном этапе выглядит намного проще, чем доказательство теоремы 6.2.3.



6.9.1. Теорема Райса. *Любое нетривиальное свойство*[18] *вычислимых функций алгоритмически неразрешимо.*

Доказательство легко вытекает из следующего результата, удобного при рассмотрении многих вопросов о неразрешимости.

6.9.2. Теорема о неподвижной точке. *Какова бы ни была вычислимая всюду определенная функция $q(n)$, найдется n, при котором*

$$U(n, x) = U(q(n), x)$$

тождественно по x, где $U(n, x)$ — гёделевская универсальная функция.

Иначе говоря, никакой эффективно вычислимый «прыжок» от $f_n(x)$ к $f_{q(n)}(x)$ не гарантирует перехода к другой функции при любом n. Например, для любой гёделевской нумерации при каком-то n будет

$$f_n(x) = f_{n+1}(x)$$

тождественно по x.

◀ *Доказательство теоремы* 6.9.1. Пусть A — множество гёделевских номеров функций с заданным свойством. В силу нетривиальности «свойства» A непусто и $A \neq \mathbb{N}$. Если предположить разрешимость A, то всюду определенная функция

$$q(n) = \begin{cases} b, & \text{если } n \in A, \\ a, & \text{если } n \in \overline{A} \ \ (\overline{A} \text{ — дополнение } A), \end{cases} \tag{6.14}$$

где $a \in A$, $b \in \overline{A}$, — не имеет *неподвижной точки* в смысле теоремы 6.9.2. ▶

Таким образом, по программе $f_n(x)$ невозможно в общем случае определить, обладает или не обладает вычисляемая функция тем или иным свойством. Алгоритмически неразрешимыми оказываются, в частности, проблемы выяснения:

---

[18] Свойство считается нетривиальным, если имеются функции, обладающие этим свойством, и — не обладающие.

- *определена ли функция хотя бы на одном входе*[19];
- *определена ли функция только на одном входе*[20];
- *конечности или бесконечности множества значений* $f(x)$, *а также множества решений* $f(x) = 0$;
- *периодичности, ограниченности, порядка роста* $f(x)$.

6.10. Когда ложь так же хороша, как правда

На возможности принятия ложных аксиом, о чем уже говорилось в разделе 6.6, имеет смысл задержаться, потому что это принципиальный вопрос. Речь идет о *неформализуемости истины* в примитивной арифметике **PA**[21] и в любой более широкой теории, включающей **PA**. Проблема в том, что в **PA** принципиально невозможно определить истинность всех *замкнутых формул*. Примером такой формулы является

$$\forall\, x > 0 : P(x) \neq 0, \tag{6.15}$$

где P — некоторый полином. Существование подходящего полинома, для которого выполняется, но не доказывается (6.15), вытекает из *теоремы* 6.3.4, которая, разумеется, неконструктивна.

Насчет существования непроверяемой формулы (6.15) мы идем по второму кругу, но в данном случае акцент иной. При изучении *теорий* и *моделей* (глава 7) важную роль играет понятие *непротиворечивости*. Так вот, в условиях *неформализуемости истины* о противоречивости или непротиворечивости нет даже возможности говорить. Отрицание (6.15)

$$\exists\, x > 0 : P(x) = 0 \tag{6.16}$$

столь же «законно», как и (6.15), ибо ни то ни другое не проверяется (не доказывается). Причем «не доказывается» абсолютно —

[19] Множество номеров таких функций неразрешимо, — но перечислимо.

[20] Множество таких функций не только неразрешимо, но и неперечислимо.

[21] На базе языка $L_0 = \{+,\ \times,\ =,\ \exists\}$.

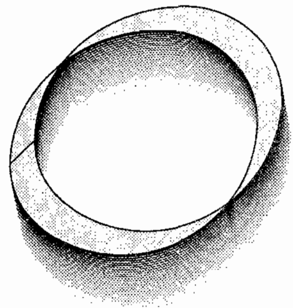
никакой алгоритм не в состоянии проверить, какая из формул (6.15), (6.16) верна. Поэтому к любой непротиворечивой аксиоматике совершенно безболезненно можно добавить любую (но только одну) из формул (6.15), (6.16), которые противоречат друг другу, и одна из них заведомо неправильна, но это может быть ясно только *Всевидящему Оку*.

Глава 7

Модели и теории

Music is the voice that tells us that
the human race is greater than it knows.

Napoleon Bonaparte

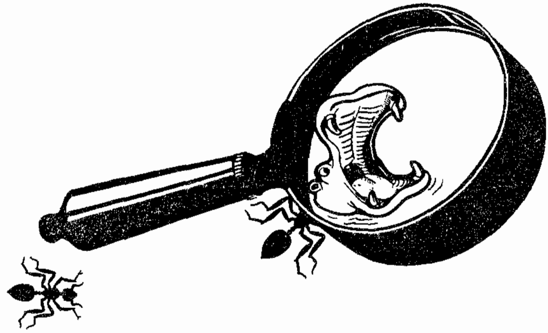


Матлогика является областью человеческой деятельности, и потому в меру размыта, сопровождается недосмотрами и ляпсусами. Как бы ни хотелось лучше, получается «как всегда». Но в этом нет ничего страшного. Потому что достоверность научных дисциплин гарантируется не безошибочностью деталей, а слаженностью течений мысли и скоординированностью виртуальных моделей между собой, не говоря о корреляциях с общепринятой, хотя и выдуманной, картиной мира.

Изложение рассчитано на тех, кто уже поднахватался, там и сям.

7.1. Логика первого порядка

Матлогика в теории множеств играет важную роль, которая под определенным углом зрения почти незаметна. Примерно как WINDOWS для MATLAB-а. Но по мере приближения к пограничным вопросам о «пределах возможного» логика выдвигается на авансцену в качестве первой скрипки. Так или иначе, допустимые границы использования кванторов, связок и переменных — влияют на происходящее, и нуждаются в уточнениях. Бо́льших или меньших в зависимости от преследуемых целей.



По отношению к другим математическим дисциплинам *матлогика* находится в особом положении по части строгости и формализации. Здесь требуется повышенное внимание к деталям и определенная щепетильность, без которых предмет теряет лицо. При этом техническая сторона дела на 90 % представляет собой скучную рутину, и до жемчужин тяжело добраться. В этих условиях нелегко профессионально овладеть предметом без хорошего учебника. Для начала можно рекомендовать [5, ч. 2], но надо иметь в виду, что достичь высокой квалификации с помощью одной книги обычно не удается, и тут многое зависит уже от индивидуальных устремлений.

С другой стороны, чтобы слушать музыку, необязательно умение играть на скрипке. Поэтому при отсутствии узкопрофессиональных амбиций возможен более экономный путь частичного проникновения в суть дела. Многое остается невидимым, но все же сохраняется возможность размышлять об основаниях математики. Или хотя бы делать вид, что, как ни странно, тоже дает эффект. Причем не меньший, потому что в условиях совершенной навигации перестаешь ориентироваться самостоятельно[1]. Взгляд на математическую логику поверх аппаратных премудростей см. в [3, т. 6].

Итак, в *логике первого порядка* кванторам $\forall$ и $\exists$ положено действовать на данном множестве X переменных. *Логика второго*

[1] Разумеется, можно привести тысячу контраргументов.

порядка разрешает одному из кванторов действовать на подмножествах X и на функциях. *Логика третьего порядка* допускает использование кванторов по множествам функций и т. д. Некоторое хождение имеет *слабая логика второго порядка*, позволяющая использовать кванторы по конечным подмножествам X и по натуральным числам. Все это разнообразие форматов влечет за собой фундаментальные отличия в результатах.

Логика первого порядка в принципе достаточна для описания почти всей математики и на общем фоне выделяется своеобразными свойствами (*теоремы полноты*, *компактности*, *Лёвенгейма—Сколема*, см. далее), каковые в логиках более высокого порядка не имеют места. Тезис насчет «всей математики», конечно, несколько шаток. Одна из аксиом *полной группы*, например, утверждает $\forall\, n \in \mathbb{N} \forall\, y \,\exists\, x : nx = y$, что не укладывается в *логику первого порядка*, ибо первый квантор действует на множестве натуральных чисел. Однако эту аксиому можно заменить бесконечным списком аксиом,

$$\forall\, y \,\exists\, x : 2x = y, \quad \forall\, y \,\exists\, x : 3x = y, \quad \ldots,$$

возвращаясь в лоно «первого порядка». Но вот в определении периодической группы $\forall\, x \exists\, n \in \mathbb{N} : nx = 1$ уйти от обращения к натуральному ряду не удается даже с помощью бесконечного списка формул. Тогда, конечно, можно вспомнить, что теория групп, как и вся «остальная математика», погружена в **ZFC**, и присовокупить к рассматриваемой аксиоматике постулаты теории множеств, теряя суверенитет и размывая автономный фундамент, чего самостийные дисциплины стараются избегать.

Формулами *первого порядка* не выражаются также понятия конечности и счетности. В определении счетности X приходится говорить о существовании *биекции*[2] между X и натуральным рядом. Та же проблема возникает и для *конечности множества по Дедекинду* как множества, которое не может быть взаимно однозначно отображено на *собственное подмножество*[3].

---

[2] Взаимно однозначного соответствия.

[3] Подмножество Y множества X называется *собственным*, если $Y \neq X$.

В другом варианте определения конечности[4] «$\exists\, n : |X| = n$» множество биекций рассматривать нет необходимости, но требуется (вроде бы) предварительное введение натурального ряда, от чего избавляет замечание *Тарского*:

7.1.1. *Множество X конечно в смысле «$\exists\, n : |X| = n$» в томм случае, когда любое непустое множество $Y \subset 2^X$ имеет максимальный элемент по включению*[5].

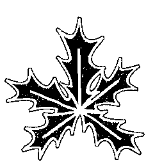
Трюк позволяет обойтись без «паровоза» $\mathbb{N}$, зато приходится иметь дело с весьма скользким (см. далее) в **ZF** «понятием множества всех подмножеств» 2^X, которое по туманности корней не уступает натуральному ряду. Если говорить точнее, то *проблема конечности* фокусируется в утверждение:

7.1.2. *В логике первого порядка не существует множества замкнутых формул, которые были бы истинны во всех конечных моделях и только в них (см. теорему* 7.8.2).

При этом в *логике второго порядка* «фильтр конечности» устанавливается одной формулой:

$$\forall\, f(\forall\, x\, \forall\, y(f(x) = f(y) \to x = y) \to \forall\, x\, \exists\, z(x = f(z))),$$

которая утверждает, что всякая *инъекция* является *сюръекцией*, но тут задействован квантор $\forall$ по *функциональной переменной* f, что в логике первого порядка не допускается.

[4] Множество, конечное в смысле $\exists\, n : |Z| = n$, *конечно по Дедекинду*. Для обратной импликации требуется опора на *аксиому выбора*.

[5] Если X бесконечно, то подмножество $Y \subset 2^X$ конечных подмножеств $Z \subset X$ (в смысле $\exists\, n : |Z| = n$) не имеет $\subset$-максимального элемента.

7.2. Теории и модели

Если не оговорено противное, речь далее идет о *теориях* и *моделях первого порядка*, т. е. о системах в операционной среде *логики первого порядка*. Алфавит сигнатуры[6)] предполагается счетным, хотя в большинстве случаев это несущественно.

7.2.1. *Теорией T в языке (сигнатуре) L называют всякое множество предложений, содержащее* **все** *предложения, которые из данного множества семантически следуют. Любое множество предложений G превращается в теорию $T \supset G$ после его замыкания по допустимым операциям, т. е. $A \in T$, если $T \models A$.*

Семантическое следование $T \models A$ означает, что *A истинно во всех интерпретациях множества предложений T*. Иными словами, с точки зрения определения никакого следования нет, есть декларация «во всех интерпретациях». Тем не менее в случае $T \models A$ говорят о «логическом» следовании, что выглядит загадочно, но имеет свой резон, см. далее. Есть также другая операция вывода $\vdash$, которая означает *синтаксическое следование* на базе формализованного алгоритмического вывода. В условиях *полноты исчисления предикатов* одно совпадает с другим, опять-таки см. далее.

7.2.2. *Теория T называется* **полной**, *если любая замкнутая формула f либо сама, либо ее отрицание $\neg f$ принадлежит T.*

7.2.3. *Множеством аксиом теории T называется всякое ее собственное перечислимое подмножество $\mathscr{P} \subset T$, такое что для каждого предложения $A \in T$ существует вывод $\mathscr{P} \vdash A$. Если существует конечное множество аксиом, T называется конечно аксиоматизируемой.*

---

6) Напомним, *сигнатурой* языка называют предметную часть алфавита, которая включает *константы языка*, *функциональные* и *предикатные* символы. *Предикаты* — это отношения или *характеристические функции этих отношений*. Последнее принимается далее в качестве определения.

Теория групп *аксиоматизируема*, а теория полей характеристики нуль[7] — нет. *Примитивная арифметика* неаксиоматизируема, равно как и все теории, содержащие в себе эту «мину».

7.2.4. *Моделью M теории T называется* ***интерпретация****, в которой истинны все формулы (теоремы) T, т. е. $M \models A$ для всех теорем $A \in T$.*

Интерпретация $\mathcal{M}$ языка L — есть преобразование φ множества *C констант языка* в некоторое множество X, сопоставляющее функциональным символам f над C — функции f_φ над X, предикатным символам R отношения R_φ. В интерпретации обычной арифметики — $\mathcal{M}$ есть $\mathbb{N}$ плюс сложение и умножение натуральных чисел, сопоставляемое функциональным символам $+$ и $\times$. Чтобы интерпретация стала моделью, необходима истинность в ней всех теорем арифметики, но с этим как раз проблема (глава 6).

Пониманию существа дела способствуют примеры.

7.2.5. Теория групп. *Язык $L = \{\cdot,\ ^{-1},\ e\}$ включает функциональные символы «$\cdot$», «$^{-1}$» и константу «e». Система аксиом*[8]:

$$\begin{aligned}
&\forall x\, \forall y\, \forall z : x \cdot (y \cdot z) = (x \cdot y) \cdot z, \\
&\forall x : e \cdot x = x \cdot e = x, \\
&\forall x : (x \cdot x^{-1} = e) \wedge (x^{-1} \cdot x = e).
\end{aligned} \tag{7.1}$$

---

[7] *Характеристика поля* является порядком единицы аддитивной группы поля, если порядок конечен, и считается равной нулю, если порядок бесконечен [3, т 8]

[8] Аксиомы равенства

$$\forall x : x = x, \quad \forall x\, \forall y : x = y \to y = x \quad \text{и др.},$$

как обычно, подразумеваются. Что касается последней аксиомы (7.1), то она может быть заменена на

$$\forall x\, \exists z : (x \cdot z = e) \wedge (z \cdot x = e),$$

что позволяет сократить алфавит L до $L' = \{\cdot, e\}$ за счет использования квантора существования. И наоборот, расширение языка L' добавлением операции «$^{-1}$» избавляет от необходимости использования квантора $\exists$, что иллюстрирует один из приемов *элиминации кванторов*, каковая имеет целью переход к эквивалентным *бескванторным формулам*.

Моделями служат группы. Группа трехмерных поворотов, например, или перестановок, или невырожденных матриц. Теория определяет лишь взаимодействие букв языка, — грамматику. Что такое «$\cdot$», «$^{-1}$», «e», — вопрос, не имеющий ответа. Что такое «$\cdot$»? Нечто, что работает, как указано выше. Поэтому ядро всякой теории образуют глаголы, действия. Вместо предметных существительных заготовлены *имена*: «x», «y»... Модели наполняют «смысловой вакуум», и по ним удобно судить о теории.

7.2.6. Теория частично упорядоченных множеств. *Язык* $L = \{\leqslant\}$ *состоит всего лишь из одного двухместного предиката* $\leqslant$. *Система аксиом*:

$$\begin{aligned} &\forall x : x \leqslant x, \\ &\forall x\, \forall y : (x \leqslant y \wedge y \leqslant x \to x = y), \\ &\forall x\, \forall y\, \forall z : (x \leqslant y \wedge y \leqslant z \to x \leqslant z). \end{aligned} \tag{7.2}$$

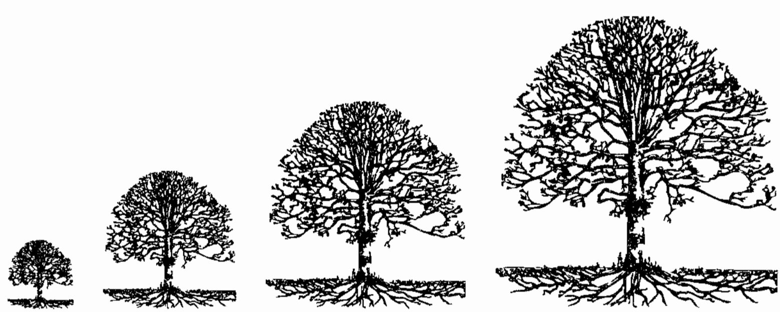
Моделями здесь служат те или иные множества с теми или иными конкретизациями отношения $\leqslant$. Банаховы пространства, полуупорядоченные некоторым конусом, конечные множества целочисленных векторов при *лексикографическом порядке* и т. п.

Добавление к (7.2) аксиомы

$$\forall x\, \forall y : (x \leqslant y \vee y \leqslant x)$$

образует теорию *линейно упорядоченных множеств*.

$\varnothing$



7.3. Семантика и формализм

Теории возникают обычно из попыток абстрагироваться от конкретных интерпретаций $\mathcal{M}$ языка L, или структур[9] над L. Иногда теорией объявляют совокупность $\mathrm{Tr}(\mathcal{M})$ всех формул, истинных в $\mathcal{M}$. Довольно часто — это путь в никуда с точки зрения контроля за истинностью. Причем именно по этому пути идет большинство математических дисциплин.

Дело в том, что очертить множество истинных формул в $\mathcal{M}$, как правило, невозможно (принципиально). Поэтому декларация $T = \mathrm{Tr}(\mathcal{M})$ во многих случаях голословна[10].

Именно такова картина в арифметике при обычной интерпретации сигнатуры

$$L = \{+, \times, =\}.$$

Ситуация даже хуже. Во-первых, не решается вопрос о принадлежности теории некоторых формул (раздел 6.4). Во-вторых, неясна непротиворечивость (раздел 6.6). В-третьих, при любой уточняющей аксиоматике за бортом остается масса верных арифметических утверждений (разделы 6.4, 6.5).

Вернемся назад. *Интерпретация* (равносильно: *структура*) $\mathcal{M}$ языка L представляет собой объединение:

- *множества* X (*универсума структуры*),
- *множества* k_j*-арных функций* $\{f_j : X^{k_j} \to X\}$,
- *множества отношений* $\{R_j \subset X^{l_j}\}$,
- *множества выделенных элементов*[11] $\{c_j \in X\}$.

---

[9] Здесь приходится говорить об интерпретациях (структурах) языка L, а не о моделях, ибо с позиций определения 7.2.4, чтобы говорить о модели, надо иметь сначала теорию, а не наоборот.

[10] Не говоря о трудностях заточения $\mathrm{Tr}(\mathcal{M})$ в рамки определения 7.2.1, ибо там требуется семантическая замкнутость совокупности $\mathrm{Tr}(\mathcal{M})$

[11] В исчислении предикатов называемых *константами языка*.

При этом ясно, что в $\mathcal{M}$ не могут быть одновременно справедливы противоположные формулы[12] φ и $\neg\varphi$. Поэтому любая «теория» $\mathrm{Tr}(\mathcal{M})$ по крайней мере *непротиворечива.*

О *противоречивости* и *непротиворечивости* надо сказать отдельно.

7.3.1. *Множество A замкнутых формул считается непротиворечивым, если из него нельзя вывести два противоположных утверждения φ и $\neg\varphi$.*

Противоречива, по определению, любая формула с нулевой оценкой истинности, т. е. ложная при любых значениях входящих переменных. Такова формула $\varphi \wedge (\neg\varphi)$. Формула

$$\varphi \wedge (\neg\varphi) \to \psi, \tag{7.3}$$

наоборот, верна при любых значениях истинности φ и ψ, т. е. *общезначима.* В справедливости (7.3) легко убедиться, вспомнив определение импликации. Функция «$\zeta \to \eta$» при ложной ζ истинна независимо от того, какова η.

Механизм (7.3) обычно закладывается в аксиоматику синтаксиса (см. далее) в несколько ином облике,

$$\neg\varphi \to (\varphi \to \psi), \tag{7.4}$$

но в результате так или иначе постулируется, что в противоречивой теории T выводится «все что угодно», и тогда T включает в себя **все** формулы.

Теперь вернемся к нашим баранам. Непротиворечива любая *совместная* (*выполнимая*)[13] теория T, т. е. имеющая модель M.

[12] Хотя и не все пары $\{\varphi, \neg\varphi\}$ могут быть разрешимы в $\mathcal{M}$.

[13] Если в T входит нелепая вроде бы формула $\exists\, x : P(x) \to \forall\, x : P(x)$, — то это само по себе не мешает совместности, ибо существует модель, в которой x может принимать единственное значение, и там формула верна.

в которой по определению 7.2.4 истинны все ее формулы, что, правда, выглядит «маслом масляным», поскольку хотя и формулируется обычно в виде теоремы [3, т. 6] — на вид лишь повторяет определение *модели*. Но это все таки теорема, поскольку есть спрятанное осложнение в различии *синтаксического* ($\vdash$) и *семантического* ($\models$) следования, каковое обычно «висит на стене и не стреляет», но атмосферу портит.

Смешение *синтаксических* и *семантических* понятий вообще является весомым фактором неразберихи. В $T \models \varphi$ говорят о *семантическом следовании* φ из T, но определяется-то $T \models \varphi$ как истинность φ во всех интерпретациях $\mathcal{M}$ теории T, и ни о каком выводе речь не идет. А как перебрать все интерпретации? Не говоря о том, что и в одной-единственной — случаются проблемы. Одно дело убедиться в справедливости $2 \times 2 = 4$, другое — установить *тождество Якоби* [3, т. 8] для какой-нибудь группы, где требуется уже доказательство. Поэтому как понимать $\varphi \in \mathcal{M}$, как доказуемость φ в $\mathcal{M}$ или как правильность с точки зрения *Всевидящего Ока*? Так что *«семантическое следование»* $T \models \varphi$ — штука на вид растяжимая, но она имеет фундаментальное решение в лице *теоремы о полноте исчисления предикатов*, и проверка истинности φ во всех интерпретациях $\mathcal{M}$ заменяется *логическим выводом*, см. далее.

Синтаксическая «импликация» $T \vdash \varphi$ — инструмент более конкретный. В принципе, это вывод φ из T при опоре на некоторый формальный язык программирования, отражающий логическую природу решаемых задач[14]. И если теория T вырастает из аксиоматики $\mathscr{P}$, то за кадром образования предложений T стоят манипуляции с аксиомами $\mathscr{P}$ и регламентированные логические заключения. При этом вовсе не факт, что замыкание $\mathscr{P}$ в смысле $\vdash$ совпадет с замыканием в смысле $\models$. И потому между

---

[14] Все логические штучки приходится формализовать. Например, приходится вводить правило «$\{p \vdash a,\ q \vdash b\}$ влечет за собой $\{p, q \vdash a \wedge b\}$», т. е. заново вводить конъюнкцию, ибо сие понятие априори компьютеру неведомо. Компьютеризация внелогической части теории — вещь относительно размытая, в крайнем случае помогает *«тезис Тьюринга»*, [3, т. 6]

определениями 7.2.1 и 7.2.3 возможно расхождение. Но в *исчислении предикатов первого порядка* $\vdash$ равносильно $\models$, что декларируется пока авансом.

Если множеству аксиом $\mathscr{P}$ удовлетворяют всевозможные интерпретации $\mathcal{M}_\nu$, то замыкание $\mathscr{P}$ по семантическому следованию (п. 7.2.1) дает теорию

$$T = \bigcap_\nu \mathrm{Tr}(\mathcal{M}_\nu). \tag{7.5}$$

Некоторый интерес в отдельных случаях может представлять множество предложений

$$\bigcup_\nu \mathrm{Tr}(\mathcal{M}_\nu), \tag{7.6}$$

справедливости которых аксиоматика $\mathscr{P}$ — не мешает. Но (7.6), как правило, противоречиво — в одной модели выполняется φ, в другой $\neg\varphi$.

Рассмотрим для примера алгебраические поля [3, т. 8], регламентируемые хорошо известной аксиоматикой[15]. Основные примеры полей с нулевой *характеристикой*: поле действительных чисел $\mathbb{R}$, рациональных $\mathbb{Q}$ и комплексных $\mathbb{C}$. Формула

$$\exists\, x(x \cdot x = 1 + 1) \tag{7.7}$$

справедлива в $\mathbb{R}$ и $\mathbb{C}$, но неверна в $\mathbb{Q}$. Поэтому теория вида (7.5) — в данном случае *не полна*. Аксиоматика поля, стало быть, слабовата — допускает слишком много разнородных интерпретаций. «Жесткость» ей придает добавление аксиомы «существования корня у любого полинома». В результате теория *алгебраически замкнутых полей характеристики нуль* — становится *полной*.

Другой показательный пример — *примитивная арифметика* **PA** на базе языка (3.11), т. е.

$$L_0 = \{+,\ \times,\ =,\ \exists\}, \tag{7.8}$$

в котором исключена математическая индукция, и ничего нельзя доказать, можно только проверить разрешимость полиномиального уравнения (перебором). Иначе говоря, все *верные* утверждения

[15] Обычные в сигнатуре $L = \{+,\ \times,\ 0,\ 1\}$ «арифметические» свойства сложения и умножения, плюс существование обратных элементов по сложению и для ненулевых — по умножению.

$\exists\, xP(x) = 0$, и только они, в L_0 доказываются [16], и их множество оказывается *перечислимо*, но не *разрешимо* (глава 6).

О чем здесь идет речь? Изначально об интерпретации. На множестве $\mathbb{N}$ задано сложение $(+)$ и умножение $(\times)$ — причем конкретно задано, — и конструктивно (перечислимо, алгоритмически) определено множество верных предложений

$$\mathrm{Tr}(\mathbf{PA}) = \big\{\exists\, xP(x) = 0\big\},$$

где $P(x)$ — целочисленный полином. При этом у «теории» Tr(**PA**) нет никакой заранее определенной аксиоматики, ибо никакие свойства сложения $(+)$ и умножения $(\times)$ не фиксированы, функции $+$ и $\times$ просто механически определены. Соответственно

$$2 + 3 = 3 + 2$$

можно проверить только по факту (вычислением). Теория заведомо неполна, потому что в ситуациях $\forall\, xP(x) \neq 0$ нет возможности проверить ни формулу $\exists\, xP(x) = 0$, ни $\neg\exists\, xP(x) = 0$. Аксиоматизируема ли Tr(**PA**) — отдельный вопрос, и он решается отрицательно (глава 6).

На территории логики язык (7.8), конечно, несколько несуразен. Собственно, это даже не язык, а регламент, ограничивающий использование квантора $\forall$ и отрицания $\neg$ при сигнатуре

$$L = \{+,\ \times,\ =\}.$$

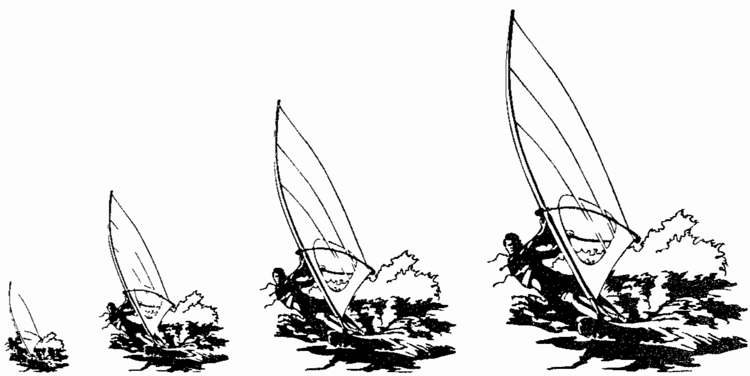
При этом в логике первого порядка из-за отсутствия формализованных свойств функциональных символов $+$ и $\times$ приходится рассматривать совершенно нелепые предложения, а простейшие факты типа

$$\forall\, x, y : x + y = y + x$$

[16] Как уже отмечалось, язык L_0 исключительно богат по своим возможностям, и позволяет описывать любые алгоритмически выразимые свойства чисел, множеств и других умопостигаемых объектов.

оказывается невозможно обосновать. Поэтому возникает естественное желание привлечь дополнительные механизмы (аксиомы), чтобы теория цивилизованно ожила. Чтобы истинными стали некоторые очевидные предложения типа $\neg\exists\, x \neq 0 : x^2 < 0$.

Проблему решает добавление к **PA** матиндукции, точнее говоря, *аксиом Пеано*. Тогда даже от $+$ и $\times$ можно отказаться, потому что сложение и умножение определяются через *функцию следования*. «Теория» Tr(**PA**) существенно расширяется, истинными становятся многие известные и неизвестные факты, хотя *полнота* не достигается. Хуже того, сама по себе непроверяемая матиндукция закладывает в ядро теории возможную *противоречивость*. По крайней мере *непротиворечивость аксиоматики* принципиально не доказывается (в рамках арифметики).

$\varnothing$ 

7.4. Исчисление предикатов

Лучше не договорить, чем утопить в деталях.

Диспозиция раздела может показаться противоестественной — как бы размышление о дебюте, когда игра уже в эндшпиле. Но именно так поступает читатель, особенно из тех, чей жизненный путь пролегает вдали от матлогики. Время от времени приходится возвращаться назад, чтобы вернуться в правильную колею.

Итак, что такое «*исчисление предикатов*»? Это логика первого порядка над алфавитом $\mathscr{A}$, в который входят логические символы ($\neg, \vee, \wedge, \rightarrow, \forall, \exists$), служебные (скобки и пр.), и *сигнатурные* — т. е. константы языка, а также функциональные и предикатные символы с указанием их «n-арности», «n-местности»[17]. Рассматриваемые формулы предполагаются *правильно построенными* (*ппф*), см. раздел 1.4, и обязательно *замкнутыми*[18]. Правила *ппф* задают над алфавитом $\mathscr{A}$ грамматику, и потому вместо $\mathscr{A}$ можно говорить о языке L или о его *сигнатуре* (внелогической части), которую обозначим той же буквой L.

7.4.1. *Замкнутая формула (предложение) φ* ***выполнима****, если существует модель*[19] *φ, пишут $L \models \varphi$.*

7.4.2. *Замкнутая формула (предложение) φ* ***общезначима****, если справедлива в любой интерпретации.*

В обоих случаях речь идет о семантических понятиях. Но если п. 7.4.1 выглядит более-менее реалистично, то как понимать дефиницию 7.4.2, имеющую дело со *всеми* интерпретациями. Как их все проверять, да и как перебрать?

Оказывается, перебирать и проверять не надо. Рассмотрим пример. Пусть $\mathscr{P}_G$ — аксиомы (7.1) теории групп, $\wedge\mathscr{P}_G$ — их *конъюнкция*, а J — *тождество Якоби для коммутаторов*. Тогда

$$\wedge\mathscr{P}_G \rightarrow J \tag{7.9}$$

общезначимая формула, верная в любой модели аксиоматики $\mathscr{P}_G$, т. е. справедливая для любой группы (конечной, бесконечной, с кручением, без кручения, поворотов, перестановок и т. п.). Откуда берется уверенность, что «для любой» — проверки-то не было. Уверенность проистекает из того, что ничего кроме

---

[17] Мы стараемся повторяться, где это не слишком дорого стоит, чтобы не приходилось метаться по тексту.

[18] Все переменные находятся под действием кванторов.

[19] То есть существует интерпретация, в которой φ истинна.

аксиом $\mathscr{P}_G$ в процессе доказательства тождества J не использовалось, не считая «*естественных логических правил вывода*».

Такого сорта «*правила*» за пределами матлогики в фокус внимания не попадают и используются как само собой разумеющиеся. Поэтому, если эти «*правила*» адекватно описать в полном ассортименте, — возникает инструмент доказательства общезначимых *теорем*[20] (*замкнутых формул, предложений*), верных в любой интерпретации любой рассматриваемой теории.

Каковы эти «*правила*»? Трудность их фиксации заключена в самоочевидности. Ограничимся пока *исчислением высказываний*. Скажем,

$$(A \wedge B) \to A, \quad (A \wedge B) \to B. \tag{7.10}$$

Истинность формул очевидна (легко проверяется по таблицам истинности для импликации и конъюнкции) и, казалось бы, не о чем говорить. Но нам необходимо освободиться от семантики. Машина не знает, что такое конъюнкция. Ей нужна формальная (синтаксическая) запись. Теперь, благодаря (7.10), если в какой-то формуле встречается слово $(A \wedge B)$, компьютер, никуда не вникая, может заменить его на A или B. Далее:

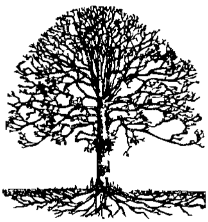
$$A \vee \neg A, \quad A \to (A \wedge B), \quad B \to (A \wedge B) \quad \text{и т. п.}$$

С полным списком *аксиом исчисления высказываний* можно ознакомиться по любому учебнику. В «списке» выделяется аксиома *модус поненс* $A \wedge (A \to B) \to B$, являющаяся *правилом вывода*.

Дело не в том, что формулой «$A \wedge (A \to B) \to B$» можно пользоваться, а в том, что ее использование позволяет искать доказательства, т. е. цепочки формул, ведущие от предположений к следствиям, от φ к ψ. Каждый раз в формуле берется какое-то истинное A, подбирается B, следующее из A, после чего A

[20] Теоремы не обязаны быть устроены по типу (7.9), т. е. быть верны «для любой группы». В предположения могут закладываться какие-то ограничения $\mathscr{R}$, и тогда $\wedge\mathscr{P}_G$ в левой части (7.9) надо заменить на $(\wedge\mathscr{P}_G) \wedge \mathscr{R}$.

заменяется на B. При автоматическом поиске доказательств это довольно громоздкая и неуклюжая процедура, но она работает.



Именно *модус поненс* позволяет пользоваться благами типа (7.10). В противном случае можно было бы разве что умиляться истинностью, скажем, $(A \wedge B) \to A$, но заменить $(A \wedge B)$ на A в какой-нибудь формуле не было бы оснований. *Модус поненс* позволяет выйти из ступора.

Итак, все аксиомы синтаксиса — суть формулы, причем *общезначимые*. *Общезначимые*, ибо элементарная проверка показывает их истинность при любых значениях (истина/ложь) входящих «аргументов». При этом *модус поненс* позволяет при помощи избавления от импликаций[21] из формулы φ вывести другую формулу ψ, т. е. *доказать* ψ в предположении φ, если таковое следование действительно имеет место.

Откуда гарантия, что **все** формулы *исчисления высказываний* могут быть получены из десятка аксиом (базовых формул) вышеозначенного «списка»? Из элементарного перебора возможностей. Варианты построения формул с помощью комбинаций логических операций

$$\neg(\text{«не»}), \quad \vee\ (\text{или}), \quad \wedge\ (\text{и}), \quad \to (\text{«следует»}),$$

с одной стороны, позволяют описать любую логическую функцию[22], а с другой — исчерпываются аксиоматикой синтаксиса. И как только это установлено, возникает взаимное соответствие

[21] Напомним, $a \to b$ лишь наполовину отвечает расхожему пониманию «если a, то b», каковое фокусируется на истинности следствия b из истинного предположения a. А если a ложно? Логическая функция-то должна быть определена на всех комбинациях переменных. Вот и получается, что *импликация* $x \to y$ как функция $\varphi(x, y)$ всюду равна 1, за исключением случая $x = 1$, $y = 0$, где она равна 0. Другими словами, из «истины» не может следовать «ложь», все остальное — возможно.

[22] Например, любая n-местная функция $\varphi(x_1, \ldots, x_n)$ записывается с помощью конъюнкций, дизъюнкций и отрицаний [3, т. 6].

между синтаксисом ($\vdash$) и семантикой ($\models$), что декларируется как *теорема о полноте исчисления высказываний*[23].

Но нам этого мало. При переходе к *исчислению предикатов* приходится дополнительно разбираться с кванторами. Как машина может быть уверена в общезначимости формул

$$\forall x f(x) \to f(t) \quad \text{или} \quad \forall x f(x) \to \exists x f(x), \tag{7.11}$$

не зная смысла кванторов. Компьютеру не объяснишь, хотя ему это и не нужно. Ему требуется грамматика — набор правил, регламентирующий, что́ можно делать с кванторными формулами. Несколько аксиом типа (7.11)[24] в итоге решают проблему

$$«\vdash \ \leftrightarrows \ \models»,$$

и исчисление предикатов обретает статус *полного исчисления*, у которого синтаксис и семантика согласованы. Мы пока не останавливаемся на доказательстве (см. следующий раздел), ибо у нас другая цель — представить результат как единое целое, чтобы видно было, откуда проистекает и куда направлен[25].

На *исчисление предикатов* важно посмотреть издалека, чтобы позиционировать как инструмент для «проигрывания» математических дисциплин. Как холст для изображения других теорий. Если же смотреть как на «теорию первого порядка *без аксиом*», то охватываются **все** замкнутые *ппф*-формулы в некотором языке — и теория выходит противоречивая. Сужение множества предложений до *общезначимых формул* ликвидирует противоречивость,

---

[23] При этом говорят о *полноте дедукции*, об *адекватности синтаксиса* и пр. Сам по себе результат довольно простой, но чрезвычайно важный по сути, потому что иначе пришлось бы «стоять на месте».

[24] Точнее, к аксиомам исчисления высказываний добавляются

$$\forall x A(x) \to A(t), \quad A(z) \to \exists x A(x),$$

а к *модус поненс* — *правило обобщения* $A(x) \to \forall x A(x)$.

[25] Такое восприятие любого предмета изучения — и в начале и в конце — необходимо для успешного завершения процесса. Это, разумеется, не исключает возможной потребности разбираться в частностях и тонкостях.

но такая теория будет *неполной*[26], *неразрешимой*, *неаксиоматизируемой*. Так что лучше смотреть как на *аппарат*, в котором *общезначимые* формулы играют первостепенную роль.

Дело в том что в *исчислении предикатов* замкнутые формулы замкнуты только по *переменным*, но не по функциональным и предикатным символам, потому что сценарий разворачивается в *логике первого порядка*. По этой причине здесь в общем случае невозможно делить формулы на истинные и ложные. В каких-то интерпретациях f_i, R_j — формула может быть истинной, в других — ложной. Именно поэтому наибольший интерес представляют *общезначимые формулы* (п. 7.4.2) как безусловно истинные, и *невыполнимые* (п. 7.4.1) как безусловно ложные. Если φ общезначима, то $\neg\varphi$ — невыполнима, и наоборот.

Что касается широты замаха *исчисления предикатов*, то оно охватывает почти всю математику. Потому что всякая теорема является *общезначимой формулой*, устроенной по типу (7.9), т. е. имеет вид

$$\wedge \textit{ПРЕДПОЛОЖЕНИЯ} \to \textit{ВЫВОД}. \tag{7.12}$$

Сей факт полезно осмыслить, поскольку в качестве примера общезначимой формулы часто приводится что-нибудь вроде

$$\forall\, x A(x) \to A(t),$$

и это сильно сдерживает фантазию. Думается, чтó может быть безусловно справедливо для любых функций и отношений? Да «что угодно», если не возбраняется делать предположения и «конъюнктивно» загонять их в левую часть (7.12). Скажем, некий функциональный символ f в L потенциально может быть любой функцией, но стоит загнать в предположения условие

$$f(\alpha x + \beta y) = \alpha f(x) + \beta f(y),$$

и это уже почти линейная функция, со многими вытекающими последствиями.

---

[26] Тогда как *исчисление предикатов* — *полно*. И эта двусмысленность «полноты» является камнем преткновения для подавляющей части населения, см. следующий раздел.

7.5. Полнота исчисления предикатов

Вернемся к проблеме взаимодействия *семантического* ($\models$) и *синтаксического* ($\vdash$) следования. По большому счету *полнота исчисления предикатов* заключается в эквивалентности «$\models$» и «$\vdash$», что в логиках более высокого порядка теряет силу. Однако в логике первого порядка:

> **7.5.1.** *Если $\varphi \models \psi$, т. е. ψ справедливо во всех интерпретациях φ, то $\varphi \vdash \psi$, т. е. ψ выводится из φ алгоритмически на базе аксиоматики логического вывода, — и наоборот.*

Заметим, все *общезначимые формулы* φ — а именно таковы все теоремы (7.12) — выводятся «из ничего»[27], что вместо $\varnothing \models \varphi$, $\varnothing \vdash \varphi$ записывают в форме $\models \varphi$, $\vdash \varphi$. Для этого случая п. 7.5.1 приобретает другую форму:

> **7.5.2.** *Любая общезначимая формула φ (пишут $\models \varphi$) выводится алгоритмически (синтаксически), — и наоборот.*

Ядро п. 7.5.2 расщепляется на несколько ингредиентов.

7.5.3. Теорема. *Всякая непротиворечивая теория совместна, т. е. имеет модель.* (!)

Утверждение 7.5.3 часто называют *теоремой Гёделя о полноте исчисления предикатов*. Внешне она не напоминает результат 7.5.2, но представляет собой трамплин к нему.

7.5.4. Следствие. *Всякая общезначимая формула выводима в исчислении предикатов, т. е. $\models \varphi \Rightarrow \vdash \varphi$.*

◄ Действительно, если φ невыводима, то множество $\{\neg\varphi\}$[28] непротиворечиво, и по теореме 7.5.3 имеет модель. Но в этой модели φ не может быть истинной, что противоречит общезначимости φ. ►

---

[27] Предположения «конъюнктивно» загоняются в левую часть (7.12).

[28] Представляющее собой множество следствий из $\neg\varphi$.

Обратная «импликация» $\vdash \varphi \Rightarrow \models \varphi$, вообще говоря, очевидна, и обычно формулируется в виде ***теоремы корректности***: «*Всякая формула, выводимая в исчислении предикатов, общезначима*». Как уже отмечалось в предыдущем разделе, все аксиомы исчисления предикатов общезначимы — отсюда, соответственно, и вытекает общезначимость вывода (как комбинации общезначимых элементов).

Теперь вернемся к центральному результату 7.5.3, который в несколько более общем виде звучит так.

(!) **7.5.5. Теорема.** *Всякое непротиворечивое множество предложений* Θ — *совместно, т. е. имеет модель.*

Теорема 7.5.5 достаточно популярна, чтобы здесь еще раз повторять ее доказательство[29]. Но проблема, стоящая за кадром, заслуживает обсуждения, потому что тут бывает не виден сам вопрос, а не формальный ответ.

Посмотрим на задачу сквозь призму *теории групп* (п. 7.2.5), которая в данном случае хороша тем, что ее метод построения моделей *свободных групп* [3, т. 13] может служить образцом для общей ситуации 7.5.5.

Итак, в качестве Θ из п. 7.5.5 возьмем множество аксиом (7.1), к которому, вообще говоря, надо добавить аксиомы равенства, либо считать их «зашитыми» в *исчисление предикатов* по умолчанию[30]. Как построить какой-нибудь вариант *универсума* модели? В язык $L = \{\cdot,\ ^{-1},\ e\}$ добавим константу a (элемент группы), и применяя к нему операции

$$a \cdot a, \quad a^{-1}, \quad (a \cdot a)^{-1}, \quad (a \cdot a) \cdot a, \quad \ldots,$$

---

[29] Более детальное изложение большинства рассматриваемых в главе вопросов см. в [4] или [5, ч. II], где многое преподносится убедительно с точки зрения диалога с читателем.

[30] *Равенство* со своей аксиоматикой чаще относят к логической части *исчисления предикатов*, исключая его тем самым из *сигнатуры*. Но иногда его вообще исключают, изучая *теории без равенства*.

придем к универсуму

$$V = \{\ \dots, a^{-2}, a^{-1}, e, a, a^2, \dots\ \}, \tag{7.13}$$

где a^k — символ, обозначающий $\underbrace{a \dots a}_{k \text{ раз}}$, соответственно

$$a^{-k} = \underbrace{a^{-1} \dots a^{-1}}_{k \text{ раз}}.$$

При этом для любых переменных x, y, z, принимающих значения в множестве V, истинны все предложения (7.1), т. е. групповые аксиомы. Модель готова (*свободная группа с одной образующей*). Что касается единственного в данном случае предиката (равенства), то он в формировании универсума (7.13) не участвует — **(!)**, см. далее, — но всевозможные предложения типа $x \cdot y^{-1} = z$, где переменные принимают значения в множестве V, — определены и эффективно проверяются.

Аксиоматика теории групп может быть образована и без операции обращения элемента — в языке $L' = \{\cdot, e\}$. Но тогда последнюю аксиому (7.1) приходится заменить на предложение

$$\forall\, x\, \exists\, z : (x \cdot z = e) \wedge (z \cdot x = e) \tag{7.14}$$

с квантором существования. Теперь, добавляя к L' константу a и многократно применяя умножение, мы получим множество $\{e, a, a^2, \dots\}$, на котором формула (7.14) не выполняется. Поэтому к сигнатуре надо добавить еще символы $a^{-1}, a^{-2}, \dots$ в качестве элементов, на которых достигается существование в (7.14), — в результате опять возникает универсум (7.13).

Использованные два приема расширения сигнатуры для получения универсума модели являются достаточными и в общей ситуации. К первичным константам языка добавляются «взятые с потолка» (или не добавляются, если и так хватает) и к этим термам многократно применяются функциональные символы, что дает новые термы $f(a_1, \dots, a_n)$. И так далее, до бесконечности.

Кроме того, для всякой выводимой из Θ формулы $\exists\, x\varphi(x)$ добавляется (если нужно) терм t, называемый «свидетелем», для которого $\varphi(t)$ также выводится в Θ, — иначе бы формула $\exists\, x\varphi(x)$ повисала нереализуемой, а так получается $\exists\, x\varphi(x) \to \varphi(t)$.

Неясным пока остается вопрос о роли непротиворечивости множества предложений Θ. Для рассмотренного примера справедливость всех аксиом (7.1) в (7.13) была очевидной. Рассмотрим более сложный пример. К сигнатуре теории групп добавим вначале два символа (*терма*) a и b. Универсум V получится состоящим из e и всевозможных слов типа «$a \cdot b^{-1} \cdot a^7 \cdot b$», что представляет собой *свободную группу с двумя образующими*[31].

Предположим, в Θ помимо (7.1) входят предложения

$$a^n = e, \quad b^2 = e, \quad (a \cdot b)^2 = e. \tag{7.15}$$

Тогда все «расплывается». Неясно, существует ли такая группа (модель) в нетривиальном варианте — при дополнительном требовании $\exists\, x(x \neq e)$, т. е. $\exists\, x\neg(x = e)$. Не противоречат ли предложения совокупности «(7.1)+(7.15)» друг другу? С ходу не разберешься. Правда, несложный анализ [3, т. 8] показывает, что группа с *определяющими соотношениями* (7.15) существует и изоморфна группе *диэдра*[32]. Отсюда, т. е. задним умом (модель-то уже есть), следует непротиворечивость Θ.

Таким образом, соотношения (7.15) ведут к счастливому финалу. В общем случае задание группы определяющими соотношениями, хотя и является универсальным способом, но о так заданной группе в общем случае (причем как правило) почти ничего нельзя сказать. Конечна она или бесконечна, коммутативна ли, содержит ли хотя бы один элемент кроме единицы.

---

[31] Пример свободной группы хорош тем, что он демонстрирует необязательность доведения интерпретации до чего-нибудь осязаемого типа группы поворотов. Поначалу ведь кажется, что интерпретация обязана быть «жестко конкретной», не оставляя свободы для толкования элементов и функций. А тут абстрактные символы и слова, и ничего более. Но этого, оказывается, вполне достаточно, чтобы служить моделью.

[32] Группа *диэдра* D_n имеет две образующих: поворот $a = 2\pi/n$ и отражение b, которые удовлетворяют равенствам (7.15).

Поэтому подключение к (7.1) каких-то *определяющих соотношений* наряду с $\exists\, x \neg(x = e)$ — в большинстве случаев делает проблему непротиворечивости Θ принципиально неразрешимой.

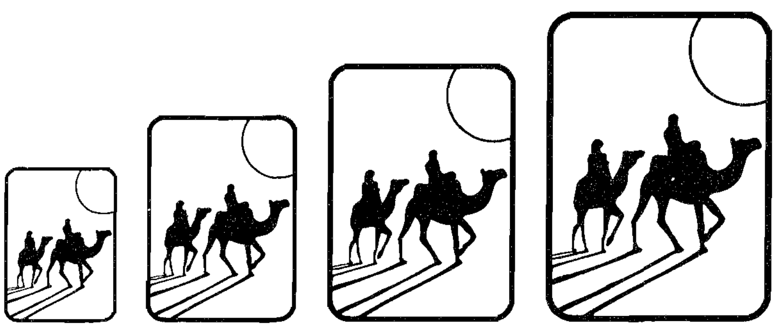
Если же непротиворечивость Θ установлена, то *модель*, вернее, пока *интерпретация*, построенная указанным выше способом, будет удовлетворять всем предложениям из Θ. Но это надо доказывать, что не так уж сложно. Сначала Θ перечислимо расширяется до *полной теории* $\Theta(\vdash)$, т. е. так, чтобы для любой формулы φ было

$$\text{либо} \quad \varphi \in \Theta(\vdash), \quad \text{либо} \quad \neg\varphi \in \Theta(\vdash).$$

Суть дальнейшего рассуждения высвечивается на простейшей ситуации, когда речь идет об исчислении высказываний, т. е. о бескванторных формулах на игровом поле *«истина-ложь»*[33]. Итак, если *теория* $\Theta(\vdash)$ (полученная замыканием Θ по синтаксическому выводу) ***полна***, а переменные $x = \{x_1, \dots, x_n, \dots\}$ пропозициональны, то из каждой пары формул

$$x_i = 1, \quad \neg(x_i = 1), \quad \text{т. е.} \quad x_i = 0,$$

одна принадлежит $\Theta(\vdash)$, что полностью определяет значения переменных, при которых все формулы теории $\Theta(\vdash)$ истинны.

$\varnothing$ 

[33] К такому случаю, вообще говоря, сводится общая ситуация. Кванторы общности заменяются кванторами существования, благодаря эквивалентности $\forall\, x : \varphi$ и $\neg\exists\, x : \neg\varphi$, а от $\exists$ избавляет введение в сигнатуру дополнительных констант с последующей заменой $\exists\, x\varphi(x) \to \varphi(t)$. Путь несколько тернист, но методично преодолевается [5, ч. II].

7.6. Полные и неполные теории

Начнем с важного замечания.

> ***Полнота теории*** и ***полнота исчисления предикатов*** — совершенно разные понятия. Беда в том, что в литературе и умах они часто путаются.

Полнота теории (определение 7.2.2) играет существенную роль в обосновании следующего важного результата.

7.6.1. Теорема. *Если непротиворечивая теория T полна и перечислимо аксиоматизируема, то она* ***разрешима.***

◄ Наличие перечислимого множества аксиом позволяет перечислять все выводимые формулы. При этом в силу полноты теории автоматически перечисляются и — невыводимые. Множество T и его дополнение оказываются оба перечислимы, а значит, по *теореме Поста* 6.2.2, T разрешимо. ►

Понятно что стремление достичь *полноты теории* опосредованно связано именно с *разрешимостью*. Но ситуация из п. 7.6.1 довольно редка — по причине «арифметической аномалии», которая в большинстве случаев (для достаточно сложных теорий) является нормой (*теорема* 6.4.2). Но это не исключает существования в пустыне неразрешимых и неаксиоматизируемых теорий оазисов благополучия. Нужны только приборы обнаружения.

7.6.2. Теорема. *Непротиворечивая теория T полна в томм случае, когда любые ее модели* ***элементарно эквивалентны***[34].

Вот другой результат из «ε-окрестности» п. 7.6.2.

7.6.3. Теорема[35]**.** *Непротиворечивая теория T полна в томм случае, когда $T = Tr(\mathcal{M})$, где $\mathcal{M}$ — любая модель теории T.*

---

[34] Модели $\mathcal{M}$ и $\mathcal{N}$ в сигнатуре S *элементарно эквивалентны*, если в них верны одни и те же предложения в S.

[35] Доказательства здесь совсем просты [22].

Таким образом, всякая полная теория является теорией вида $Tr(\mathcal{M})$. Танцевать от модели не так легко, кстати, как может показаться. Для обозримости нужна аксиоматика, выделение которой и составляет главную трудность при изучении теорий $Tr(\mathcal{M})$, ибо найти «генетический код» $Tr(\mathcal{M})$, как правило, не удается. Попытка же начать теорию с другого конца, с абстрактной аксиоматики, вызывает осложнения иного сорта[36].

Вернемся, однако, к признакам полноты. Теоремы 7.6.2, 7.6.3 в качестве критериев мало удобны. Чаще используют либо *тест Воота*, либо *элиминацию кванторов*.

7.6.4. Тест Воота. *Пусть счетная теория T не имеет конечных моделей и $\mathfrak{m}$-категорична*[37] *для некоторой бесконечной мощности $\mathfrak{m}$. Тогда T полная теория*[38].

Что касается *элиминации кванторов*, то она представляет собой более действенный инструмент. Причем не только для исследования полноты теорий, но и для изучения других задач — например, о *выразимости предикатов*, см. [5, ч. II].

7.6.5. Определение. *Теория T в сигнатуре S допускает **элиминацию кванторов**, если для любой формулы φ этой теории существует эквивалентная бескванторная формула ψ, т. е.*

$$T \models \varphi \leftrightarrow \psi.$$

Например, арифметическая формула $\exists\, x(x > 0) \wedge (a + x = b)$ эквивалентна бескванторной формуле $a > b$. Тогда как в *арифметике сложения* в сигнатуре

[36] Аксиоматизация — процесс творческий, и тут часто не удается закрыть ворота для совсем других интерпретаций. Результат чаще всего не тот, какой ожидался. Либо не все «истины» попадают в теорию, либо появляются «непрошенные гости». Например, аксиоматизация понятия метрики допускает к рассмотрению океан возможностей, каковые сами по себе даже не представляют интереса, но входят в себестоимость достигаемой общности. Хотим мы того или нет, в сектор прицела попадает масса аномальных ситуаций, см. [3, т. 5]. Но иметь дело приходится с тем, что получается.

[37] Теория считается *$\mathfrak{m}$-категоричной*, если имеет хотя бы одну модель мощности $\mathfrak{m}$, и любые две такие модели изоморфны (*мощность модели* — это мощность ее универсума).

[38] Например, *«теория плотного линейного порядка без концевых точек»*, где критерий Воота быстро приводит к необходимому заключению.

$S = (\mathbb{Z}, =, <, +)$ формула $\exists\, z(x = z + z)$, верная для четных x, не эквивалентна никакой бескванторной формуле.

Освободиться от кванторов, конечно, можно всегда *за счет расширения сигнатуры*. Но в данном случае речь идет об «элиминации» при фиксированном алфавите. Либо с алфавитом проделываются те или иные трюки, но контролируется, что они не меняют теории.

Возможность перехода от замкнутых формул к бескванторным — означает по сути возможность перехода к *пропозициональным переменным* и, как следствие, возможность оценки истинности и выделения в каждой паре $(\varphi, \neg\varphi)$ одной формулы, принадлежащей теории. Таким образом, *теории, допускающие элиминацию кванторов, полны*[39], ибо там есть конкретный инструмент для проверки любой замкнутой формулы на предмет принадлежности теории.

Уточнение сказанного тут было бы несколько громоздко, и потому мы ограничимся иллюстрационным примером[40]. О неразрешимости арифметики уже много раз говорилось. Интересно что *арифметика Пресбургера* — арифметика со сложением, но без умножения, — *полна и разрешима*[41]. Речь идет об арифметике в сигнатуре

$$S = (\mathbb{Z},\ =,\ <,\ +). \tag{7.16}$$

Сразу ясно, что при такой сигнатуре *элиминация кванторов* невозможна, поскольку ни одна формула $\exists\, z(x = z + \ldots + z)$ не эквивалентна *бескванторной* — на территории (7.16). Обойти трудность можно введением счетного семейства предикатов

$$\overset{2}{=},\quad \overset{3}{=},\quad \overset{4}{=},\quad \ldots,$$

где $\overset{k}{=}$, как обычно, означает равенство по модулю k. И тогда в

$$\left(\mathbb{Z},\quad =,\quad <,\quad +,\quad \overset{2}{=},\quad \overset{3}{=},\quad \overset{4}{=},\quad \ldots\right) \tag{7.17}$$

[39] Мы не уточняем некоторые детали, см. [4].

[40] Тем более что тема подробно излагается в любом учебнике. Но там, кстати, неискушенный читатель теряется иногда как раз из-за обилия деталей.

[41] То же самое установил *Сколем* относительно арифметики с умножением, но без сложения.

элиминация кванторов возможна, что не очень сложно доказывается, см. [4]. Арифметика, таким образом, в сигнатуре (7.17) полна и разрешима. Решена, конечно, не та задача, которая изначально ставилась. Но расширение (7.17) сигнатуры (7.16) не меняет множества выразимых предикатов[42)], и потому переход от сигнатуры (7.16) к (7.17) в данном случае не меняет теории, а значит, *арифметика Пресбургера — полна и разрешима*.

Обратим внимание, что *арифметика Пресбургера* в разных источниках излагается крайне неодинаково[43)]. Причины тут вообще-то объективные. Начинать можно с натурального ряда в сигнатуре, а можно и с констант 0, 1, компенсируя нищету сигнатуры введением аксиом. Можно даже избежать расширения сигнатуры (7.17) за счет расширения аксиоматики [5, ч. II]. Кроме того, всякое изложение больше или меньше блуждает между теорией как совокупностью формул, вырастающих из аксиом, и той или иной интерпретацией, каковая подразумевается, но не оговаривается.

Такая неаккуратность типична для матлогики, потому что педантичность здесь обходится еще дороже. Слишком много частностей, чтобы вытаскивать их на свет божий. Мы этим тоже постоянно грешим. Скажем, язык *примитивной арифметики* записывается как $L_0 = \{+, \times, =, \exists\}$, хотя надо бы включить натуральный ряд. Знак равенства, как предикатный символ, то упоминается, то — нет, хотя подразумевается в наличии, в то же время возможны теории без знака равенства.

Возвращаясь к *элиминации кванторов*, заметим, что сей феномен является мощным инструментом, позволяющим решать весьма сложные задачи и за пределами математической логики. Например, теории, допускающие *элиминацию кванторов*, обладают *модельной полнотой*[44)]. Отсюда буквально в несколько строчек выводится *теорема Гильберта о нулях* (Nullstellensatz).

7.7. Теоремы компактности

Из рассуждений в пользу *теорем* 7.5.3, 7.5.5 ясна справедливость следующего результата[45)].

---

42) Например, $x \stackrel{2}{=} y$ выражается как $\exists\, z(x = y + z + z)$.

43) Что вообще характерно для многих разделов математической логики — и это аудиторию нередко ставит в тупик.

44) Теория *модельно полна*, если для ее моделей из включения $\mathcal{M} \subset \mathcal{N}$ следует, что $\mathcal{M}$ — *элементарная подмодель* $\mathcal{N}$.

45) Потому что модель для п. 7.5.5 конструировалась не более чем счетная.

7.7.1. Теорема. *Непротиворечивое множество замкнутых формул конечной или счетной сигнатуры имеет* **счетную** *модель.*

Поскольку непротиворечивость теории гарантируется существованием модели, п. 7.7.1 может быть переформулирован следующим образом.

7.7.2. Теорема. *Если теория имеет модель, то она имеет также* **счетную** *модель*[46].

Несколько иной тип формулировки возникает в связи с другим подходом к непротиворечивости, опирающимся на конечность вывода любой формулы. Модель может быть сколь угодно мощна, но только ее конечная часть может иметь отношение к доказательству отдельной теоремы. Если формула выводится в рамках некоторой системы, то она выводится и в рамках конечной подсистемы[47]. Поэтому любое противоречие всегда выводится из конечного множества предложений. Следовательно:

7.7.4. *Если любое конечное подмножество множества X замкнутых формул непротиворечиво, то X непротиворечиво.*

7.7.5. *Если любое конечное подмножество множества X замкнутых формул имеет модель, то X имеет модель.*

7.7.6. Теорема. *Если множество предложений несовместно, то несовместно и некоторое его конечное подмножество.*

Перечисленные результаты крутятся вокруг общего стержня и, так или иначе, связаны со взаимодействием *конечного* и *бесконечного. Теоремы компактности* 7.7.5, 7.7.6 имеют многочисленные

[46] При конечной или счетной сигнатуре. В общем случае гарантируется существование *либо счетной модели, либо модели мощности сигнатуры.*

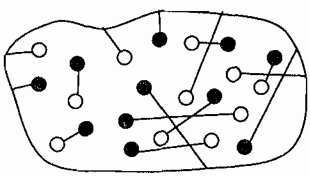
[47] Фиксация чего представляет самостоятельный интерес.

7.7.3. Теорема. *Если $X \vdash f$, то существует конечное подмножество $S \subset X$ замкнутых формул, такое что $S \vdash f$.*

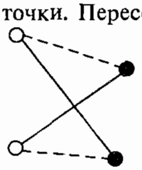
следствия за пределами матлогики. *Если любой конечный подграф бесконечного графа* Γ *k-окрашиваем, то и* Γ *k-окрашиваем.* Такого сорта результаты подталкивают к мысли о справедливости общего результата: *«если любая конечная подзадача* (*не*)*решается, то и вся задача* (*не*)*решается»*.

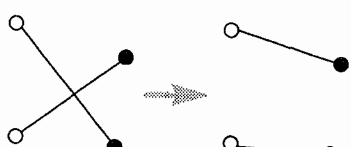
В общем случае это не так. Рассмотрим пример.

7.7.7. *При любом расположении на плоскости n черных и n белых точек, никакие три из которых не лежат на одной прямой, их можно попарно соединить* (*черную с белой*) *отрезками прямых так, что отрезки не будут пересекаться*[48].



Слева на рисунке изображен фрагмент общей картины при неком произвольном соответствии черных и белых точек с многочисленными пересечениями отрезков. Избавиться от пересечений позволяет очень простой алгоритм последовательного уменьшения общей длины соединяющих отрезков.

На каждом шаге выбираем произвольную точку пересечения. Ей отвечают две белых и две черных точки. Пересекающиеся отрезки меняем на непересекающиеся (пунктирные)  , т. е. действуем по схеме



При этом общая длина отрезков уменьшается — поэтому алгоритм сходится за конечное число шагов[49].

---

[48] По-видимому, это задача *Дейкстры.*

[49] На отдельных шагах число пересечений может даже увеличиваться. Но при достижении минимума «общей длины» пищи для алгоритма, т. е. пересечений, больше нет.

На фоне результатов типа 7.7.5, 7.7.6 естественно предположить, что п. 7.7.7 остается в силе, если точек (тех и других) счетное число. Но это не так. Первый симптом, указывающий на неправомочность обобщения, заключается в том, что попытка записи обобщения п. 7.7.7 в *логике первого порядка* упирается в необходимость использования квантора $\exists$ по предикату (по соответствию точек). Но это, правда, еще не дает гарантию отрицательного ответа. Гарантию дает контрпример, в котором черные точки имеют координаты $\left(k, \frac{1}{k}\right)$, белые — $\left(-k, -\frac{1}{k}\right)$. **(?)**

7.8. Теоремы Лёвенгейма—Сколема

Утверждения типа 7.7.2 называют *теоремами Лёвенгейма—Сколема*. Множественное число здесь употреблено, чтобы оставить место для вариаций. Факт 7.7.2 был декларирован в контексте полноты исчисления предикатов, каковая в данной ситуации несущественна. Более удобная версия:

7.8.1. Теорема Лёвенгейма—Сколема о понижении мощности. *Если множество S замкнутых предложений имеет модель*[50] *в конечной или счетной сигнатуре, то оно имеет также* ***счетную*** *модель*[51].

Утверждение 7.8.1 называют *теоремой о понижении мощности модели*. Но мощность модели можно и повышать. Вот два результата на эту тему.

7.8.2. Теорема. *Если множество S замкнутых предложений имеет модель сколь угодно большой конечной мощности, то оно имеет также бесконечную модель.*

---

[50] То есть *интерпретацию*, в которой истинны все формулы S. Замена «теории» в п. 7.7.2 «множеством замкнутых предложений» освобождает от необходимости замыкания S по логическому следованию, и от головной боли, связанной с этим.

[51] Для более мощных сигнатур можно утверждать существование модели мощности, не превышающей мощности сигнатуры. К формулировке 7.8.1 можно добавить вывод о том, что провозглашаемая «счетная модель» является *элементарной* подмоделью исходной модели.

Доказательство имеет смысл рассмотреть в качестве простого примера использования техники, присущей данной области. ◀ Присовокупим к S всевозможные предложения

$$\varphi_n = \exists\, x_1 \ldots \exists\, x_n \neg(x_1 = x_2) \wedge \neg(x_2 = x_3) \wedge \ldots \neg(x_n = x_1),$$

образуя $S^* = S \cup \Phi$, где $\Phi = \bigcup\limits_{n=1}^{\infty} \varphi_n$.

Если множество предложений $\Gamma \subset S^*$ конечно, то

$$\Gamma \subset S \bigcup_{n=1}^{k} \varphi_n$$

при некотором k. А $S \bigcup\limits_{n=1}^{k} \varphi_n$ имеет модель любой конечной мощности $m > k$, что следует из предположения теоремы. Эта модель будет моделью и для меньшего (по включению) Γ. Но тогда *теорема компактности* 7.7.5 гарантирует существование модели[52] для всего S^*, тем более — для $S \subset S^*$. ▶

7.8.3. Теорема Лёвенгейма—Сколема о повышении мощности. *Если множество S замкнутых предложений имеет бесконечную модель, то оно имеет также модель сколь угодно большой мощности*[53].

Это *теорема о повышении мощности модели*. Доказательство схематично напоминает предыдущее. Сигнатура дополняется новыми символами α, принадлежащими множеству $\mathcal{A}$ любой наперед заданной мощности. Затем S расширяется до

$$S^* = S \cup \big\{\neg(\alpha = \beta) : \alpha,\ \beta \in \mathcal{A},\ \alpha \neq \beta\big\}$$

и далее по схеме доказательства п. 7.8.2.

7.9. «Парадоксы» и сюрпризы

Существование счетных моделей, утверждаемое теоремами из предыдущих разделов, бывает далеко не очевидным, а иногда и парадоксальным при поверхностном взгляде.

---

[52] Каковая по самому определению S^* может быть только бесконечной.

[53] Таким образом, у теорий с конечной сигнатурой либо бесконечных моделей вообще нет, либо бесконечные модели есть любой мощности.

Рассмотрим **ZF**. Сигнатура $\{\varnothing, \in, =\}$ небогата. Функциональных символов нет, одна константа $\varnothing$ и два предикатных символа $\in$ и $=$. Построение счетного универсума модели, в духе рецептуры для обоснования полноты исчисления предикатов, происходит здесь за счет единственного механизма добавления «свидетелей» — для всякой выводимой из **ZF** формулы

$$\exists\, x\varphi(x)$$

добавляется (если нужно) терм t, чтобы формула не повисала нереализуемой. Если теперь предположить непротиворечивость **ZF** (что приходится делать, ибо доказать невозможно), то *теорема* 7.7.1 гарантирует существование счетной модели[54]. Иными словами, существует такая счетная совокупность множеств, что вместе с отношением $\in$ она образует модель **ZF**. Тут и возникает нашумевший в свое время *парадокс Сколема*, в основе которого лежит следующее «противоречие».

В **ZF** присутствует аксиома, утверждающая существование, наряду с любым множеством X, множества всех его подмножеств 2^X. В то же время *теорема Кантора* 2.4.9 гарантирует, что мощность 2^X всегда больше мощности X[55]. Вот и получается: с одной стороны, в счетном универсуме несчетных множеств нет вообще, но хотя бы одно бесконечное X — есть (аксиома **Z5**); с другой стороны, 2^X — несчетно.

Но противоречия нет. *Теорема Кантора* 2.4.9 на самом деле утверждает, если присмотреться к доказательству, отсутствие биекции между X и 2^X, что в *наивной* (*доаксиоматической*) *теории множеств* было фактически эквивалентом несчетности континуума. Именно в этом смысле «континуум» 2^X несчетен в счетном универсуме $\mathcal{M}$. Счетность 2^X внутри $\mathcal{M}$ непознаваема. Она

[54] Именно версия 7.7.1 здесь лучше подходит, потому что, опираясь на теорему 7.8.1, пришлось бы танцевать от *универсума фон Неймана*, который множеством не является.

[55] Как легко убедиться, доказательство этого факта (п. 2.4.9) проходит в любом универсуме **ZF**.

видна только извне, в надмодели[56]. Поэтому фраза «континуум 2^X можно пересчитать в метатеории» имеет определенный смысл. Но если при этом под 2^X понимать обычный континуум $[0, 1]$, как зачастую делается, получается чушь.

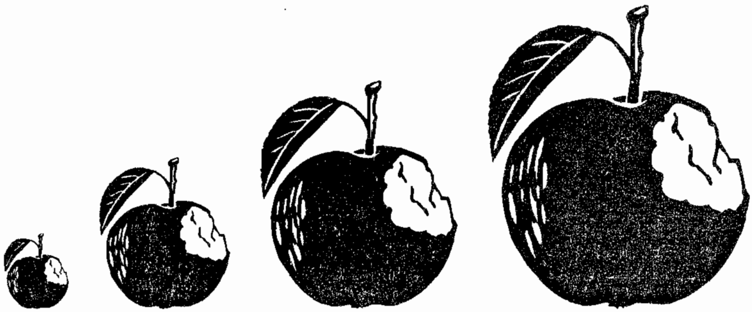
Несмотря на данное исчерпывающее и в общем-то прозрачное объяснение «парадокса», чувство неудовлетворенности остается по другой причине. Множество $X \in \mathcal{M}$ бесконечно, и тогда множество его подмножеств 2^X должно быть (вроде бы) несчетно в обычном смысле. Но роль универсума $\mathcal{M}$ в том и проявляется, что в него входят не все подмножества X (которые видны, может быть, извне, из метатеории), а только те, существование которых можно доказать, вывести из аксиоматики **ZF**, выписывая цепочки формул[57]. А поскольку X счетно и «цепочек» счетное число, то и 2^X будет счетно, если смотреть извне.

Кроме того, счетную модель **ZF** «никто руками не трогал», и что это за чудо — мало кто анализировал. Даже насчет знака принадлежности $\in$ странные мысли закрадываются. Это ведь не то отношение, о котором складывается впечатление из простых примеров. Это лишь предикатный символ, рамки которому задают только аксиомы **ZF**. Но достаточны ли здесь *тиски аксиоматики*, чтобы не впустить в толкование $\in$ какую-нибудь чертовщину? Аксиомы метрики, например, тако́й люфт оставляют, что метрические пространства кишат аномалиями [3, т. 5].

Нестандартные модели. Из *теоремы* 7.8.3 *Лёвенгейма—Сколема о повышении мощности* вытекает существование различных непривычных моделей. Например, несчетных моделей *арифметики Пеано*, всевозможных расширений действительной прямой и т. п. До поры до времени все это казалось никчемным явлением, пока *Робинсон* [17] не приспособил его для точного определения понятий *бесконечно малых* и *бесконечно больших* величин, каковыми

[56] В которой график биекции $f : X \to 2^X$ является элементом универсума, и потому f имеет законную силу.

[57] Собственно, даже счетность $\mathcal{M}$ — феномен метатеоретический, изнутри $\mathcal{M}$ ненаблюдаемый.

$\varnothing$ 

баловались еще *Ньютон* и *Лейбниц*, не утруждая себя приведением в систему. Да и *Ферма* отметился на том же поприще, привлекая для анализа «малое число» $\xi > 0$, обладающее свойством $\xi^2 = 0$. Производная тогда

$$f'(x) = \frac{f(x+\xi) - f(x)}{\xi}$$

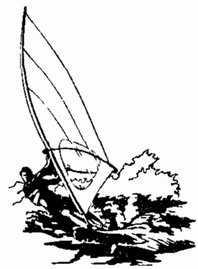
без всяких там пределов и «(ε, δ)-виражей». Однако концы с концами в XVII веке все-таки не сходились, хотя в то время это не так заметно было. Потом стало раздражать.

Современный анализ избавился от *бесконечно малых* ценой введения пагубного для психического восприятия (ε, δ)-языка. Мы тоже в первом томе затратили усилия на разъяснения того, что *бесконечно малая* — это не постоянная, а переменная величина, убывающая так-то. И это, пожалуй, правильный ракурс для общего математического образования, особенно на первоначальной стадии. Но теперь появился *нестандартный анализ* [17], где вполне законны тезисы типа «пусть $\varepsilon > 0$ меньше любого действительного $x > 0$». Надо лишь уметь сводить воедино противоречивые на вид предположения, что собственно и происходит в нестандартных моделях. Доказательства становятся проще, но особой популярностью новая метла пока не пользуется.

Глава 8

Универсумы ZF и форсинг

Интересно, Создатель Поднебесной,
какой аксиоматикой был связан?



Вдали от истоков математика очень слабо использует аксиоматический потенциал. То есть логическая сложность построений в диапазоне от арифметики до топологии невелика, и потому теория множеств в ее фундаментальном значении мало кому нужна. Примерно как шарообразность Земли улитке. Но материей движет дух, повторяя неисповедимыми путями узоры первопричин.

8.1. Имеет ли ZF модель

Универсумы V и L, *фон Неймана* и *Гёделя*, принято считать моделями теории множеств. Строго говоря, это не так. Для существования модели обязательна непротиворечивость аксиоматики, каковая в данном случае принципиально не может быть установлена (раздел 6.4). Конечно, это «беда», к которой все давно привыкли, и непротиворечивость предполагается по умолчанию. Но даже в предположении непротиворечивости статус универсумов V и L, как моделей, не вполне безукоризненный, потому что они не являются «вроде бы» множествами, но тут отчасти выручает счетная модель (теорема 7.7.1, см. также раздел 7.9).

Насчет оброненного «вроде бы» необходимо высказаться отдельно. Дополнение **ZF** аксиомой о существовании ***недостижимого кардинала*** доказывает непротиворечивость **ZF**. Так же как арифметика непротиворечива с позиций **ZF**, потому что из *трансфинитной индукции* вытекает — обыкновенная, и вообще *аксиомы Пеано* оказываются теоремами **ZF**.

8.1.1. *Кардинал ζ называют* ***недостижимым****, если для любого меньшего кардинала $\alpha < \zeta$ мощность множества 2^α меньше мощности ζ.*

Поначалу кажется, что такое определение трещит по швам. Но по здравому размышлению, почему бы не допустить, что маховик аксиомы степени

$$X, \quad 2^X, \quad 2^{2^X}, \quad \ldots$$

не в состоянии превзойти некий барьер мощности. Нечто вроде *формульной недостижимости*. В конце концов, прибавляя по $1/k^2$, $k = 1, 2, 3, \ldots$, тоже ведь не удается уйти в бесконечность. Разумеется, это не аргумент, и спорить можно до хрипоты. Но опыт показывает, что допущение существования *недостижимого кардинала* к противоречиям не приводит.

8.1.2. Аксиома о недостижимом кардинале. *Недостижимый кардинал существует.*

Коэн (1934–2007)

Аксиома 8.1.2, ограничивая сверху рост мощности при последовательном расширении множеств в рамках **ZF**, приводит к построению нормальной модели, устанавливая тем самым непротиворечивость **ZF**. Правда, аксиома несуществования *недостижимого кардинала* «также хороша». *Коэн* склоняется к первой альтернативе: «*...недостижимые кардиналы можно принять, ибо, как показал опыт, это не ведет к противоречиям, и мы развили некоторую интуицию, позволяющую надеяться, что противоречие не появится никогда*».

(!) Несмотря на указанные выше замечания мы тоже будем считать V и L моделями **ZF** в более широком смысле, нежели в определении 7.2.4. Но тогда надо помнить, что из существования «таких» моделей непротиворечивость **ZF** не следует.

8.2. Конструктивный универсум Гёделя

Гёдель
(1906–1978)

Универсум Гёделя L, как уже отмечалось в разделе 3.6, представляет собой класс множеств, конструируемых поэтапно с опорой на то, что уже построено, т. е. формулы и кванторы, как инструменты построения, могут быть обращены лишь к уже сконструированным множествам.

Процесс конструирования можно себе мыслить как последовательное применение операции расширения $\mathrm{Def}(X)$, которая из X производит множество всех подмножеств X, но не всех подмножеств 2^X, а только тех, которые уже были построены на предыдущих шагах. Если, скажем, есть натуральный ряд $\mathbb{N}$ в форме

$$\{\varnothing,\ \{\varnothing\},\ \{\varnothing, \{\varnothing\}\},\ \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\},\ \ldots\},$$

и ничего более, то $\mathrm{Def}(\mathbb{N}) = \{\mathbb{N}, \{\mathbb{N}\}\}$, потому что подмножества $\mathbb{N}$ еще не сформированы. Кстати, от 2^X тоже нельзя требовать охвата всех подмножеств X, которые «видны» извне модели [1)], — что становится понятно, если всмотреться в запись **Z7** и учесть расшифровку (3.2) включения «$\subset$» [2)].

Из сказанного ясно, что построение универсума L по схеме

$$L_0 = \varnothing, \quad L_{\alpha+1} = \mathrm{Def}(L_\alpha), \tag{8.1}$$

и

$$L_\alpha = \bigcup \{L_\beta : \beta < \alpha\}$$

для *предельных ординалов* α, с последующим объединением $L = \bigcup\limits_{\alpha} L_\alpha$, вообще говоря, требует уточнения. Уточнения, собственно, требует

[1)] Иначе говоря, речь можно вести о тех множествах, для обнаружения которых есть инструменты. Если же 2^X понимать буквально, то странно выглядит, например, *измеримость* ***всех*** *множеств по Лебегу* при замене **АС** менее жесткими аксиомами (глава 4). Куда деваются неизмеримые? Они не исчезают, но становятся «невидимы».

[2)] Синтаксическая формалистика снимает многие трудности, возникающие из-за неосмотрительного применения аксиомы **Z7**.

сама макро-операция $\mathrm{Def}(X)$, каковую естественно начинить микро-механизмами, оговорив, какие формулы и какие аксиомы **ZF** можно использовать на каждом шаге. При этом **Z7** заведомо не годится, потому что мешает в кучу то, что уже сделано, и то, что будет сделано[3]. Детально процедуру построения универсума L *Гёдель* и *Коэн* организуют каждый по-своему, но в итоге получается одна и та же наименьшая по включению совокупность множеств, содержащая все *ординалы* и замкнутая относительно простейших теоретико-множественных операций.

8.3. Метатеоретические трансформации

По отношению к дисциплинам типа арифметики или дифуров матлогика является *метатеорией*, поскольку изучает их извне. При этом надтеоретический характер логики служит постоянным источником головной боли, потому что необходимо все время помнить, откуда ведется наблюдение, со стороны или изнутри изучаемой модели $\mathcal{M}$. Взгляды-то внешние и внутренние надлежит увязывать, а возникающие картины получаются то одинаковые, то разные. Если $X \in Y$ внутри модели, то и снаружи это выглядит как $X \in Y$. То же самое можно сказать про утверждение «X — *ординал*» и многие другие *абсолютные формулы*.

8.3.1. *Формула* φ *называется* ***абсолютной***, *если из истинности в* $\mathcal{M} \subset \mathcal{N}$ *вытекает ее справедливость в расширенной модели* $\mathcal{N}$, *и наоборот*[4].

Вот небольшой список *абсолютных формул*:

- $z = x \cap y$, $u = x \cup y$;
- $z = \{x, y\}$ (неупорядоченная пара);
- $z = \langle x, y \rangle$ (упорядоченная пара);
- $z = x \times y$ (декартово произведение);

[3] Но когда модель будет готова, **Z7** в ней должна выполняться.

[4] Разумеется, при условии что переменные φ принадлежат $\mathcal{M}$.

- «z является функцией»;
- «множество z транзитивно».

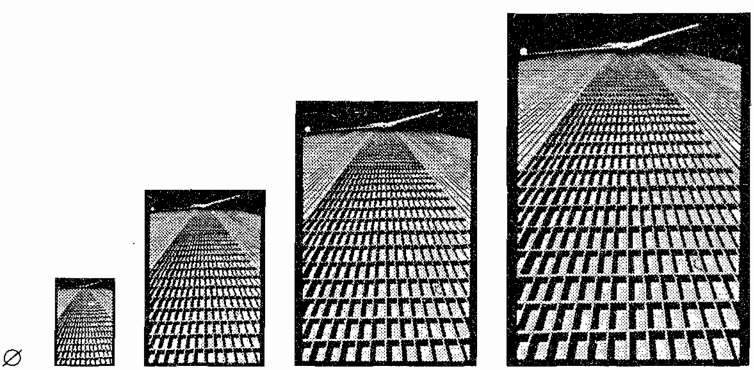
Продолжение списка вместе с обоснованием см. в [19, ч. II, гл. 4]. Нетрудно понять, что абсолютны все *атомарные формулы*, а также формулы с ограниченными кванторами или им эквивалентные.

Существуют также предложения типа

$$«X \text{ — } \textit{счетно}», \quad «X \text{ — } \textit{кардинал}», \quad «X = 2^Z», \text{ —}$$

истинность которых относительна. Если в надмодели X — *счетно*, то в самой модели может не найтись *биекции* с натуральным рядом, а то и самого́ натурального ряда. В $\mathcal{M}$ множество X может быть *кардиналом*, а в надмодели $\mathcal{N} \supset \mathcal{M}$ у X может существовать *биекция* с меньшим *ординалом*[5]. Наконец, у множества $Z \subset \mathcal{M}$ и того же Z, но уже из $\mathcal{N}$ — множества подмножеств могут быть разные, и тогда смысл $X = 2^Z$ расщепляется.

Справедливость *аксиомы выбора* **AC** — тоже явление относительное. Потому что в одних моделях **AC** может выполняться, в других нет — в зависимости от наличия или отсутствия во «внутренней среде» функций выбора. Утверждать сие до некоторых пор



Рисунки А. Фоменко

[5] Иначе говоря, свойство «быть *кардиналом*» зависит от того, какие биекции во «внутренней среде» есть в наличии.

можно было только предположительно, но *Гёдель* и *Коэн* построили соответствующие модели, что уже отмечалось и комментировалось в разделе 3.6. Результат *Гёделя* о справедливости **AC** в *конструктивном универсуме* L довольно прост, и объясняется возможностью «вытянуть» ***все*** множества из L в трансфинитную последовательность, тем самым вполне упорядочивая их, что дает *функцию выбора*, сопоставляющую любому $X \in L$ наименьший элемент X. Справедливость *гипотезы континуума* **ГК** в L устанавливается также просто, хотя и не без мало-мальской волокиты [19, ч. II, гл. 5].

8.3.2. *Если не вникать в детали, причина истинности* **ГК** *в* L *заключается в следующем. Всякое конструктивное подмножество* X *натурального ряда принадлежит некоторому счетному* L_α, *где* α — *счетный ординал* [6]. *Поэтому множество всех конструктивных подмножеств* $\mathbb{N}$, *т. е.* $2^{\mathbb{N}}$, *вкладывается в множество всех счетных ординалов, мощность которого равна* $\aleph_1$. *Так что в* L *получается* $|2^{\mathbb{N}}| \leqslant \aleph_1$. *Противоположное неравенство* $|2^{\mathbb{N}}| \geqslant \aleph_1$ *следует из теоремы Кантора. Окончательно*

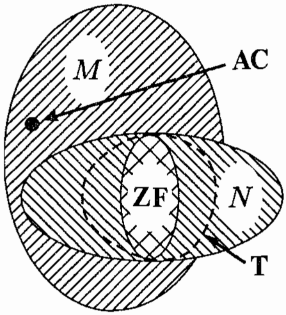
$$|2^{\mathbb{N}}| = \aleph_1.$$

Что касается моделей *Коэна*, в которых **не** выполняются ни **AC**, ни **ГК**, то это уже гроссмейстерские трюки, о которых сказано далее. Пока задержимся на взаимоотношениях теории T с ее моделями $\mathcal{M}$. Вопрос затрагивался в разделах 3.6, 7.3, но здесь стоит кое-что повторить, поскольку именно на взаимодействии аксиоматики теории со специальными моделями базируются результаты о независимости **AC** и **ГК** от **ZF**.

Допустим, теория T с аксиоматикой $\mathscr{P}$ непротиворечива, и $\mathcal{M}$ — модель T. Если формула φ верна в $\mathcal{M}$, то это не значит, что φ следует из $\mathscr{P}$. Истинность φ в $\mathcal{M}$ может проистекать из специфики модели. Но это значит, что «не-φ», т. е. $\neg\varphi$, не принадлежит T. Если же в $\mathcal{M}$ верна формула $\neg\varphi$, то φ — не принадлежит T.

[6] Множество X конструктивно, если оно принадлежит некоторому L_α.

Таким образом, если для непротиворечивой теории удается построить две модели, в одной из которых верна формула φ, а в другой $\neg\varphi$, то это указывает на независимость φ от аксиоматики. Другими словами, можно утверждать, что ни φ, ни $\neg\varphi$ — не являются теоремами T. Именно на этом пути модели *Гёделя* и *Коэна* обнаруживают независимость **AC** и **ГК** от **ZF**.



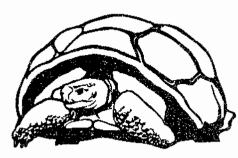
Слева изображена визуальная инсценировка. Аксиоматика **ZF** вложена в теорию T (внутри пунктирной), представляющую собой совокупность синтаксических следствий **ZF**. Две модели M и N, естественно, охватывают T, одна — включает **AC**, другая — нет.

8.4. Аксиома конструктивности

Взаимоотношения универсумов V **и** L в значительной степени остаются неопределенными. *Конструктивный универсум* L представляет собой минимальную по включению модель **ZF**, содержащую все ординалы, тогда как V — максимальную. Тем не менее принципиально нельзя исключить равенства

$$V = L. \tag{8.2}$$

Средства построения, конечно, разные, но итоги теоретически могут быть и одинаковые. Хотя каждый шаг (3.12) по направлению к V имеет взрывной характер, а движение (8.1) к L гораздо медленнее, — для обеспечения $L = V$ *черепахе* вовсе нет необходимости догонять *Ахиллеса*, достаточно проползти по всем точкам, где тот побывал.



Декларация (8.2) представляет собой *аксиому конструктивности*, на данный момент констатирующую не что иное, как обрезание V по контуру L, — иначе говоря, перевод исследования в границы L. Работ, посвященных взаимоотношению V и L, не так много, а диапазон мнений здесь весьма широк — от «почти равны» до «беспрецедентно далеки».

По всей видимости, хороший ответ не будет найден по причине некоторой расплывчатости отдельных аксиом **ZF**. Например, *аксиомы степени*, которая на себе вытягивает все построение универсума V, и утверждает существование множества всех подмножеств любого имеющегося множества.

Но что значит «всех»? В каком смысле? Определенного ответа нет в системе **ZF**. Проблема может показаться надуманной, но это далеко не казуистика. Имеющиеся инструменты должны позволять хотя бы косвенно «просигналить» о существовании множества. Если же оно остается «вещью в себе», никак не дающей о себе знать, то «существует» с равным успехом можно поменять на «не существует». О чем свидетельствует, кстати, *гипотеза континуума*.

8.4.1. Теорема. *Если система* **ZFC** *непротиворечива, то и* «**ZFC**+ $(V \neq L)$» *— непротиворечива.* $\triangleright$

8.5. Пермутационные модели

Всякой теории нужны берега. Для ощущения края и для понимания того, что происходит при изменении условий. Не с целью «жить» в новых обстоятельствах, а с намерением извне оценить данность и, может быть, найти новые инструменты.

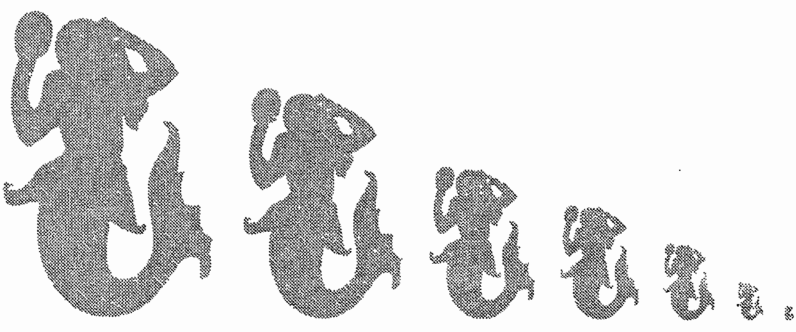
Как раз с этих позиций интересна теория множеств **ZFA** с *праэлементами*, или *атомами*. Интересна не потому, что в нее заманчиво погрузиться и там остаться. Шаг в **ZFA** дает возможность лучше почувствовать ценность и мотивацию системы **ZF**. А кроме того подсказывает новые идеи.

Итак, в **ZF** элементов, собственно, нет. Элементами служат множества, конструируемые из $\varnothing$. В **ZFA** помимо $\varnothing$ вводится *множество A атомов*, каковые могут использоваться в качестве элементов. Понятно, аксиоматика **ZF** должна быть перестроена, по крайней мере косметически. Потому что внедрение в **ZF** инородных сущностей требует разборчивости, особенно при переходе со смыслового уровня на синтаксический, когда здравый смысл уже не работает. Обойтись минимальным добавлением

$$\mathbf{Z^A}.\quad Z \in A \leftrightarrow Z \neq \varnothing \wedge \neg\exists\, X \in Z$$

не удается, ибо атомы вмешиваются в синтаксис аксиом **ZF**. Проблема, конечно, легко решается. Тем не менее возникает новая аксиоматика, поскольку «довесок» A не остается сбоку бантиком, а диффундирует в **ZF**.

Естественно возникает вопрос «зачем это нужно».



Разумеется, не для того, чтобы охватить совокупности типа множества русалок. Числа и функции тоже не нуждаются в статусе *атомов*, потому что их множества легко отождествить с изоморфными представителями в **ZF** (см. раздел 3.5). Поэтому «элемента» $\varnothing$, как строительного блока, хватает вроде бы на все случаи жизни. Вместе с тем в **ZFA** появляются новые, по сравнению с **ZF**, степени свободы, которые бывают неожиданно полезны. В частности, недоказуемость *аксиомы выбора* в системе **ZFA** легко устанавливается с помощью так называемых *пермутационных моделей Френкеля—Мостовского*.

Речь идет о моделях в рамках *универсума Френкеля—Мостовского* FM, который строится по аналогии с *универсумом фон Неймана* V, но его рост начинается не с $\varnothing$, а с $\varnothing$ плюс A. Понятно, что $V \subset FM$ в смысле $X \in FM$, если $X \in V$.

Рассмотрим следующую модель, основанную на идее симметризации. Пусть A *бесконечно*. Всякая перестановка π элементов A порождает преобразование[7] π множеств $X \in FM$. При этом какие-то множества меняются, какие-то — нет. Заведомо не меняются множества $X \in V$, вырастающие без участия *атомов*. Множество $X \in FM$ назовем *симметрическим*, если для него можно указать такое конечное множество атомов $\{a_1, \ldots, a_n\}$ (*основание* X), что $\boxed{\pi(X) = X}$ для каждой перестановки π, оставляющей все точки $\{a_1, \ldots, a_n\}$ неподвижными: $\pi(a_j) = a_j$. Иначе говоря, множество X *симметрическое*, если, не трогая конечного числа атомов, остальные можно переставлять как угодно.

Рассмотрим далее класс $\mathcal{U}$ всех *наследственно симметрических множеств* X (симметрическим является само X, все элементы X, все элементы элементов X и т. д.). Класс $\mathcal{U}$ замкнут в **ZFA**, и потому является моделью **ZFA**. При этом, очевидно, $V \subset \mathcal{U}$; в модель $\mathcal{U}$ входят также: все атомы, ибо каждый атом является своим *основанием*; все множество A; любое конечное подмножество A; а также бесконечные подмножества $Z \subset A$, *имеющие конечные дополнения* $A - Z$. О множествах на верхних уровнях иерархии здесь говорить нет необходимости, а вот на следующий заурядный с виду факт важно обратить внимание.

8.5.1. Лемма. *Бесконечное множество $Z \subset A$, входящее в $\mathcal{U}$, не может иметь бесконечное дополнение $A - Z$.*

◄ Допустим противное, т. е. оба множества Z и $A - Z$ бесконечны. Тогда, каково бы ни было основание $\{a_1, \ldots, a_n\}$, вне $\{a_1, \ldots, a_n\}$ найдутся два атома a и b, один в Z, другой в $A - Z$, которые некоторой допустимой (не затрагивающей основания) перестановкой π меняются местами. В результате $\pi(Z) \neq Z$, $\pi(A - Z) \neq A - Z$. ►

[7] Для простоты используем то же обозначение π.

Лемма 8.5.1 тривиальна по доказательству, но фундаментальна по существу. Из нее сразу следует:

8.5.2. Теорема. *В модели $\mathcal{U}$ аксиома выбора не выполняется. Следовательно,* **AC** *в* **ZFA** *не может быть доказана (не вытекает из аксиом* **ZFA***).*

◀ Если бы **AC** имела место в $\mathcal{U}$, то $A \in \mathcal{U}$ можно было бы разбить на два бесконечных множества Z и $A - Z$, перечисляя элементы A с помощью функции выбора f,

$$a_0 = f(A), \quad a_1 = f(A - a_0), \quad a_2 = f(A - \{a_0, \quad a_1\}), \quad \ldots\ ^{8)},$$

и раскидывая атомы поочередно в Z и $A-Z$. Но тогда возникло бы противоречие с леммой 8.5.1. ▶

8.6. Расширение моделей

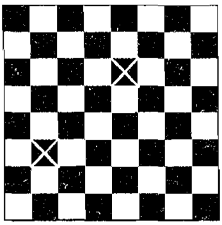
Создание модели — задача архисложная. Особенно из-за туманности района поиска. Неясно, чтó искать. Для чего — объяснимо. Но что и как? Такая проблема встает в любой области, вплоть до Сотворения Мира. Поэтому, чтобы не начинать каждый раз с нуля, пробуют танцевать от уже имеющихся моделей, расширяя их или модернизируя каким-либо способом.

Успехи на пути «расширения» общеизвестны. От натуральных чисел — к действительным, потом — в функциональные пространства. В этой цепочке, правда, как многим кажется, ничего не создавалось, а лишь обнаруживалось уже существующее. Другим, наоборот, кажется, что в Мире все выдумано. В том числе — Поднебесная. И шаг от $\mathbb{R}$ к $\mathbb{C}$ — лишнее тому подтверждение, ирреальность вымысла налицо. Однако к комплексным числам постепенно привыкают, и те мало-помалу как бы «материализуются». Поэтому идею виртуального расширения лучше иллюстрируют малоизвестные модели типа *короткой арифметики*

[8] И трансфинитно продолжая процесс (см. раздел 4.2), если A несчетно. Но для противоречия и счетного варианта A хватает.

Гильберта [3, т. 14], где исходную модель дополняют потусторонними муляжами, но это дает эффект «по сю сторону».

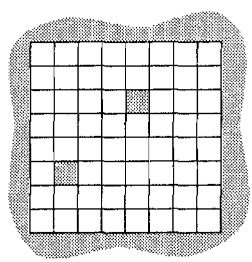
Полезны также пустяковые на вид частные примеры. Рассмотрим известную школьную задачу. *Требуется накрыть фишками домино фигуру, полученную из клетчатого квадрата 8 на 8 удалением двух клеток на одной из диагоналей. Каждая фишка накрывает две клетки.*



◄ Решение с изюминкой тоже хорошо известно. Раскрасим исходный квадрат как шахматную доску. Тогда клетки, расположенные на одной диагонали, имеют одинаковый цвет. Фишка же домино накрывает две клетки разного цвета. Поэтому накрыта может быть только фигура, имеющая одинаковое количество черных и белых клеток. ►

На первый взгляд о теории моделей в смысле п. 7.2.4 здесь речь не идет. Но идеологически ситуация та же самая. Разница лишь в том, что в данном случае интерпретируется одна задача, тогда как в п. 7.2.4 фигурирует интерпретация бесконечной совокупности задач (в рамках данного языка и данной аксиоматики). Когда рассматривается лишь одна задача, адекватность разных интерпретаций исходной постановке, как на ладони — и потребность в наукообразии исчезает.

Исходную задачу можно себе представлять как фрагмент некой теории, имеющей дело с клетчатыми фигурами и некоторым их взаимодействием. При этом никакой окраски. Как будто все происходит в бесцветной Вселенной. В этом случае придание фигурам расцветки представляет собой *внешний трюк* по отношению к исходной модели. Как бы расширение модели за пределы Вселенной, уход в иные измерения.



8.7. Форсинг и теоремы Коэна

Метод форсинга был создан *Коэном* [11] на пути к решению проблемы **ГК**, но оказался чрезвычайно эффективным в решении массы других проблем теории множеств, матлогики и теории моделей. Головоломный характер метода привлек к его доработке и упрощению многих исследователей, и сейчас это уже совсем не та неприступная крепость, которая была изначально. Метод излагается во всевозможных руководствах — например, [7, 11, 12, 19, 22][9], — но в детальном исполнении остается все же предметом не для легкого чтения. По назначению *форсинг* можно было бы охарактеризовать как метод построения *счетно-транзитивных моделей*[10] (СТ-*моделей*), обладающих теми или иными желаемыми свойствами. Подоплека примерно такова.

Допустим, **ZFC** непротиворечива и потому имеет модель V. Тогда по *теореме Лёвенгейма—Сколема* 7.8.1 существует счетная модель $M \subset V$, и даже СТ-*модель* $\mathcal{M} \subset V$, что устанавливается несложным дополнительным рассуждением. Далее, пусть H — некоторое подмножество $\mathcal{M}$ (в приложениях H — основной «рычаг управления» для достижения тех или иных целей) и

$$g : H \to \{0, 1\} \tag{8.3}$$

— некоторая *генерическая функция*[11] (из $V \setminus \mathcal{M}$), с помощью которой модель $\mathcal{M}$ расширяется до СТ-*модели*

$$\mathcal{M}[g] \supset \mathcal{M},$$

называемой *генерическим расширением* $\mathcal{M}$.

Делается это, например, так[12]. Пусть $G \subset 2^H$ — множество функций с конечными областями определения из H в $\{0, 1\}$. На $\mathcal{M}$ вводится отношение $x \overset{g}{\in} y$, определяемое существованием такого $f \in G$, что

$$f \in g, \quad \langle f, x \rangle \in y.$$

[9] См. также [21] и статью: *Cohen P.* The Discovery of Forcing // Rocky Mountain J. Math. 2002. (**32**)4. 1071–1100.

[10] Напомним, множество X *транзитивно*, если из $Z \in Y \in X$ следует $Z \in X$, т. е. если элементы элементов X являются элементами X.

[11] Характеризуемая определенными свойствами, каковые для почти всех функций вида (8.3) выполняются, что, разумеется, требует обоснования.

[12] Методика рассыпалась ныне на ручейки, впадающие в тот же океан.

Затем формируются $\{x\}_g$ как множества множеств $y \in \mathcal{M}$ меньших x по g-включению ($y \overset{g}{\in} x$), после чего $\mathcal{M}[g]$ определяется как

$$\mathcal{M}[g] = \{\{x\}_g : x \in \mathcal{M}\}.$$

Далее устанавливается, что $\mathcal{M}[g]$ также является СТ-*моделью*[13] **ZFC**, причем $\mathcal{M}$ и $\mathcal{M}[g]$ *имеют одни и те же ординалы*, *и* (что довольно неожиданно) — *одни и те же кардиналы.*

Вот как это работает в *доказательстве теоремы Коэна* 3.6.4, которая может быть переформулирована следующим образом.

8.7.1. Теорема. *Если* **ZFC** *имеет модель, то и* **ZFC**$+\neg$**ГК** *имеет модель.*

◀ Выбирая $H \subset \mathcal{M}$ равным $\aleph_0 \times \aleph_2^{\mathcal{M}}$, где $\aleph_2^{\mathcal{M}}$ — *второй несчетный кардинал в* $\mathcal{M}$, получаем, что и в генерическом расширении $\mathcal{M}[g]$ — $\aleph_2^{\mathcal{M}}$ также является *вторым несчетным кардиналом.* Но тогда в $\mathcal{M}[g]$ множество $S \subset 2^{\mathbb{N}}$ подмножеств натурального ряда

$$S_\alpha^g = \{n : g(\alpha, n) = 1\}, \tag{8.4}$$

где ординалы $\alpha \in \aleph_2^{\mathcal{M}}$, — имеет мощность $\aleph_2^{\mathcal{M}}$, что в силу $S \subset 2^{\mathbb{N}}$ свидетельствует о ложности **ГК**[14]. ▶

Все сложности приходятся на разбор полетов с $\mathcal{M}[g]$, т. е. на проверку модельного статуса и выяснение свойств. Что касается непосредственно *форсинга*, или *вынуждения*, то это механизм, спрятанный внутри описанной схемы, и в общем-то имеющий техническое предназначение. Но идеологический его потенциал настолько велик, что метод работает в разном исполнении в довольно широком диапазоне разнокалиберного моделирования.

По большому счету, *вынуждение* — это отношение между «условиями» и формулами, «$p \models \varphi$» — «условие p вынуждает

---

[13] Наименьшей по включению моделью, содержащей в себе $\mathcal{M}$ и g.

[14] Заметим, что в V множество подмножеств (8.4) вовсе не обязано быть *вторым несчетным кардиналом.*

формулу φ»[15]. При этом в множествах типа G вводится полуупорядоченность, и устанавливается, что для $p, q \in G$ из $p < q$ и справедливости формулы φ с параметром p следует справедливость той же формулы с параметром q, т. е.

$$p < q, \quad p \models \varphi \quad \Rightarrow \quad q \models \varphi.$$

Вся эта механика естественным образом применяется для проверки справедливости в $\mathcal{M}$ и $\mathcal{M}[g]$ аксиом **ZF** или **ZFC** и других предложений типа $\neg$ **ГК**.

Описанная выше схема ориентирована на доказательство *теоремы* 8.7.1, и претерпевает определенные изменения при решении иных задач. В частности, для доказательства *теоремы* 3.6.3 генерическая модель $\mathcal{M}[g]$ непосредственно не годится, потому что *аксиома выбора справедлива в* $\mathcal{M}[g]$. Однако между $\mathcal{M}$ и $\mathcal{M}[g]$ удается вклинить промежуточную модель $\mathcal{N}$, в которой истинным оказывается отрицание **AC**. Для конструкции $\mathcal{N}$ используется идея *симметризации имен* как в *пермутационной модели*. Об «именах» в теории множеств часто говорят, но при этом полезно иметь в виду, что множество и его имя — суть одно и то же (с точностью до изоморфизма), хотя лишний синоним иметь удобно, особенно когда слов не хватает.

8.8. Булевозначный анализ

Булевозначный анализ [12] изначально создавался для упрощения *форсинга*. Но результат превзошел ожидания. Средство оказалось универсально, и теперь востребовано во многих областях.

«Булевозначный анализ не только связан со многими топологическими и геометрическими идеями, но и предоставляет технологию расширения содержания уже доказанных теорем. Каждая теорема, доказанная классическими средствами, обладает новым неочевидным содержанием, относящимся к „переменным“ множествам. Точнее говоря, любая доказанная теорема порождает новое

[15] Плохо только, что «условия» — это обычно множества или функции (опять-таки множества как графики), т. е. термины идут вразрез со смысловым значением слов. Да и само «вынуждение» не очень удачный термин.

семейство теорем, занумерованное всевозможными полными булевыми алгебрами или, что то же самое, негомеоморфными стоуновыми пространствами»[16].

На примере **ZF** или **ZFC** суть метода можно описать следующим образом. Отождествим множества с их характеристическими функциями. В этом случае множеству подмножеств 2^X будет соответствовать множество всевозможных $\{0, 1\}$-функций, с областью определения X и областью значений $\{0, 1\}$. С учетом этого обстоятельства *универсуму фон Неймана* V будет сопоставлен аналог $\mathbb{V}^{\{0,1\}}$, состоящий из $\{0, 1\}$-функций. На этапах аналогичных (3.12) множества $\mathbb{V}_{k+1}$ будут множествами $\mathbb{V}_{k+1} = 2^{\mathbb{V}_k}$ всевозможных $\{0, 1\}$-функций

$$\chi : \mathbb{V}_k \to \{0, 1\}. \tag{8.5}$$

Ну а предельные ординалы $\mathbb{V}_\alpha$ определяются по тому же принципу (3.13), после чего $\mathbb{V}^{\{0,1\}}$ образуется как объединение

$$\mathbb{V}^{\{0,1\}} = \bigcup_\alpha \mathbb{V}_\alpha,$$

причем $\mathbb{V}^{\{0,1\}}$ — всего лишь изоморфный вариант V, так что ничего нового. Однако изменение формы переводит модель в другую среду, и возникает трамплин для мутации.

Простой и в то же время гениальный трюк состоит здесь в замене *множества значений* $\{0, 1\}$ характеристических функций множеством $\mathbb{B}$, где $\mathbb{B}$ — любая *полная булева алгебра*, см. раздел 10.4. В результате характеристические функции (8.5) заменяются $\mathbb{B}$-функциями

$$\chi : \mathbb{V}_k \to \mathbb{B},$$

со значениями в $\mathbb{B}$, и универсум $\mathbb{V}^{\{0,1\}}$ расширяется до $\mathbb{V}^{\mathbb{B}}$.

Это ядро идеи. Чтобы конструкция $\mathbb{V}^{\mathbb{B}}$ могла выполнять роль модели **ZFC**, необходимо кое-что сделать. На соответствующем пути устанавливаются *оценки истинности формул*, а также

[16] *Кутателадзе С. С.* Что такое булевозначный анализ? // Сибирские электронные матем. изв. 2006. Т. 3. С. 402–427 (http://semr.math.nsc.ru).

изготавливаются инструменты для работы на территории $\mathbb{V}^{\mathbb{B}}$. В частности, все теоремы **ZFC** из V переносятся в $\mathbb{V}^{\mathbb{B}}$ (*принцип переноса*). Кроме того, методика обрастает всякими другими приспособлениями, обеспечивающими диалог между V и $\mathbb{V}^{\mathbb{B}}$.

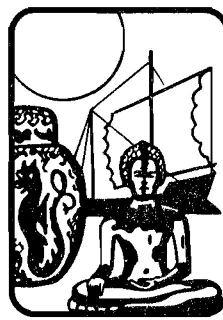
Так или иначе, в результате возникает внешняя по отношению к V модель $\mathbb{V}^{\mathbb{B}}$, характеризуемая плохо интерпретируемыми в ощущениях (плохо укладывающимися в голове) объектами и совершенно новыми (ранее неизвестными) процедурами проверки формул. Фантом получается как бы из другого мира. Тем не менее это модель, и она способна проливать свет, а широкий диапазон выбора *булевой алгебры* $\mathbb{B}$ дает огромную свободу маневра. При этом, несмотря на инопланетный дух булевозначных муляжей, переходы типа «от V к $\mathbb{V}^{\mathbb{B}}$» выглядят более естественно для воображения, развившегося в земных условиях.

Глава 9

Метафизическая

Imagination rules the world.

Napoleon Bonaparte



Философская надстройка над метаматематикой — это такая область всеобщей некомпетентности, где самовыражаться можно без опасения быть убедительно опровергнутым. В то же время эта неблагонадежная сфера чрезвычайно важна для развития науки. Потому что приходится вставать на заблуждения, чтобы увидеть горизонты. Потому что формализованные дороги кончаются, а для создания новых — важны не столько новые идеи, сколько освобождение от предыдущего гипноза. Потому что направляющая стратегия кончилась, и куда идти неясно. А под рукой ничего, кроме интуиции.

9.1. Вселенная как модель

Выдуманная ли штука математика? Или физика? Разумеется, выдуманная. Но выдумывалась-то она из ощущений и помыслов этого Мира. Из наблюдений физических явлений в условиях «близорукости» под аккомпанемент безотчетных интерпретаций. То есть в пределах генотипически сдерживаемых фантазий. В результате, собственно, и появились точные науки [1] и математика, как их виртуальная основа.

[1] Да и неточные.

Но потом многое стало рушиться, потому что в бесхитростной картине мира обнаружились противоречия, а за лицевой стороной происходящего стали проглядываться причины другого уровня. Осязаемые картины на первом плане начали расплываться, и превратились в муляжи. Сформированные тысячелетиями и устоявшиеся понятия вдруг перестали служить опорой, потеряв смысл и ореол подлинности. Особенно ярко это проявилось в *теории относительности* и в *квантовой механике*.

Шаг в микромир взорвал представления классической физики. Сначала под грузом противоречий рухнула модель атома *Резерфорда*. В новой модели *Бора* от элементарных частиц остались одни названия. Электрон из электрически заряженного шарика превратился в фикцию, обязанную пребывать в непонятных состояниях и совершать какие-то квантовые скачки. Короче, новая модель констатировала экспериментально установленные эффекты, но ничего не объясняла.

И тут *Луи де Бройль* заговорил о волнах материи. Без всяких к тому логических оснований. Единственным оправданием была аналогия с волновыми процессами, в которых частоты колебаний, как правило, дискретны. Не такова ли природа дискретности излучения атома, — призадумался *де Бройль*. Но здесь-то что колеблется?

Де Бройль (1892–1987)

Не дожидаясь пока выяснится, что колеблется, *Шрёдингер* подобрал уравнение колебаний, гениально игнорируя возникающие по ходу дела безответные вопросы. Что колеблется, до сих пор неясно, но *фокус в целом* работает. Вопрос о природе колебаний был закрыт «волнами вероятности». Однако теперь авторитет теории достаточно велик, чтобы «волны вероятности» заменить эквивалентной формулировкой «колеблется непонятно что». Короче говоря, процесс завершился по *Планку*, который говорил, что научная истина торжествует по мере того, как вымирают ее противники.

История показательна не только сама по себе, но и как образец современных физических исследований, уходящих от всего, что доступно на ощупь. Поэтому в той или иной степени правдоподобная реконструкция сценария заслуживает внимания.

Напряженность электрического поля вдали от гармонического излучателя меняется по закону

$$E = E_0 e^{i(\omega t - kr)}, \tag{9.1}$$

где ω — круговая частота, k — волновой вектор, r — радиус-вектор.

Поскольку *де Бройль* приписал частицам длины волн по аналогии с фотонами, то в качестве волновой функции было естественно испробовать (9.1) с заменой E на «непонятно что». Так возникла волновая функция

$$\psi(r,t) = \psi_0 e^{\frac{i}{\hbar}(Et - pr)}, \tag{9.2}$$

Шрёдингер
(1887–1961)

отличающаяся от (9.1) перезаписью параметров с учетом хорошо известных связей

$$E = \hbar\omega, \quad p = k\hbar,$$

где $\hbar$ — постоянная Планка, деленная на 2π.

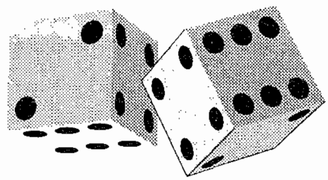
Уравнение для (9.2) легко подбирается дифференцированием [2]. С учетом

$$\frac{p_x^2 + p_y^2 + p_z^2}{2m} = E$$

получается *уравнение Шрёдингера*

$$\frac{\partial\psi}{\partial t} = \frac{i\hbar}{2m}\left(\frac{\partial^2\psi}{\partial x^2} + \frac{\partial^2\psi}{\partial y^2} + \frac{\partial^2\psi}{\partial z^2}\right). \tag{9.3}$$

Сценарий заслуживает того, чтобы его пережить. Если в электродинамике решением волнового уравнения служит колебание измеряемой величины, а использование комплексных решений — вопрос удобства, то зде ь наоборот. Физической интерпретации колебаний нет, а волновая функция изначально определяется как комплексная, чтобы меньше было поводов для критики. И если бы речь шла только о поиске дискретных спектров, то все можно было бы списать на требования удобства, считая ψ-функцию полезной *фикцией* для промежуточных действий. Но в квантовой механике есть масса других задач, и потому «фикцию» приходится извлекать на свет и приспосабливать, например, для изучения интерференции электронов. Вопрос интерпретации ψ-функции в этом случае становится острее, но в общепринятом смысле он так и не решается. Поиски логики останавливаются на волнах вероятности, что, надо признать, является оптимальным выходом из положения, ибо внешняя сторона дела похоже вероятностна — и язык в какой-то мере адекватен. Возникает непривычная ситуация. Квантовая механика справляется с обширным кругом явлений в отсутствие их понимания. Физики насчет понимания могут спорить, но это вопрос терминологии.



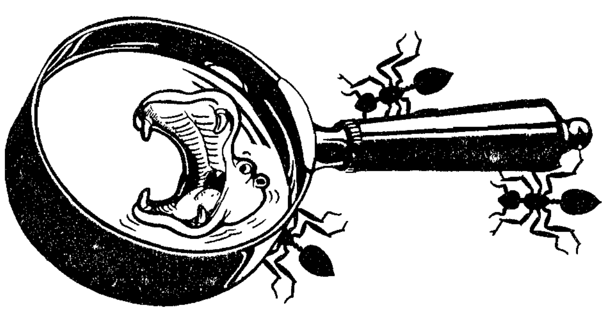
Если кому-то в данном выше описании чудятся издевательские нотки, то их нет. Здесь, скорее, восхищение. Потому что явно шизофренический стиль мышления демонстрирует феноменальную эффективность. «Колеблется непонятно что», как Оно связано с реальностью — не ясно, но в итоге вычисления дают «правильные результаты» в проекции на измеряемые параметры. И квантовая механика, слава Богу, постепенно становится на эту платформу аксиоматического толка, переставая вешать населению лапшу на уши по поводу корпускулярно-волновой природы частиц. Все постепенно скатывается к очень симпатичной позиции: «мы не знаем почему, но такой рецепт дает правильный результат». Американцы в подобных ситуациях легко смиряются. Но русскому человеку без «почему» результат не нужен. И это до некоторой степени трагедия, либо счастье, ибо сия загадка, по-видимому, непробиваема.

Использование вспомогательных моделей для описания физических явлений, вообще говоря, не новость. Комплексная плоскость — явно выдумка, но вычисления в $\mathbb{C}$ для блага, скажем, электротехники — не производят впечатления «не от мира сего». Потому что природа объекта ясна (таково впечатление), а связь с вычислениями ментально прослеживается. То есть условность присутствует, но она мысленно осязаема. С элементарными частицами все иначе. Природа объекта не ясна, связь с вычислениями находится «по ту сторону» и никакой естественной интерпретации не поддается.

Нечто подобное наблюдается всегда, когда внимание выходит за пределы обыденного диапазона. Трафаретные концепции расползаются. Представление о частице как о «твердом шарике» не просто деформируется с помощью каких-то поправок вразумительного толка, а превращается в «ничто», обладающее немыслимыми свойствами. То же самое происходит при попытке выйти из области привычных скоростей и вообще привычных масштабов пространства и времени, чему хорошим примером служит *специальная теория относительности* (СТО) [2].

Оба этих примера, квантовая механика и СТО, демонстрируют зыбкость понятий, формируемых естественным жизненным опытом. При этом квантовая механика сразу совершает прыжок через пропасть, увлекая нас в сумасшедший дом, где исходное понятие материальной частицы перестает служить опорой. *Теория относительности* более консервативна в своем стремлении придерживаться догм прошлых веков. Понятия времени, пространственной координаты, скорости, — остаются в первозданном виде, но для «зашкаливающих» значений их взаимодействие приобретает совершенно дикие формы, чтобы избежать противоречий. Сумасшедший дом другой, но результат тот же:

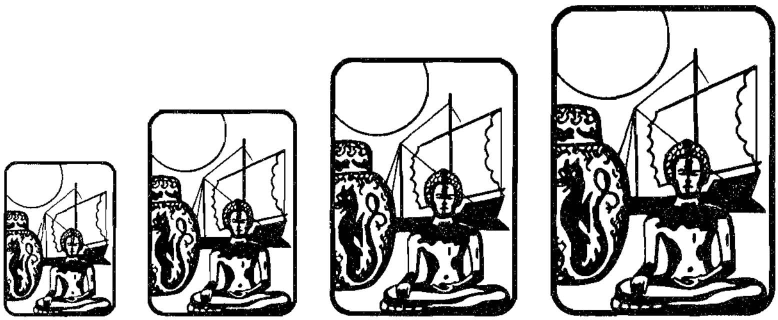
9.1.1. *Модельные представления о мире, созданные «не выходя из дома», на просторах Вселенной перестают работать.*



[2] Каковая, между прочим, ничего не объясняет, но передвигает загадку из одного места в другое, организуя весь клубок противоречий в теорию вокруг «единственного» постулата — постоянства скорости света.

9.2. Феномен познания

Интересно, что в математике, кажущейся стерильной и независимой, происходит то же самое. Конечно, никакой «стерильности и независимости» нет. Человек, как психологическая надстройка над своим ограниченным опытом, «инфицирован» и зависим. И его действия во всех направлениях подвержены влиянию приобретенного опыта и неосознанно преследуемых целей.



Разве *теория множеств* является плодом свободного ума? Да нет же. Аксиоматику формируют впечатления и намерения. При этом в дело вступает воображение, создающее и консервирующее образы. Затем *инерция воображения* набирает такую силу, что выдуманное уже не пускает в сторону.

Возьмем для примера гештальт *континуума* как образец материализованного призрака. Созданный воображением и взаимным гипнозом, континуум стал «живее всех живых». И потому, скажем, независимость *гипотезы континуума* не укладывается в голове. Даже великий *Лузин* говорил: «Мощность continuum'а, если только мыслить его как множество точек, есть единая некая реальность и она должна находиться на алефической шкале там, где она на ней есть». Вот более полная цитата:

«Первое, что приходит на ум, это то, что установление мощности continuum'а есть дело свободной аксиомы, вроде аксиомы о параллелях для геометрии. Но в то же время, как при инвариантности всех прочих аксиом геометрии Евклида и при варьировании аксиомы о параллельных меняется самый смысл

Лузин
(1883–1950)

произнесенных или написанных слов: „точка“, „прямая“, etc. — смысл каких слов должен меняться, если мы делаем мощность continuum'а подвижной на алефической шкале, все время доказывая непротиворечивость этого движения? Мощность continuum'а, если только мыслить его как множество точек, есть единая некая реальность и она должна находиться на алефической шкале там, где она на ней есть; нужды нет, если определение этого места затруднительно или, как прибавил бы J. Hadamard, „даже невозможно для нас, людей“».

Вот это и есть *инерция воображения*. Отрезок $[0, 1]$ не Богом создан, а придуман человеком, причем стойт на некоторых посылках. И сильно меняется при смене предположений. Но все время помнить об этом трудно. Образ окаменел в подсознании. В результате кажется, что «промежуточное по мощности множество» там либо есть, либо его там нет. Уж *Лузин* как никто другой понимал, что говорить о наличии тех или иных множеств внутри $[0, 1]$, а уж тем более об их мощности, — бессмысленно в отрыве от модели, в которую $[0, 1]$ *согласованно* погружен. Притом графики необходимых *биекций* не могут быть исключены или включены по прихоти в эту модель. Эти «графики»[3], в свою очередь, обязаны быть согласованы с *универсумом* модели. Вот такой бюрократический хвост тянется за *континуумом*, но об этом хвосте в суете будней как-то не вспоминается.

Понятие *множества* дает наглядный пример того, как любое явление начинает рассыпаться по мере углубления в него. Изначально множество представляется очень естественным и простым понятием. Что проще может быть феномена «*совокупности элементов*»? Но всматриваясь и уточняя, мы вынуждены забираться в такие дебри, что от первого определения остается дырка от бублика. Сначала наивная точка зрения ломает себе зубы на «бесконечности», и от разнообразия мнений приходится спасаться юридическими средствами, декларируя ту или иную аксиоматику. В результате возникает некоторый формализм типа

[3] Стоящие в стороне от $[0, 1]$.

ZFC, играющий роль «судебной системы», принципиально неспособной решить массу вопросов, не говоря о фундаментальной проблеме «непротиворечивости законодательства»[4]. Кроме того, аксиоматика уводит от множеств в сферу регламента допустимых действий. Мы-то хотели заняться «существительными», а теория получается «о глаголах»[5]. И в эту «глагольную» систему ZFC вписываются совершенно разные модели — неясно, какую принять. И чем дальше идет теория, тем более по ходу дела ветвятся и трансформируются понятия, уходя на совсем другие этажи, откуда изначальные воззрения даже не видны.

9.2.1. *Представления о мире, возникшие «естественно» либо созданные кустарными способами, всегда приблизительны и, если работают, то «только дома».*

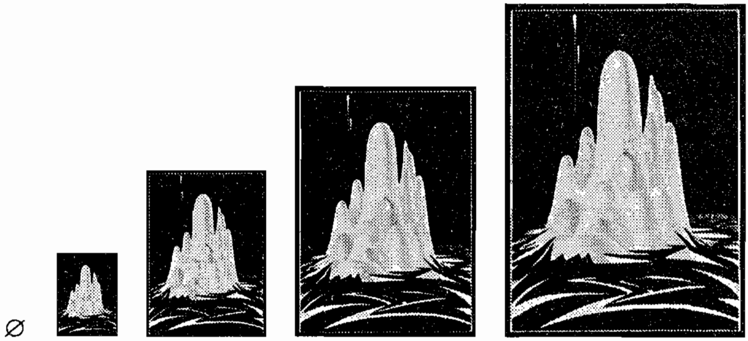
9.3. Бесконечное

Проблема бесконечности — проста, как выстрел из пистолета, но в ней один к одному отражается тайна Вселенной. Игнорировать — невыносимо, постичь — невозможно. Модели типа замкнутого пространства — не спасают. Ибо «во что» погружена модель? И как устроен Мир, и Кто его создал, и Как сумел? И кто создал Того, кто создал Мир?

Бесконечность обнаруживает себя в любом направлении — надо лишь внимательно присмотреться. Например, если речь идет о физическом пространстве, то ограниченность размерности не приводит к эмоциональному дискомфорту. Трехмерность *Среды* представляется вполне естественной, и потребности рассматривать пространства бóльших размерностей, куда все погружено, не возникает. Вроде бы. Потому что не вполне ясно, что будет, если человека долго приучать к многомерным вложенным друг в друга пространствам. Не возникнет ли у него «проблемы бесконечности» в связи с размерностью?

[4] Причем дело вовсе не в «сыгранности» ZFC.

[5] Так и в физике, если только оная не останавливается на полпути.



Рисунки А. Фоменко

Что же касается *длины*, то соответствующая «проблема» возникает автоматически, ибо система ощущений так устроена. Но теорфизика-то стоит на́д «заблуждением чувств». Тем не менее — не может обойти понятие пространства. Как-то, конечно, выкручивается, модифицируя, — в микро- и макромире. Но, может быть, недостаточно решительно. Может быть, кардинально надо изменить концепцию. Конечно, отказ от парадигмы пространства и времени звучит диковато. Потому что свыклись. Но вполне вероятно, что глубина нашего космического непонимания покоится на переносе доморощенных понятий на все Мироздание. Таково ли Пространство, каким оно кажется локально? Не оборачивается ли ***Пространством в окрестности бытия*** — нечто совсем другое? И главное, откуда Оно берется? Если «оттуда», то из чего происходит это «оттуда». И так опять до бесконечности, что порождает еще одну нескончаемую иерархию. Так что все дороги ведут в бездонную воронку.

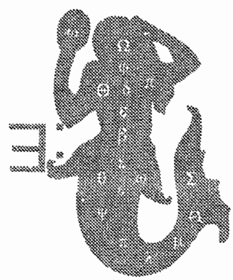
Глава 10

Приложения

When we try to separate anything out by itself,
we find it hitched to everything else in the Universe.

Muir's law

Ниже приводится информация о различных теоретико-множественных конструкциях, каковая разбросана по другим томам, и здесь представлена в более-менее консолидированном виде, иногда в сжатом, а местами и в расширенном формате.



10.1. Вещественные числа

Занимаясь анализом, думать об аксиомах **ZF** совсем не обязательно. Ра́вно как в автобиографии этап развития от сперматозоида до окончания средней школы можно обойти молчанием, хотя именно на этом этапе почти все закладывается. Так и здесь. Начинать можно даже не с натуральных чисел, а прямо — с вещественных.

При этом надо иметь в виду, что геометрическая наглядность континуума $[0, 1]$ мешает видеть наличие проблемы. Использование десятичного представления чисел,

$$0{,}\alpha_1\alpha_2\ldots = \sum_{k=1}^{\infty} \frac{\alpha_k}{10^k}, \tag{10.1}$$

не спасает, потому что куда ряд сходится? Иррациональных чисел-то еще нет. И получается замкнутый круг. Поэтому прыжок в иррациональный океан требует теоретической подпорки. Можно, например, вещественные числа определить как пределы *фундаментальных последовательностей* $x_1, x_2, \ldots$ из рациональных чисел. Но заполнится ли при этом вся числовая ось $\mathbb{R} = (-\infty, \infty)$. Неясно ведь, не дадут ли *фундаментальные последовательности* из уже определенных вещественных чисел в пределе новые числа. И еще масса вопросов: как *последовательности Коши* отождествлять, не имея априори в распоряжении самих пределов; как организовать упорядочение и т. п. Так что проблема введения иррациональных чисел не так проста. Но и не так сложна, конечно, хотя у *Фихтенгольца* на неторопливое изложение уходит полсотни страниц.

Общепринятое ныне построение теории вещественных чисел опирается на дедекиндовы сечения.

10.1.1. *Непустое множество A рациональных чисел определяет* **сечение** *Дедекинда $d(A)$ при выполнении двух условий*:

1. *Если $\alpha \in A$, $\beta < \alpha$ и β — рациональное число, то $\beta \in A$.*
2. *В A нет наибольшего числа*[1].

Подготавливая почву для сечений стать числами, необходимо определить для них понятия больше, меньше, равенства, суммы и т. д. Это легкая и немного скучная задача. Например, неравенству $d(A) < d(B)$ приходится сопоставить строгое включение: $A \subset B$, но $A \neq B$. Сумме $d(A) + d(B)$ — сечение множества $A + B$, состоящего из рациональных чисел $\alpha + \beta$, где $\alpha \in A$, $\beta \in B$. Чтобы такие определения имели смысл, надо проверить стандартные условия, которым они обязаны удовлетворять. Скажем, отношение неравенства должно быть транзитивно:

$$\alpha < \beta, \quad \beta < \gamma \quad \Rightarrow \quad \alpha < \gamma.$$

[1] Если бы речь шла об A, состоящем из рациональных $x < 3$, то на роль сечения годилось бы число 3. Но в случае «$x^2 < 2$» указать сечением $\sqrt{2}$ пока нельзя, поскольку игра начинается в отсутствие иррациональных чисел.

В данном случае это обеспечивается транзитивностью строгого включения для множеств:

$$A \subset B,\ B \subset C \Rightarrow A \subset C.$$

Так же легко проверяются обычные свойства сложения для сечений. И так далее. Короче, все это рутинная работа, которая заканчивается определением на сечениях обычных числовых операций. После этого *термин «сечение» приравнивается термину «вещественное число»*. Рациональные сечения — множество элементов $x < \alpha$, где α рационально — оказываются рациональными числами. Все другие сечения называются — *иррациональными*.

Вопрос о полноте $\mathbb{R}$ решается *основной теоремой Дедекинда*:

10.1.2. Теорема. *Любое сечение в области вещественных чисел является вещественным числом.*

◄ Пусть сечение определяется множеством A вещественных чисел. Пусть A_r — множество всех рациональных чисел из A. *Вещественное число*[2] $\sup A_r$ определяет сечение A, как множество чисел $x < \sup A_r$. ►

Легко видеть, что действительная прямая $\mathbb{R}$, получаемая с помощью *сечений Дедекинда*, оказывается *плотной* и не имеет *щелей*.

10.1.3. *Линейно упорядоченное множество X называют* ***плотным***, *если между любыми двумя его элементами имеется по меньшей мере еще один элемент в X.*

Примером *щели* может служить, скажем, множество рациональных чисел без $x = 2$. Сечение $\langle x < 2, x > 2 \rangle$ будет *щелью*. Это базируется на несколько иной форме определения сечения.

---

[2] Точная верхняя грань $\sup M$ ограниченного сверху множества M определяется как сечение Дедекинда, задаваемое множеством Γ верхних граней γ, таких что $\gamma > m$ для любого $m \in M$. Легко убедиться, что дополнение Γ' удовлетворяет условиям определения 10.1.1 и поэтому $d(\Gamma') = \sup M$ является сечением.

10.1.4. *Сечением* $\langle A, B\rangle$ *линейно упорядоченного множества* X *называют разбиение* X *на два непустых подмножества* A *и* B, *таких что любой элемент из* A *предшествует любому элементу из* B. *Если в сечении* $\langle A, B\rangle$ *у* A *нет последнего элемента, а у* B *— первого, то говорят, что* $\langle A, B\rangle$ *имеет* ***щель.***

Описанная выше процедура добавления чисел, соответствующих сечениям, имеющим щели, ликвидирует все щели, и множество оказывается *полным по Дедекинду* (без щелей).

10.2. Гипотеза Суслина

В рамках **ZFC** представляет интерес не только построение моделей системы в целом, но и рассмотрение отдельных множеств с помощью фиксации дополнительных свойств. В этом направлении любопытна следующая *гипотеза Суслина.*

10.2.1. SH. *Линейно упорядоченное множество без концевых точек, плотное и полное по Дедекинду, у которого каждое семейство попарно непересекающихся интервалов не более чем счетно, — порядково изоморфно действительной прямой* $\mathbb{R}$.

Если условие насчет «непересекающихся интервалов» заменить требованием *сепарабельности*, п. 10.2.1 превращается в известную теорему, от которой *Суслин*, надо полагать, и отправлялся, формулируя свою гипотезу.

Судьба **SH** похожа на судьбу **ГК** — не по накалу страстей, конечно. Просто *гипотеза Суслина* шла вторым номером и пришла к тому же финишу, оказавшись, как и **ГК**, независимой от **ZFC**, что установлено было методом *форсинга* усилиями *Йеха*, *Тененбаума* и *Соловея.*

10.3. Алгебраические поля

Помимо континуума практический интерес имеют и другие числовые поля, причем не обязательно континуального размаха. Например, алгебраические числа, над которыми парит теория многочленов, в совокупности образуют счетное множество, построение которого гораздо сложнее конструкции более мощного $\mathbb{R}$. И там есть довольно красивые виражи и весьма неожиданные результаты (хотя бы *теорема о примитивном элементе* или, скажем, странные закономерности *круговых многочленов*), подробности в [3, т. 8].

10.3.1. Теорема о примитивном элементе. *Любое алгебраическое расширение F поля P нулевой характеристики может быть порождено одним **примитивным элементом**.*

При изучении расширений полей важную роль играют ***круговые многочлены***

$$\Phi_n(x) = (x - \varepsilon_1)\dots(x - \varepsilon_r),$$
$$r = \varphi(n),$$

корнями которых служат исключительно *примитивные корни* из единицы.

В случае простого n

$$\Phi_n(x) = x^{n-1} + \dots + x + 1.$$

В общем случае для вычисления $\Phi_n(x)$ приходится вникать в теоретико-числовую специфику. Начало ряда выглядит так:

$$\Phi_1(x) = x - 1, \qquad \Phi_2(x) = x + 1,$$
$$\Phi_3(x) = x^2 + x + 1, \qquad \Phi_4(x) = x^2 + 1,$$
$$\Phi_6(x) = x^2 - x + 1, \qquad \Phi_8(x) = x^4 + 1,$$
$$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1.$$

Создается впечатление, что коэффициентами $\Phi_n(x)$ могут быть лишь ± 1. Такая закономерность прослеживается довольно далеко. Но уже один из коэффициентов $\Phi_{210}(x)$ оказывается равным 2, а далее — *коэффициенты $\Phi_n(x)$ могут быть любыми целыми числами*. Удивительной может показаться даже сама целочисленность коэффициентов $\Phi_n(x)$.

10.4. Булевы алгебры

Дж. Буль
(1815–1864)

Во многих дисциплинах на авансцену выходят не обязательно числовые множества. Одна из таких весьма эффективных в приложениях структур — *булева алгебра*, представляющая собой, по определению, дистрибутивную *решетку с дополнениями* и не равными друг другу *нулем* $\mathbf{0}$ и *единицей* $\mathbf{1}$.

10.4.1. *Частично упорядоченное множество E называют* ***решеткой****, если любая пара элементов $x, y \in E$ имеет как супремум*[3] $\sup\{x, y\}$, *так и инфимум* $\inf\{x, y\}$.

При изучении решеток широко используются обозначения

$$\sup\{x, y\} = x \vee y,$$
$$\inf\{x, y\} = x \wedge y.$$

Решетку E называют *дистрибутивной*, если для любых элементов $x, y, z \in E$ выполняются равенства[4]

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z). \tag{10.2}$$

Понятно, что операции $\wedge$, $\vee$ удовлетворяют требованиям (аксиомам) *коммутативности*

$$x \vee y = y \vee x, \quad x \wedge y = y \wedge x, \tag{10.3}$$

ассоциативности

$$x \vee (y \vee z) = (x \vee y) \vee z, \quad x \wedge (y \wedge z) = (x \wedge y) \wedge z, \tag{10.4}$$

а также *законам поглощения*

$$x \vee (x \wedge y) = x, \quad x \wedge (x \vee y) = x, \tag{10.5}$$

[3] *Супремум* $\sup A$ подмножества $A \subset E$ определяется как наименьший элемент в множестве всех верхних границ A. *Инфимум* $\inf A$ — как наибольший элемент в множестве всех нижних границ множества A.

[4] Двойственное (10.2) соотношение:

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$$

Если в *решетке* E имеются наименьший и наибольший элементы $\mathbf{0}$ и $\mathbf{1}$, и для каждого $x \in E$ существует единственный дополнительный элемент $\neg x$, такой что

$$x \vee \neg x = \mathbf{1}, \quad x \wedge \neg x = \mathbf{0}, \tag{10.6}$$

то E называют *решеткой с дополнениями*.

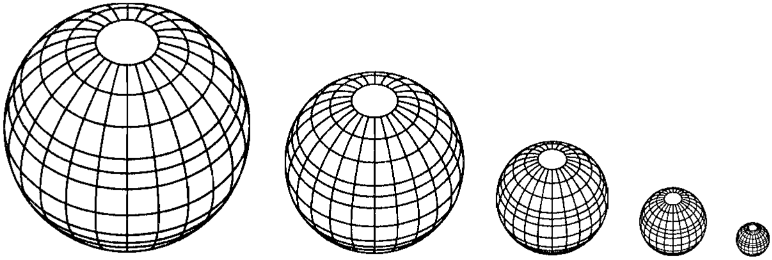
Наконец, как уже отмечалось, ***булевой алгеброй*** называется дистрибутивная *решетка с дополнениями* и неравными друг другу *нулем* $\mathbf{0}$ и *единицей* $\mathbf{1}$.

Нетрудно сообразить, что́ здесь стоит за кадром. Если взять произвольное непустое множество X, то множество всех его подмножеств будет *булевой алгеброй* $\mathbb{B} = 2^X$, в которой частичный порядок определяется включением $\subset$, а операциям $\vee$, $\wedge$, $\neg$ отвечают теоретико-множественные операции *объединения* $\cup$, *пересечения* $\cap$ и *дополнения* «$'$».

Понятно, что присутствие в $\mathbb{B}$ *всех* множеств 2^X необязательно. *Булевой алгеброй* будет и любая система множеств $\mathbb{B} \subset 2^X$, замкнутая по операциям $\cup$, $\cap$, «$'$», и содержащая $\varnothing$ и X. Правда, соответствующая замкнутость в случае $\mathbb{B} = 2^X$ очевидна, тогда как подходящие варианты $\mathbb{B} \subset 2^X$ не так легко указать. Разумеется, за исключением тривиального случая $\mathbb{B} = \{\varnothing, X\}$, который лежит в основании математической логики [3, т. 6].

Указанный пример является универсальным, в том смысле что *любая булева алгебра может быть реализована в виде семейства множеств* $\mathbb{B} \subset 2^X$, *замкнутого по операциям* $\cup$, $\cap$, «$'$» *и содержащего* $\varnothing$ *и* X (*теорема Стоуна*).

Иногда говорят, что при определении булевой алгебры не надо бы наводить тень на плетень, а лучше сразу начинать с «замкнутых по операциям» семейств множеств, раз уж с точностью до изоморфизма, по *теореме Стоуна*, к тому все сводится. Но это аналогично предложению свести теорию алгоритмов к машинам Тьюринга. Содержательное разнообразие булевых алгебр довольно велико [6], и его легко потерять, сводя все к одной схеме.



Семейства множеств — это просто инструмент, на котором можно сыграть любую «булеву мелодию».

Заметим, если X топологическое пространство, то *система всех открыто-замкнутых подмножеств X образует булеву алгебру.* Однако в естественных топологиях обычно есть только два множества $\varnothing$ и X, которые одновременно открыты и замкнуты. Чтобы алгебра открыто-замкнутых множеств была нетривиальной, необходимо ввести дополнительные ограничения на топологию X. Если X *вполне несвязно*[5], то это обеспечивает наличие в X достаточного числа открыто-замкнутых множеств, и *теорема Стоуна* теперь звучит так: *какова бы ни была булева алгебра $\mathbb{B}$, существует вполне несвязный компакт (пространство Стоуна), алгебра всех открыто-замкнутых множеств которого изоморфна* $\mathbb{B}$.

В целом *булева алгебра* представляет собой обширную дисциплину с красивыми и весьма эффективными в прикладном отношении результатами. За соответствующей информацией можно обратиться к источникам, не ограниченным рамками одного параграфа, см. [6]. Остановимся только на аксиоматически-модельной стороне дела.

Использованный выше описательно-индуктивный способ введения *булевых алгебр* легко модифицируется, причем «неузнаваемо» — благодаря большому числу внутренних взаимосвязей в системе. Некоторые из таких взаимосвязей лежат почти на по-

[5] То есть открыто-замкнутые множества образуют его *базис*.

верхности, как например, *принцип двойственности*[6], позволяющий автоматически получать новые соотношения из имеющихся — переходом к двойственным функциям[7]. Другие взаимосвязи скрыты довольно глубоко и служат источником задач, решаемых десятилетиями.

Итак, *булева алгебра* может быть определена, в том числе, как аксиоматическая система (10.2)–(10.6), которая, в свою очередь, допускает значительные вариации, оказываясь, например, эквивалентной системе (10.3), (10.4) плюс

$$\neg(\neg x \vee y) \vee \neg(\neg x \vee \neg y) = x \quad (\textit{аксиома Хантингтона});$$

либо плюс

$$\neg(\neg(x \vee y) \vee \neg(x \vee \neg y)) = x \quad (\textit{аксиома Роббинса}).$$

Эквивалентность аксиом *Хантингтона* и *Роббинса* в данном контексте не поддавалась обоснованию около 60 лет. Хороший пример на тему, как в трех соснах можно плутать всю жизнь.

10.5. Конструктивизм

Взгляд на числа, как и вообще на Мир, сильно зависит от философской позиции. Интуиционисты, например, отрицали *континуум* как множество точек, а рассматривали его как «среду становления точек». А убеждения в необходимости все поставить на конструктивную основу мало что оставляли от математики. При этом парадигма конструктивизма время от времени пробуждается, особенно в связи с веяниями теории алгоритмов (глава 6), каковая в классических областях ведет к крайнему «экстремизму».

---

[6] Рассмотренный в [3, т. 6] применительно к булевой алгебре $\{\mathbf{0}, \mathbf{1}\}$, но сохраняющий силу и в общем случае.

[7] Функция $\varphi(x_1, \ldots, x_n)$, образованная элементарными операциями $\vee$, $\wedge$, $\neg$, называется *двойственной* по отношению к $\psi(x_1, \ldots, x_n)$, если

$$\varphi(x_1, \ldots, x_n) = \neg\psi(\neg x_1, \ldots, \neg x_n),$$

где у $\psi(x_1, \ldots, x_n)$ все «конъюнкции» $\wedge$ меняются на «дизъюнкции» $\vee$, «дизъюнкции» — на «конъюнкции», $\mathbf{1}$ на $\mathbf{0}$, $\mathbf{0}$ на $\mathbf{1}$.

При десятичной записи чисел (10.1) естественно задаться вопросом, как и чем α_n определяются. В ситуациях типа

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!} + \ldots$$

есть алгоритм вычисления α_n, т. е. — конечное правило. Но этого нельзя сказать обо всех вещественных числах, поскольку $[0, 1]$ — континуум, а множество конечных правил счетно.

Но даже при наличии алгоритма бесконечное количество знаков — в некотором роде фикция, ибо процесс вычислений никогда не заканчивается. Позиция же классического анализа состоит в несколько «безответственной» декларации, что бесконечность состоялась — безостановочная работа проведена до конца, и вот вам иррациональное число.

10.5.1. *Число называется* ***конструктивно определяемым****, если все его десятичные знаки α_n алгоритмически вычисляются, т. е. $\alpha_n = f(n)$, где $f(n)$ — эффективный алгоритм, определенный при любом n.*

В силу $\alpha_n = f(n)$, где функция $f(n)$ вычислима и определена при любом n, получается, что множество конструктивных чисел *неперечислимо* (*теорема* 6.2.4), т. е. *конструктивно несчетно.* Ни равенство $a = b$, ни отношение $a < b$ — для конструктивных чисел в общем случае оказываются непроверяемы (*теорема Райса* 6.9.1).

При записи числа в двоичной системе каждое α_n принимает одно из двух значений,) или 1. Допустим, всюду определенная вычислимая функция $f(k)$ перечисляет *без повторений* те номера n, которым отвечает $\alpha_n = 1$, т. е. те позиции в записи числа, где стоят единицы. Изначально во всех позициях пусть стоят нули. Через N шагов в каких-то N позициях будут расставлены единицы. Получится рациональное число

$$S_n = 0{,}00101101\ldots011.$$

Последовательность $\{S_n\}$ монотонно возрастает, $S_{n+1} > S_n$, и ограничена, $S_n \leqslant 1$. Но *если $f(k)$ перечисляет неразрешимое множество, — воспользоваться классической теоремой анализа о сходимости ограниченной монотонной последовательности не удается.* В этом случае $\{S_n\}$ называют *последовательностью Шпеккера.*

10.5.2. *Последовательность Шпеккера, будучи монотонной и ограниченной, не может сходиться, поскольку не является фундаментальной. Например, $f(k) = 2$ все не появляется, но гарантировать, что не появится, — невозможно. Если вдруг появится, — значение S_n сразу подпрыгнет на $1/4 = 2^{-2}$, и это может произойти, когда угодно.*

В то же время $f(k)$ — совершенно нормальная функция с точки зрения анализа, а S_n — совершенно нормальная последовательность рациональных чисел, которая монотонна и ограничена, но не сходится!

Заметим, кстати, что S_n можно записать в виде

$$S_n = \sum_{k=1}^{n} 2^{-f(k)}.$$

На языке числовых рядов отмеченная катастрофа звучит не менее безнадежно. Ряд $\sum\limits_{k=1}^{\infty} 2^{-f(k)}$ ограничен ($\leqslant 1$), но не сходится, хотя все члены положительны.

Вспомним, как в анализе доказывается обратное. Пусть Ω_N обозначает множество значений $f(k)$ при $k \geqslant N$, и пусть $m(N)$ есть минимальное в Ω_N число[8]. Легко видеть, что

$$m(N) \to \infty \quad \text{при} \quad N \to \infty, \tag{10.7}$$

поскольку $f(k)$ перечисляет Ω_0 без повторений, т. е. все элементы Ω_0 различны. Из (10.7) следует

$$\sum_{k=N}^{\infty} 2^{-f(k)} \leqslant 2 \cdot 2^{-m(N)} \to 0 \quad \text{при} \quad N \to \infty,$$

[8] Существующее в силу ограниченности Ω_N снизу.

т. е. хвост ряда стремится к нулю — ряд сходится. Соответственно, последовательность S_n фундаментальна.

Разногласие подходов локализовано в том месте, где предполагается существование минимального в Ω_N числа $m(N)$. В классическом анализе предположение выглядит естественно, и его фундаментальный характер, способный направить математику по разным путям, — остается незамеченным. Существование $m(N)$ в некотором роде предполагает, что вычисление $f(k)$ проведено до конца, и минимум надо выбрать на *«состоявшемся»* бесконечном множестве Ω_N.

Тут бы, конечно, на конструктивном углублении в анализ лучше не задерживаться. Конфликт респектабельных теорий наносит ущерб репутации обеих сторон. Авторитет машины Тьюринга идет на убыль, когда выясняется, что вычислимость замешана в скандалах с устоявшимися областями математики. В то же время подрывается доверие к анализу, когда уходящий в гудок пар сообщает, что здесь не все чисто. Тем не менее результаты конструктивного анализа, не влияя ни на что рецептурно, поддерживают тонус и бдительность. Последнее весьма существенно для ощущения среды, в которой развивается математика.

10.6. Мера Лебега

Когда многочисленные задачи стали упираться в несостоятельность понятий интеграла и объема[9], внимание исследователей сконцентрировалось на поиске хороших определений. Положение спас Лебег. Решая частную задачу измерения площадей на искривленных поверхностях, он в итоге построил общую теорию меры, решив проблему в известном смысле окончательно. Все *конструктивно* задаваемые множества стали измеримыми.

[9] Дающей о себе знать в парадоксах измерения экзотических множеств, см. [2], в сходимости рядов Фурье к неинтегрируемым по Риману функциям, в теоретико-вероятностных противоречиях и т. п.

Простое и ясное изложение теории меры имеется в [10], см. также [3, т. 5] и [16]. Идеологическая сторона дела здесь такова. В «плоском» варианте за исходный пункт берется определение площади прямоугольника $m(P) = ab$, где a и b — стороны P. Площадь фигуры S (пусть пока на $[0, 1] \times [0, 1]$), представимой в виде ***конечной*** совокупности ***непересекающихся*** прямоугольников $\{P_n\}$, полагается равной

$$m(S) = \sum_n m(P_n), \tag{10.8}$$

что называют *аддитивностью* меры $m(S)$. Из аддитивности в данном случае вытекает *счетная аддитивность*, или *σ-аддитивность*, — т. е. справедливость (10.8) в случае бесконечного числа слагаемых.

Далее для ограниченных множеств определяется *внешняя мера*

$$\mu^*(A) = \inf \sum_n m(P_n), \tag{10.9}$$

где инфимум берется по всевозможным покрытиям множества A конечными или ***счетными*** системами прямоугольников.

Наконец, множество A называется *измеримым по Лебегу*, если по любому $\varepsilon > 0$ можно указать такую конечную совокупность A_ε непересекающихся прямоугольников, что

$$\mu^*(A \Delta A_\varepsilon) < \varepsilon. \tag{10.10}$$

Меру Лебега $\mu(A)$ измеримого множества A полагают равной [10] $\mu^*(A)$.

В общем случае работает аналогичная схема, с той лишь разницей, что вместо прямоугольников берется та или иная система простейших множеств, мера которых задается директивно, после чего проделываются похожие манипуляции. В отличие от рассмотренной ситуации σ-аддитивность может «не вытекать», и тогда ее приходится постулировать.

[10] Упомянутая в определении внешней меры ограниченность множеств приводит к $\mu(A) < \infty$, но простым техническим приемом (разбиения множества на клетки) это ограничение обходится, охватывая множества бесконечной меры типа всей плоскости.

10.6.1. Теорема Лебега. *Совокупность измеримых множеств замкнута относительно операций счетного объединения и счетного пересечения, а мера μ σ-аддитивна*[11]. ▷

Поскольку любое открытое множество на $[0, 1] \times [0, 1]$ представи́мо в виде счетного объединения замкнутых прямоугольников, то на $[0, 1] \times [0, 1]$ измеримы любые открытые и замкнутые множества, а также их счетные объединения и пересечения (и не только они).

Аксиоматика теории меры охватывает весьма широкий класс ситуаций. Вот стандартная модель иной содержательной природы (из теории вероятностей). На счетном множестве

$$\Omega = \{\omega_1, \ldots, \omega_n, \ldots\}$$

задана «мера точек» $p_n = m(\omega_n)$, удовлетворяющая условию нормировки

$$\sum_{n=1}^{\infty} p_n = 1.$$

Измеримы оказываются любые подмножества $A \subset \Omega$, а мера

$$\mu(A) = \sum_{\omega_n \in A} p_n$$

получается σ-аддитивной.

В теории *меры Лебега* важную роль играют *борелевские множества* [16], являющиеся элементами минимальной σ-алгебры, порожденной классом открытых множеств $\mathbb{R}^n$. Иногда создается впечатление, что на прямой — это и есть измеримые по Лебегу множества. *Это неправильно*. Всякое борелевское множество измеримо по Лебегу, но не всякое измеримое по Лебегу — борелевское. Точное положение дел: *всякое измеримое по Лебегу множество — есть борелевское плюс множество меры нуль.*

---

[11] Т. е. $\mu(\Omega) = \sum\limits_{n}^{\infty} \mu(\Omega_n)$, если множества Ω_n попарно не пересекаются и $\Omega = \bigcup\limits_n \Omega_n$.

Заслуживает упоминания *непрерывность σ-аддитивной меры*, каковой называют следующее свойство:

$$\mu(\Omega) = \lim_{n\to\infty} \mu(\Omega_n)$$

для любой цепочки вложенных множеств конечной меры

$$\Omega_1 \supset \Omega_2 \supset \dots \quad \text{и} \quad \Omega = \bigcap_n \Omega_n.$$

Схема Лебега идейно очень похожа на *схему Жордана*, опиравшуюся на «древнегреческую» аппроксимацию измеряемого множества S изнутри и снаружи:

$$P \subset S \subset Q,$$

где P и Q — семейства непересекающихся прямоугольников, P укладывается в S, а Q — накрывает S. При совпадении супремума $m(P)$ и инфимума $m(Q)$ множество S объявлялось измеримым. Очень близко, казалось бы, — но измеряется меньше, чем у *Лебега*. У *Лебега* чуть по-другому, однако определения начинают работать, в результате измеряется не кое-что, а «все»[12].

Преимущества схемы Лебега определяются следующей причиной. Если на совокупности $\mathcal{P}$ непересекающихся прямоугольников задать функцию

$$\rho(P, Q) = m(P \Delta Q), \tag{10.11}$$

то это *полуметрика*, становящаяся метрикой после отождествления тех P и Q, для которых $m(P\Delta Q) = 0$. В результате $\mathcal{P}$, вернее, множество его эквивалентных классов (т. е. фактор-множество по отношению эквивалентности $m(P\Delta Q) = 0$), по метрике (10.11) становится метрическим пространством. Дальнейшее

[12] Известны различные схемы введения *меры Лебега*, в том числе — основанные на идее зажимания искомой величины с двух сторон, но не так как у *Жордана*. *Внутренняя мера Лебега* μ_* определяется как внешняя мера дополнения: $\mu_*(A) = \mu^*(X\backslash A)$. Измеримость A обеспечивает $\mu_* = \mu^*$.

сводится к ***пополнению*** этого пространства, что и приводит к «полному пространству измеримых множеств»[13].

10.7. Измеримые функции

Функцию $f : X \to Y$ называют *измеримой*, если в X измерим прообраз $f^{-1}(A)$ любого измеримого в Y множества A. В случае $f : X \to \mathbb{R}$ работает то же определение, но на прямой избирается система борелевских множеств (!), а не система множеств, измеримых по Лебегу. При этом функцию f называют *борелевской*, либо *измеримой по Борелю*, либо *B-функцией*, а $f : X \to Y$, для контраста, называют *μ-измеримой*. Однако обременительная аккуратность постепенно сходит на нет, и вещественные функции начинают называть просто измеримыми, что вносит определенную путаницу.

Непрерывные функции являются, безусловно, B-функциями, но не обязаны быть измеримыми в смысле Лебега. Поэтому когда их называют просто измеримыми — появляются «странности». *Непрерывная функция от измеримой — всегда измерима, а измеримая от непрерывной — необязательно.* В то же время где-нибудь рядом располагается теорема, утверждающая измеримость композиции измеримых функций. Аудитория в шоке.

Функция $f : X \to \mathbb{R}$ *измерима* (на самом деле *B-измерима*), если при любом $\alpha \in \mathbb{R}$ измеримы *лебеговские множества*

$$X_\alpha(f) = \{x : f(x) < \alpha\}.$$

Естественно, возникает вопрос, почему бы не выбросить борелевскую конструкцию за борт, заменив лебеговской и ликвидировав двойственность толкования. Потому что лебеговскую измеримость легко декларировать, но трудно проверять. Достаточно вспомнить о непрерывных функциях.

[13] При описанной точке зрения задача помещается в колею выполнения рутинных операций. В этом и состоит прикладная значимость функционального анализа. Дается координатная сетка мышления, превращающая хаотичное блуждание в целенаправленную деятельность.

В то же время борелевских множеств и функций вполне хватает для многих приложений. При этом борелевские функции переводят измеримые *по Лебегу* множества в измеримые — *по Лебегу*, что, собственно, и требуется для интегрирования по Лебегу.

Функции, значения которых отличаются на множестве нулевой меры, считаются *эквивалентными*. В пространствах измеримых функций в качестве элементов обычно подразумеваются *классы эквивалентных функций*. Конкретную функцию называют *представителем* своего класса.

Когда говорят о поточечной сходимости измеримых функций, имеется в виду *сходимость почти всюду*, $f_n \xrightarrow{\text{п. в.}} f$, т. е. $f_n(x) \to f(x)$ может нарушаться на множестве нулевой меры.

10.8. Множества Витали и Бернштейна

10.8.1. Неизмеримое множество Витали. *Пусть фигурные скобки обозначают дробную часть числа. Введем на* $[0, 1]$ *отношение эквивалентности*

$$x \sim y, \quad \text{если} \quad \{x - y\} \quad \text{рационально},$$

и отнесем к множеству V *по одному элементу из каждого класса эквивалентности (аксиома выбора). Определим далее множества* V_r *как сдвиг* V *на рациональное* r *по модулю* 1,

$$V_r = \{x : x = \{v + r\}, v \in V\},$$

т. е. к числам v *прибавляется* r, *и берется дробная часть* $v + r$.

Счетное объединение всех непересекающихся множеств V_r *дает весь промежуток* $[0, 1]$. *Поэтому*

$$\sum_r^{\infty} \mu(V_r) = 1,$$

чего не может быть, если V *измеримо, поскольку в предположении противного все*

$$\mu(V_r) = \mu(V).$$

Другая конструкция неизмеримого множества принадлежит *Бернштейну* [16].

10.8.2. Множество Бернштейна. *Существует такое неизмеримое множество $B \subset \mathbb{R}$, что как B, так и его дополнение $\overline{B} = \mathbb{R} \setminus B$ — оба пересекаются с любым несчетным замкнутым подмножеством $\mathbb{R}$.*

Манипулируя *аксиомой выбора*, можно зайти очень далеко [20]:

10.8.3. *Существует множество D, дающее в пересечении с любым $X \subset \mathbb{R}$ ненулевой меры — неизмеримое множество.*

Тут уместно повторить замечание из [3, т. 12]: *Конечно хорошо, если два-три человека в пределах Галактики будут заниматься построением и анализом подобных примеров. Но не дай бог, увлечение станет повальным. Дорога-то ведет в никуда, по-видимому. Для общего образования целесообразны первые несколько шагов: роль аксиомы выбора, растущей из пропасти, существование неизмеримых множеств, как принципиальной преграды для измерения всего и вся. Далее начинается наркомания.*

10.9. Категории Бэра

Одной из задач теории меры является выделение множеств нулевой либо полной меры, чтобы придать смысл формулировкам типа «почти всюду». Аналогичные устремления имеет *категорная классификация*.

10.9.1. Определение. *Множество $U \subset X$ называется множеством первой категории, если оно представимо в виде объединения счетного числа нигде не плотных*[14] *множеств. Множество не первой категории — называется множеством второй категории.*

---

[14] Множество *плотно* в X, если имеет непустое пересечение с любой окрестностью, и *нигде не плотно*, если не плотно ни в какой окрестности (если его замыкание не имеет внутренних точек).

Множество рациональных точек вещественной прямой, хотя всюду плотно, является множеством первой категории, как счетное объединение точек, а множество иррациональных — второй. *Канторово множество C* также относится к первой категории, поскольку нигде не плотно.

Категорные идеи возникли при выяснении того, насколько плох может быть предел непрерывных функций. *Поточечный предел на* $[0, 1]$ *всюду сходящейся последовательности непрерывных функций является функцией, непрерывной всюду, за исключением множества точек первой категории.* Отсюда следует, что производная дифференцируемой функции не может быть всюду разрывной. Множество ее точек разрыва — есть множество точек первой категории.

10.9.2. Теорема Бэра о категории. *Полное метрическое пространство является множеством второй категории*[15].

Сюрпризом выглядит следующий факт.

10.9.3. *Всякое множество X на прямой можно разбить на два взаимодополняющих множества A и B, из которых A — множество первой категории, а B имеет меру нуль, см.* [3, т. 12].

10.9.4. Следствие из 10.9.3. *Отрезок* $[0, 1]$ *можно разбить на два взаимодополняющих множества A и B, из которых A — множество второй категории, а B имеет меру* 1.

Несмотря на феномен 10.9.3 во взаимодействии меры и категории есть некоторая доля согласованности. Более того, оказывается справедлив следующий результат, неожиданный теперь в противоположном направлении.

10.9.5. Теорема Серпинского. *В предположении справедливости гипотезы континуума существует такое взаимно однозначное отображение $f : \mathbb{R} \to \mathbb{R}$, что $f(X)$ имеет меру нуль в томм случае, когда $X \subset \mathbb{R}$ — множество первой категории.*

[15] Эквивалентная формулировка: *в полном пространстве пересечение любого счетного семейства открытых всюду плотных множеств — всюду плотно.*

Неожиданным образом тут выстреливает *гипотеза континуума*, наделяя теорему 10.9.5 «метафизическими свойствами». Результат 10.9.5 является отправным пунктом для взаимоотношений двойственности [16] между теориями меры и категории. Причем эти «взаимоотношения» работают вне какой бы то ни было зависимости от *гипотезы континуума*, т. е. **ГК** дает здесь теоремную подсказку.

Заметим, что категорные методы эффективны при доказательстве разнообразных теорем существования, [16].

10.9.6. Определение. *Множество $X \subset \mathbb{R}^n$ обладает* ***свойством Бэра****, если представимо в виде $X = A \Delta B$, где A — открытое множество, а B — множество первой категории*[16].

Теория множеств, обладающих *свойством Бэра*, представляет интерес как аналог теории меры Лебега. Обладание «свойством» служит аналогом измеримости, а множества первой категории играют роль *нуль-множеств*, с букетом параллельных результатов. Аксиома выбора «по тем же нотам» позволяет гарантировать существование множеств, не обладающих *свойством Бэра*. Примером такого сорта является *множество Бернштейна*.

10.9.7. ***Совершенное множество*** *определяется как непустое замкнутое множество, не имеющее изолированных точек. Совершенными могут быть множества, не имеющие внутренних точек (вопреки ожиданиям), — канторово множество, например. Другой сюрприз: всякое совершенное множество на $\mathbb{R}$ — несчетно.*

10.9.8. Теорема Кантора—Бендиксона. *Любое несчетное замкнутое подмножество $\mathbb{R}^n$ может быть представлено как объединение счетного множества и — совершенного.* ▷

Класс несчетных ***замкнутых*** подмножеств интересен сам по себе. Если множество всех подмножеств множества X имеет мощность, бóльшую чем мощность X, то:

---

[16] Обратите внимание на аналогию $X = A \Delta B$ с условием (10.10).

10.9.9. *Совокупность всех несчетных* ***замкнутых*** *подмножеств* $\mathbb{R}^n$ *имеет мощность континуума* c, *т. е. ту же мощность что и* $\mathbb{R}^n$.

С 10.9.9 перекликается следующий результат.

10.9.10. *Совокупность всех борелевских подмножеств* $\mathbb{R}^n$ *имеет мощность континуума.*

Сокращения и обозначения

◀ и ▶	начало и конец рассуждения, темы, доказательства
$\triangleright$	утверждение приводится без доказательства
$\triangleleft$	утверждение легко может быть доказано
(?)	предлагает проверить или доказать утверждение в качестве упражнения, либо довести рассуждение до «логической точки»
(!)	предлагает обратить внимание
«в томм случае»	«в том и только том случае»
АС	аксиома выбора
ГК	гипотеза континуума
$A \to B$	из A следует B
$x \in X$	x принадлежит X
$X \cup Y, \quad X \cap Y, \quad X \setminus Y$	объединение, пересечение и разность множеств
$\overline{X} = X'$	дополнение X
$X \subset Y$	X подмножество Y, в том числе имеется в виду возможность $X \subseteq Y$, т. е. между $X \subset Y$ и $X \subseteq Y$ различия не делается
$X \in Y$	множество X является элементом множества Y
$\sigma(X) = X \cup \{X\}$	
$\sim$	отношение эквивалентности, определяемое контекстом; в случае изоморфизма вместо $\sim$ чаще используется знак обыкновенного равенства $=$
$\varnothing$	пустое множество
$\dot{\Omega} = \partial\Omega$	граница Ω
2^{Ω}	множество всех подмножеств множества Ω
$\mathbb{N}$	множество натуральных чисел $\{1, 2, \ldots\}$

$\mathbb{Z}$	множество целых чисел $\{\dots, -1, 0, 1, \dots\}$
$\mathbb{R} = (-\infty, \infty)$	вещественная прямая
$\mathbb{P}$	множество простых чисел
$\mathbb{Q}$	множество положительных рациональных чисел
$\mathbb{R}^n$	n-мерное евклидово пространство
$\aleph_0$	мощность счетного множества
$\mathbf{c}$	мощность континуума
$[a]$	целая часть числа a
$\{a\}$	дробная часть числа a
$\exists$	квантор существования
$\forall$	квантор общности
I_X	тождественное отображение $X \to X$
p_r	r-е по счету простое число
$\mathrm{Dom}(f)$	область определения функции f
L	конструктивный универсум Гёделя
V	универсум фон Неймана

Литература

1. *Barwise J.* Admissible sets and structures. Berlin; Heidelberg; New-York: Springer-Verlag, 1975.
2. *Босс В.* Интуиция и математика. Изд. 3-е. М.: URSS, 2008.
3. *Босс В.* Лекции по математике. Т. 1: Анализ; Т. 2: Дифференциальные уравнения; Т. 3: Линейная алгебра; Т. 4: Вероятность, информация, статистика; Т. 5: Функциональный анализ; Т. 6: От Диофанта до Тьюринга; Т. 7: Оптимизация; Т. 8: Теория групп; Т. 9: ТФКП; Т. 10: Перебор и эффективные алгоритмы; Т. 11: Уравнения математической физики; Т. 12: Контрпримеры и парадоксы; Т. 13: Топология; Т. 14: Теория чисел; Т. 15: Нелинейные операторы и неподвижные точки. М.: URSS, 2004–2010.
4. *Булос Дж., Джеффри Р.* Вычислимость и логика. М.: Мир, 1994.
5. *Верещагин Н. К., Шень А.* Лекции по математической логике и теории алгоритмов. Ч. 1: Начала теории множеств; Ч. 2: Языки и исчисления; Ч. 3: Вычислимые функции. М.: МЦНМО, 2002.
6. *Владимиров Д. А.* Булевы алгебры. М.: Наука, 1969.
7. *Йех Т.* Теория множеств и метод форсинга. М.: Мир, 1973.
8. *Клини С. К.* Введение в метаматематику. 4-е изд. М.: Издательство ЛКИ/URSS, 2008.
9. *Кановей В. Г.* Аксиома выбора и аксиома детерминированности. М.: Наука, 1984.
10. *Колмогоров А. Н., Фомин С. В.* Элементы теории функций и функционального анализа. М.: Наука, 1972.
11. *Коэн П. Дж.* Теория множеств и континуум-гипотеза. М.: Мир, 1969.
12. *Кусраев А. Г., Кутателадзе С. С.* Введение в булевозначный анализ. М.: Наука, 2005.
13. *Мальцев А. И.* Алгоритмы и рекурсивные функции. М.: Наука, 1986.
14. *Матиясевич Ю. В.* Десятая проблема Гильберта. М.: Наука, 1993.
15. *Мартин-Лёф П.* Очерки по конструктивной математике. М.: Мир, 1975.
16. *Окстоби Дж.* Мера и категория. 2-е изд. М.: Издательство ЛКИ/URSS, 2008.

17. *Робинсон А.* Введение в теорию моделей и метаматематику алгебры. М.: Наука, 1967.
18. *Роджерс Х.* Теория рекурсивных функций и эффективная вычислимость. М.: Мир, 1972.
19. Справочная книга по математической логике: В 4 ч. / Под ред. Дж. Барвайса. М.: Наука, 1982–1983.
20. *Халмош П.* Теория меры. М.: ИЛ, 1953.
21. *Shelah S.* Proper and Improper Forcing. Berlin: Springer-Verlag, 1998.
22. *Шенфилд Дж.* Математическая логика. М.: Наука, 1975.

Предметный указатель

В. Босс

Лекции по математике

Том 16

Теория множеств: От Кантора до Коэна

Краткое и ясное изложение предмета

В *«Лекциях по математике» В. Босса* вышли тома:
1. Анализ. 2. Дифференциальные уравнения. 3. Линейная алгебра. 4. Вероятность, информация, статистика. 5. Функциональный анализ. 6. От Диофанта до Тьюринга. 7. Оптимизация. 8. Теория групп. 9. ТФКП. 10. Перебор и эффективные алгоритмы. 11. Уравнения математической физики. 12. Контрпримеры и парадоксы. 13. Топология. 14. Теория чисел. 15. Нелинейные операторы и неподвижные точки. 16. Теория множеств: От Кантора до Коэна.

В условиях информационного наводнения инструменты вчерашнего дня перестают работать. Поэтому учить надо как-то иначе. «Лекции» дают пример. Плохой ли, хороший – покажет время. Но в любом случае, это продукт нового поколения. Те же «колеса», тот же «руль», та же математическая суть, – но по-другому.

В. Босс

Из отзывов читателей:

Чтобы усвоить предмет, надо освободить его от деталей, обнажить центральные конструкции. Это тяжелая работа, которая в «Лекциях» проделывается автором.

Дается то, чего недостает. Общая картина, мотивация, взаимосвязи. И самое главное — легкость вхождения в любую тему.

Содержание продумано и хорошо увязано. Громоздкие доказательства ужаты до нескольких строчек. Виртуозное владение языком.

НАУЧНАЯ И УЧЕБНАЯ ЛИТЕРАТУРА
URSS
E-mail: URSS@URSS.ru
Каталог изданий в Интернете:
http://URSS.ru
Тел./факс (многоканальный):
+ 7 (499) 724–25–45

10356 ID 124857

9 785397 021623

Отзывы о настоящем издании, а также обнаруженные опечатки присылайте по адресу **URSS@URSS.ru**.
Ваши замечания и предложения будут учтены и отражены на web-странице этой книги в нашем интернет-магазине **http://URSS.ru**