ВВЕДЕНИЕ В АКСИОМАТИЧЕСКУЮ ТЕОРИЮ МНОЖЕСТВ

Н. И. Казимиров

Петрозаводск 2000

УДК 517.2

Казимиров Н. И. Введение в аксиоматическую теорию множеств: Учеб. пособие. — Петрозаводск: Изд-во (не опр.), 2000. — 104 с.

Книга представляет собой краткое изложение курса аксиоматической теории множеств и посвящена теории порядковых и кардинальных чисел, а также изложению фундаментальных математических определений в терминах теории множеств, и может быть использована для подготовки спец. курсов по теории множеств.

Библиогр. 14 назв.

Рецензенты:

д.ф.-м.н. А. В. Иванов, д.ф.-м.н. В. М. Тdigitrarин

Содержание

Введение

Изложение курса начнем с рассмотрения наивной (канторовской) теории множеств [1, 2]. Для начала опишем *язык* (или символику) теории множеств. В теории множеств (как в наивной, так и в формальной) мы любой объект считаем множеством, т. к., во-первых, это ничуть не мешает нам моделировать при помощи теории множеств реальные объекты, а во-вторых, это упрощает построение самой теории.

Для обозначения произвольных множеств мы будем использовать латинские буквы $a, b, \ldots, z$, которые в дальнейшем будем называть *переменными*.

Основной логической формулой при описании множеств является формула вида $x \in y$, где переменные x, y могут быть заменены любыми другими переменными. Отметим также, что в формуле $x \in y$ переменные x, y, обозначающие произвольные множества, имеют несколько более конкретный смысл, а именно, y обозначает некое множество элементов-множеств, среди которых есть множество x. Поэтому формула $x \in y$ читается «x есть элемент y» или же «x принадлежит y», иногда также говорят «y содержит x (в качестве элемента)». Из основной, а далее мы будем называть ее *атомарной*, формулы можно при помощи логических связок и кванторов строить новые *формулы*, описывающие различные свойства множеств. Для этого введем в рассмотрение символы логических связок и кванторов: $\rceil$ заменяет частицу «не», $\wedge$ — союз «и», $\vee$ — «или», $\to$ — «следует», $\Leftrightarrow$ — «тогда и только тогда, когда», «равносильно», $\forall$ — «для любого», $\exists$ — «существует».

Построение формул происходит рекурсивно с использованием атомарной формулы и логических связок и кванторов. Так, при помощи атомарной формулы можно построить формулы: $(x \in y) \wedge (x \in z)$, $\exists x\ ((x \in z) \wedge \rceil (x \in y))$. Переменная в формуле называется *связанной*, если она стоит под каким-либо квантором, в противном случае она называется *свободной*. Так, в формуле $\exists x\ ((x \in z) \wedge (\rceil (x \in y))$ переменная x связанная, а переменные y, z свободные.

Сами формулы мы также будем часто обозначать переменными, для этих целей мы используем греческие буквы φ и ψ, указывая в скобках, если нужно, переменные, свободно входящие в формулы. Например, мы можем обозначить формулу $x \in y$ через φ, $\varphi(x)$, $\varphi(y)$, $\varphi(x, y)$ или $\varphi(y, x)$. При этом всегда следует помнить, какие именно переменные указаны в скобках, чтобы при замене переменных не нарушалась структура формулы. Так, если у нас через $\varphi(x)$ обозначена формула $x \in y$, то $\varphi(z)$ будет обозначать формулу $z \in y$; если же мы обозначили через $\varphi(x)$ формулу $y \in x$, то $\varphi(z)$ уже будет обозначать формулу $y \in z$!

Чтобы не использовать громоздкие записи формул (которые к тому же часто оказываются неудобочитаемыми), мы будем использовать сокращения записи для формул. Ниже приводится список сокращений, в котором слева от значка := ставится определяемый символ, а справа — формула, которую он заменяет.

$$
\begin{aligned}
\forall x \in a:\ \varphi &:= \forall x\ (x \in a \to \varphi)\\
\exists x \in a:\ \varphi &:= \exists x\ (x \in a \wedge \varphi)\\
a \subseteq b &:= \forall x\ (x \in a \to x \in b)\\
a = b &:= (a \subseteq b) \wedge (b \subseteq a)\\
a \subset b &:= (a \subseteq b) \wedge (a \neq b)\\
a \notin b &:= \rceil (a \in b)\\
a \neq b &:= \rceil (a = b)
\end{aligned}
$$

Первые два определения здесь являются не сокращениями для конкретных формул, а схемами сокращений, а каждое конкретное сокращение определяется уже конкретной заменой переменной φ на некоторую формулу.

Некоторые из этих формул читаются специальным образом, а именно, $a \subseteq b$ читается «a содержится в b» или «a есть подмножество b», $a \subset b$ — «a есть собственное подмножество b».

Все обозначения, приведенные тут, стандартны и встречаются во всех областях математики. Заметим, что равенство множеств мы определяем, а не рассматриваем его как нечто предопределенное, и выражает оно тот факт, что множества, состоящие из одних и тех же элементов, равны.

Кроме обозначения формул используются также обозначения для множеств. Это связано с тем, что множества можно задавать посредством некоторых формул. Например, для обозначения множества, составленного из двух элементов x, y, используется символ $\{x, y\}$. Определение такого множества через описание его элементов осуществляется указанием формулы $\varphi(z) := z = x \vee z = y$, т.е. множество $\{x, y\}$ состоит из всех таких элементов z, для которых истинно $\varphi(z)$. Такой способ описания множеств мы и зафиксируем в следующих обозначениях (обычно их принято называть *термами*). Через $\{x |\ \varphi(x)\}$ условимся обозначать множество всех таких x, для которых $\varphi(x)$ истинно,[1] далее положим:

$$
\begin{aligned}
\{a, b\} &:= \{x |\ x = a \vee x = b\} \\
\{a\} &:= \{a, a\} \\
a \cap b &:= \{x |\ x \in a \wedge x \in b\} \\
a \cup b &:= \{x |\ x \in a \vee x \in b\} \\
a \setminus b &:= \{x |\ x \in a \wedge x \notin b\} \\
\cup a &:= \{x |\ \exists y \in a :\ x \in y\} \\
\mathrm{Exp}(a) &:= \{x |\ x \subseteq a\} \\
S(a) &:= a \cup \{a\} \\
\emptyset &:= \{x |\ x \neq x\}
\end{aligned}
$$

Понятно, что все эти термы, кроме $S(a)$, имеют свои названия, и все эти названия стандартны для любой области математики. Например, $a \cap b$ обозначает пересечение множеств a и b, терм $\mathrm{Exp}(a)$ обозначает множество всех подмножеств множества a и называется экспонентой или степенным множеством множества a, а терм $\{a\}$, обозначающий одноточечное множество, называется *синглéтом*. Терм $S(a)$ будет использоваться нами достаточно часто при изложении курса, поэтому мы введем название и для него. Множество $S(a)$ будем называть *последующим* за множеством a. Если раскрыть его определение более подробно, то нетрудно заметить, что для всякого элемента $x \in S(a)$ имеет место $x \in a \vee x = a$. Это множество на один элемент расширяет множество a, добавляя в качестве элемента само множество a.

[1]Такой способ описания множеств заставляет нас использовать термы, в которых присутствуют связанные переменные и формулы: в терме $\{x |\ \varphi(x)\}$ переменная x связана, а фигурные скобки играют здесь роль квантора с тем лишь отличием, что в итоге мы получаем не формулу, а терм. Таким образом, язык, который мы описываем сейчас, не является языком *первого порядка* [3, 4]. Поскольку языки первого порядка имеют несколько преимуществ (с точки зрения простоты их изучения) перед остальными языками, то в § 1.1 мы построим теорию множеств в языке первого порядка — без использования подобных термов.

Из определения равенства множеств нетрудно заключить, что для каждого множества x истинно $x = x$, поэтому в пустом множестве $\emptyset$ нет ни единого элемента. Пустое множество $\emptyset$ нам также необходимо для построения теории множеств, как, например, число ноль в арифметике. Так как мы хотим в результате пересечения множеств всякий раз получать множество, то мы обязаны предусмотреть и тот случай, когда два множества, пересечение которых мы ищем, не имеют общих элементов, т. е. их пересечением является пустое множество.

На этом завершается описание языка теории множеств.[2]

С самого начала мы предположили, что все множества, какие мы рассматриваем в наивной (канторовской) теории множеств представляют из себя произвольные наборы множеств, никаких других ограничений на понятие множества мы не накладывали. Покажем, что такое достаточно произвольное определение множества не может быть корректным с точки зрения логики, ибо приводит к противоречию. Следующий парадокс, который мы получим здесь, называется парадоксом Расселла.

Поскольку атомарная формула $x \in y$, выражающая принадлежность множества x к множеству y, имеет смысл для любых множеств x и y, ничто не мешает нам рассмотреть такой ее вид: $x \in x$. С точки зрения здравого смысла формула $x \in x$ должна быть ложной для любого множества x, ибо мы считаем, что часть некоего объекта (в данном случае множества) не может совпадать с самим этим объектом. Поэтому мы вводим следующее определение: множество x такое, что $x \notin x$, называется *регулярным*, а множество x, для которого $x \in x$, назовем *сингулярным*.

Снова нам ничто не мешает собрать все регулярные множества в одно множество R, точнее, $R := \{x \mid x \notin x\}$. Попытаемся теперь ответить на следующий вопрос: регулярно или сингулярно множество R?

Предположим, что множество R регулярно, т. е. $R \notin R$. Но тогда R удовлетворяет тому свойству, которым оно само определено, значит, $R \in R$. Противоречие. Предположим тогда, что R сингулярно, т. е. $R \in R$. Но тогда R не удовлетворяет тому свойству, которым определены его элементы, следовательно, $R \notin R$. Противоречие.

Итак, множество R не регулярно и не сингулярно, чего быть не может, если мы принимаем закон исключенного третьего (либо A, либо не A). Так может быть, R — не множество?

---

[2] Более подробно о языках теории множеств и их анализ см. в [3, 4].

Полученный парадокс, как может показаться, доказывает несостоятельность самой идеи множества, как высшей точки абстракции в математических науках. На самом же деле весь тот путь, который мы прошли при построении множеств и при рассмотрении парадокса Расселла, уже дает предпосылки к решению этого парадокса. Мы с самого начала считали, что множество есть произвольная совокупность (множеств), что привело к построению парадоксального множества R. Насколько велико это множество, мы также не знаем, ибо мы предположили существование сингулярных множеств. С другой стороны, если предположить, что все множества регулярны, то R будет просто множеством всех множеств. Конечно, это не избавляет нас от противоречия, но зато дает повод попытаться исключить из рассмотрения сингулярные множества, а также «слишком большие» совокупности множеств путем навязывания множествам некоторых условий или, как принято говорить, *аксиом*.

Мы пойдем примерно по тому же пути, каким в свое время пошел Цермело, опубликовавший впервые в 1908 году некоторые аксиомы теории множеств, которые были впоследствии дополнены Френкелем. Мы воспользуемся методом формализации Гильберта, который впервые был применен Гильбертом при построении формальной аксиоматической геометрии [5] (чем, собственно, была закрыта проблема пятого постулата Евклида) и развит в его совместном с Бернайсом фундаментальном труде «Основания математики» [6].

Для этого мы попытаемся определить основные требования к множествам так, чтобы избежать известных парадоксов наивной теории множеств и в то же время сохранить уровень абстракции понятия множества.

Перечислим некоторые из этих требований.

1) Основное свойство равенства (по Гильберту [6]), заключающееся в следующем: если $x = y$, то если истинно $\varphi(x)$, то таково же и $\varphi(y)$. Это свойство множеств мы будем называть *объемностью*.

2) Существование пустого множества $\emptyset$.

3) Из двух множеств x и y можно получить пару множеств $\{x, y\}$, которая также будет множеством.

4) Для всякого множества x ко множествам отнесем и его объединение $\cup x$.

5) Для всякого множества x множеством назовем и его степень $\mathrm{Exp}(x)$.

6) Если x множество, а $\varphi(z)$ — формула, то множеством будет также и $\{z|\ z \in x \wedge \varphi(z)\}$.

7) Все множества будем считать регулярными.

Все эти требования, кроме последнего, отражают конструктивные аксиомы множеств, т. е. аксиомы, являющиеся, по сути, правилами для построения множеств, отправляясь от пустого множества. Однако этих аксиом еще оказывается недостаточно для того, чтобы формализовать в теории множеств большинство математических результатов, например, из-за отсутствия аксиомы бесконечного множества. Полный набор аксиом, представляющий сегодня формальную теорию множеств Цермело—Френкеля включает девять аксиом, с формулировки которых мы и начнем рассмотрение аксиоматической теории множеств.

Глава 1

ОСНОВАНИЕ

§ 1.1 Формальная аксиоматика

Предмет изучения данного параграфа представляет собой язык первого порядка (ибо в качестве термов мы используем только переменные), более простой, чем тот, с которым мы имели дело во введении, с набором аксиом, которые мы приведем чуть позже. Язык, который мы опишем здесь, по традиции мы будем называть ZF — по первым буквам создателей аксиоматической теории множеств Цермело (Zermelo) и Френкеля (Fraenkel). Этот же символ (ZF) мы будем использовать и для обозначения только аксиоматики нашей теории.

Как и прежде, мы используем здесь латинские буквы $a, b, \ldots, z$ в качестве переменных, пробегающих множества, греческие буквы φ и ψ в качестве обозначений формул и принимаем все те правила построений формул и сокращений записи формул, о которых шла речь во введении. [1]

Аксиоматика ZF (по Колмогорову [4]) представляет собой следующий список аксиом.

S1. Аксиома экстенсионáльности (объемности):

$$x = y \to (x \in z \to y \in z).$$

S2. Аксиома пустого множества:

$$\exists u\, \forall z\; z \notin u.$$

[1] Мы пока избегаем использования сокращений для записи множеств (термов), которые были уже определены во введении, поскольку хотим сформулировать аксиомы в максимально простом языке, см. [3, 4].

S3. Аксиома пары:

$$\exists u\, \forall z\, (z \in u \Leftrightarrow (z = x \vee z = y)).$$

S4. Аксиома объединения (суммы):

$$\exists u\, \forall z\, (z \in u \Leftrightarrow \exists v\, (z \in v \wedge v \in x)).$$

S5. Аксиома степенно́го множества (экспоненты):

$$\exists u\, \forall z\, (z \in u \Leftrightarrow z \subseteq x).$$

S6[φ]. Схема аксиом содержательности (выделения):

$$\exists u\, \forall z\, (z \in u \Leftrightarrow z \in x \wedge \varphi(z)),$$

где формула $\varphi(z)$ языка ZF не содержит свободно переменной u.

S7. Аксиома регулярности (фундирования):

$$(\exists z\; z \in x) \to (\exists z \in x : \rceil \exists u\, (u \in z \wedge u \in x)).$$

S8[φ]. Схема аксиом подстановки:

$$\exists u\, \forall z\, (z \in u \Leftrightarrow \exists x \in v :\; \varphi(x, z) \wedge \forall w\, (\varphi(x, w) \to z = w)),$$

формула $\varphi(x, z)$ не содержит свободно переменных u и v.

S9. Аксиома бесконечности:

$$\exists u\, (\forall z\, (\forall x\; x \notin z) \to z \in u \wedge$$
$$\forall z \in u :\; (\forall v\, (\forall x\; x \in v \Leftrightarrow x \in z \vee x = z) \to v \in u)).$$

Нетрудно убедиться в том, что первые семь аксиом S1 – S7 практически в точности повторяют те требования к множествам, которые были нами сформулированы во введении. Например, аксиома S2 выражает существование пустого множества, для этого достаточно воспользоваться определением терма $\emptyset$, приведенного нами во введении. Аксиома S1 имеет более тривиальный вид, чем наше требование 1). Оказывается, что аксиомы S1 достаточно для выполнения 1), о чем свидетельствует следующая теорема о равенстве множеств.

Теорема 1.1. *Равенство множеств удовлетворяет следующим свойствам:*

1) $x = x$ *для любого множества* x.

2) *для произвольной формулы* $\varphi(x)$ *со свободной переменной* x:

$$x = y \to (\varphi(x) \to \varphi(y))$$

Доказательство. Первое утверждение вытекает непосредственно из определения равенства и правил вывода, для проверки второго необходимо воспользоваться всеми сокращениями для формул и правилами вывода (см. [6]), а также аксиомой S1.

Сначала заметим, что равенство множеств симметрично, т. е. из $x = y$ вытекает $y = x$, что проверяется непосредственно по определению формулы равенства.

Доказательство утверждения 2) проводится индуктивно по сложности формулы φ, а аксиома S1 является базой индукции. Именно, сначала необходимо проверить, что 2) справедливо в том случае, когда $\varphi(x)$ является атомарной формулой. При этом φ может иметь один из следующих двух видов: либо $\varphi(x) := z \in x$, либо $\varphi(x) := x \in z$. Понятно, что вместо z можно подставить любую другую переменную. Справедливость утверждения 2) для формулы $z \in x$ вытекает непосредственно из определения равенства (см. Введение); для формулы $x \in z$ утверждение 2) есть в точности аксиома S1.

Итак, 2) выполняется для атомарной формулы. Предположим далее, что 2) верно для формул $\varphi(x)$ и $\psi(x)$. Теперь необходимо показать, что 2) будет справедливо и для формул $\rceil\varphi(x)$, $\varphi(x) \wedge \psi(x)$, $\exists z\ \varphi(x, z)$, где z свободно входит в φ. Все прочие формулы являются комбинациями перечисленных только что формул, поэтому нет необходимости их рассматривать.[2]

Рассмотрим сначала $\rceil\varphi(x)$. По предположению

$$x = y \to (\varphi(x) \to \varphi(y)),$$

откуда заменой переменных получаем

$$y = x \to (\varphi(y) \to \varphi(x)).$$

Из симметричности равенства и по правилу контрапозиции [6] получаем

$$x = y \to (\rceil\varphi(x) \to \rceil\varphi(y)),$$

что и требовалось.

Рассмотрим теперь $\varphi(x) \wedge \psi(x)$. Поскольку в силу предположения имеем

$$x = y \to (\varphi(x) \to \varphi(y)), \quad x = y \to (\psi(x) \to \psi(y)),$$

то по правилу соединения выводов [6] получим:

$$x = y \to (\varphi(x) \to \varphi(y)) \wedge (\psi(x) \to \psi(y)),$$

[2]Действительно, $\varphi \vee \psi \Leftrightarrow \rceil(\rceil\varphi \wedge \rceil\psi)$; $\varphi \to \psi \Leftrightarrow \rceil\varphi \vee \psi$;
$[\varphi \Leftrightarrow \psi] \Leftrightarrow (\varphi \to \psi) \wedge (\psi \to \varphi)$; $\forall x\ \varphi \Leftrightarrow \rceil(\exists x\ \rceil\varphi)$.

откуда по правилу введения конъюнкции [6] заключаем:

$$x = y \to (\varphi(x) \wedge \psi(x) \to \varphi(y) \wedge \psi(y)).$$

Рассмотрим, наконец, формулу $\exists z\ \varphi(x, z)$. Из предположения

$$x = y \to (\varphi(x, z) \to \varphi(y, z))$$

по правилу введения квантора существования [6] получаем

$$x = y \to (\varphi(x, z) \to \exists t\ \varphi(y, t)),$$

откуда контрапозицией приходим к

$$x = y \to (\forall t\ \rceil\varphi(y, t) \to \rceil\varphi(x, z)),$$

где применяем правило введения квантора всеобщности [6]:

$$x = y \to (\forall t\ \rceil\varphi(y, t) \to \forall t\ \rceil\varphi(x, t)),$$

откуда заменой переменных и по правилу контрапозиции получим:

$$x = y \to (\exists z\ \varphi(x, z) \to \exists z\ \varphi(y, z)).$$

Итак, мы показали, что при построении произвольной формулы, отправляясь от атомарной формулы, на каждом шаге построения формула удовлетворяет свойству 2). Таким образом, для любой заданной формулы $\varphi(x)$ свойство 2) выполнено. □

Данная теорема о равенстве показывает, что равенство множеств, определенное нами через атомарную формулу принадлежности, удовлетворяет аксиомам равенства, сформулированным Гильбертом в «Основаниях математики» [6].

Аксиома регулярности выражает несколько иное свойство множеств, чем то, которое было обозначено нами 7), а именно: в каждом множестве есть наименьший по принадлежности элемент. Почему это так, нам еще предстоит выяснить. Обычно множества, удовлетворяющие аксиоме S7, называют *фундированными* (см., например, [7, 8]), что отмечено нами в названии аксиомы. На самом деле, любое фундированное множество регулярно, о чем также пойдет речь в следующем параграфе.

Роль схемы аксиом подстановки и аксиомы бесконечности мы установим немного позднее, когда уже будет накоплен некоторый опыт работы с множествами.

В этом параграфе мы рассмотрели формальную аксиоматику теории множеств и соответствующий формальный язык ZF. В дальнейшем мы не будем придерживаться только языка ZF при построении тех или иных объектов в теории множеств и при доказательстве ее теорем. Это неразумно, т. к. формальный язык, будучи чрезвычайно строгим инструментом, не является удобочитаемым языком. Поэтому чаще всего мы будем применять разговорный (русский) язык и сокращения для термов, принятых нами во введении, однако при этом не следует забывать о том, что все наши рассуждения о множествах должны формализовываться в ZF.

Все последующее построение теории называется *содержательной* частью теории множеств, ибо под множествами мы будем все же понимать не чисто формальные термы, а некоторые вполне понятные нам объекты.

§ 1.2 Основные свойства множеств

Приведем здесь еще раз сокращения записи множеств, используемые в нашем изложении: $\{x|\ \varphi(x)\}$, $\{a, b\}$, $a \cap b$, $a \cup b$, $a \setminus b$, $\cup a$, $\mathrm{Exp}(a)$, $S(a)$, $\emptyset$.

То, что большинство из этих термов являются множествами, нам еще предстоит доказать. А сейчас условимся, что в качестве переменных, обозначающих множества, мы будем использовать не только строчные латинские буквы $a, b, \ldots, z$, но также заглавные $A, B, \ldots, Z$, кроме S (она занята у нас для обозначения последующего множества), все греческие, кроме φ, ψ и ω, и все готические $\mathfrak{A}, \mathfrak{a}$, $\mathfrak{B}, \mathfrak{b}, \ldots$, $\mathfrak{Z}, \mathfrak{z}$, кроме $\mathfrak{c}$, $\mathfrak{V}$ и $\mathfrak{U}$, сочетая их с различными математическими акцентами (например, A', $\tilde{x}$ и прочее). Буквы ω, $\mathfrak{c}$, $\mathfrak{V}$ и $\mathfrak{U}$ будут использоваться нами как обозначения некоторых конкретных объектов, т. е. в качестве термов-констант.

Кроме перечисленных способов записи множеств (термов) мы будем вводить и новые, но в силу достаточно большого их количества мы не будем перечислять здесь все эти термы, а вместо этого условимся, что всякое новое обозначение мы будем вводить либо средствами разговорного (русского) языка, либо при помощи символа $:=$, как мы это уже делали ранее. Этот же символ мы будем использовать при определении некоторых формул, например, $\varphi(x) := \emptyset \in x$.

Теорема 1.2. *Пусть A, B — множества, φ — некоторая формула языка* ZF*. Тогда термы $\{x|\ x \in A \wedge \varphi(x)\}$, $\{A, B\}$, $A \cap B$, $A \cup B$, $A \setminus B$, $\cup A$, $\mathrm{Exp}(A)$, $S(A)$, $\emptyset$ суть множества.*

Доказательство. Для термов $\{x|\ x \in A \wedge \varphi(x)\}$, $\{A, B\}$, $\cup A$, $\mathrm{Exp}(A)$, $\emptyset$ доказательство непосредственно вытекает из аксиом S2—S6. Рассмотрим терм $A \cup B$. Нетрудно видеть, что $A \cup B = \cup\{A, B\}$, откуда по аксиоме пары и аксиоме объединения получаем, что $A \cup B$ есть множество. $A \cap B = \{x | x \in A \wedge x \in B\}$, откуда по аксиоме содержательности получаем, что и $A \cap B$ — множество. Аналогично проверяется терм $A \setminus B$. Далее, поскольку $S(A) = A \cup \{A\}$ и $\{A\} = \{A, A\}$, то по уже доказанному $S(A)$ — множество. □

Часто вместо терма $\{x|\ x \in A \wedge \varphi(x)\}$ используют семантически равный ему терм $\{x \in A|\ \varphi(x)\}$, чтобы подчеркнуть, что данный терм определяет множество как часть другого более широкого множества A при помощи формулы $\varphi(x)$, и в этом случае говорят, что множество $\{x \in A|\ \varphi(x)\}$ является *определяемой* (формулой φ) *частью* множества A.

Итак, мы видим, что для терма $\{x|\ \varphi(x)\}$ мы не всегда можем сказать, что он является множеством, аксиома содержательности, которая ограничивает нас в этом, — это своеобразная «плата» за устранение известных парадоксов теории множеств. Однако мы найдем применение и терму $\{x|\ \varphi(x)\}$ в общем виде, когда будем вести разговор о классах множеств (§ 1.7). Основная же часть теории (не касающаяся классов множеств), подчеркнем еще раз, должна формализовываться в языке ZF.

Обратимся теперь к аксиоме регулярности S7. Фактически эта аксиома утверждает, что для каждого множества x оно либо пусто, либо в нем найдется такой элемент z, что пересечение $z \cap x$ пусто. Это требование (фундированность) более сильное, чем регулярность, в чем нас убеждает следующая

Теорема 1.3. *Для любых множеств A и B*

$$A \notin A, \qquad A \in B \to B \notin A.$$

Доказательство. Предположим, $A \in A$. Рассмотрим множество $\{A\}$. В этом множестве по аксиоме регулярности существует элемент z (т. к. $\{A\}$ не пусто), не имеющий общих элементов с A. Очевидно, что $z = A$, а по аксиоме регулярности $\emptyset = z \cap A = A \cap A = A$, что противоречит тому, что A не пусто (ведь $A \in A$).

Для доказательства второй части утверждения рассмотрим множество $\{A, B\}$. По аксиоме регулярности существует $z \in \{A, B\}$ такой, что $z \cap \{A, B\} = \emptyset$, откуда $A \cap \{A, B\} = \emptyset$ или $B \cap \{A, B\} = \emptyset$.

Если $A \cap \{A, B\} = \emptyset$, то $B \notin A$. Если же $B \cap \{A, B\} = \emptyset$, то $A \notin B$. Противоречие. Итак, $B \notin A$. □

Замечание 1. Аналогичные теоремы можно доказывать для произвольных конечных последовательностей множеств. Так, например, если имеет место $A \in B \in C \in D \in E$, то не верно, что $E \in A$. Для доказательства нужно рассмотреть множество $\{A, B, C, D, E\}$, которое является множеством как определяемая часть множества $\mathrm{Exp}(A \cup B \cup C \cup D \cup E)$, и вновь применить аксиому регулярности. Этот пример можно обобщить и до бесконечных наборов множеств с некоторыми ограничениями.

Определение 1.1. Пусть задана некоторая формула $\varphi(x)$ языка ZF. Мы говорим, что формула φ определяет множество a *однозначно*, или что a, для которого φ истинно, *единственно*, если $\varphi(a)$ и для любых x, y из того, что $\varphi(x) \wedge \varphi(y)$, следует $x = y$.

Читателю предлагается самостоятельно проверить, что все конструкции множеств $\{x \in A |\ \varphi(x)\}$, $\{A, B\}$, $A \cap B$, $A \cup B$, $A \setminus B$, $\cup A$, $\mathrm{Exp}(A)$, $S(A)$, $\emptyset$ определяются однозначно по исходным множествам A, B и формуле φ.

Определение 1.2. *Упорядоченной парой* (по Курато́вскому) множеств a и b называется терм $\{\{a\}, \{a, b\}\}$, для которого впредь мы будем использовать обозначение (a, b), а множества a и b называются, соответственно, *левой* и *правой координатами* пары (a, b).

Теорема 1.4. *Упорядоченная пара множеств есть множество и для любых множеств a, b, c, d имеем:*

$$(a, b) = (c, d) \Leftrightarrow (a = c) \wedge (b = d)$$

Доказательство. По аксиоме пары нетрудно получить, что $\{a\}$ и $\{a, b\}$ суть множества, поэтому (x, y) также множество по аксиоме пары. Докажем вторую часть теоремы.

Импликация справа налево следует из определения упорядоченной пары и ее единственности при заданных координатах.

Пусть $(a, b) = (c, d)$, т. е. $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. По аксиоме пары здесь возможны следующие варианты: $\{a\} = \{c\} \wedge \{a, b\} = \{c, d\}$ или $\{a\} = \{c, d\} \wedge \{a, b\} = \{c, d\}$ или $\{a\} = \{c, d\} \wedge \{a, b\} = \{c\}$ или $\{a\} = \{c\} \wedge \{a, b\} = \{c\}$.

Пользуясь определением равенства, в первом случае получим $a = c$ и если $b = c$, то и $c = d$ и, следовательно, $b = d$, если $b \neq c$, то $b = d$. Так или иначе, получаем $a = c \wedge b = d$.

Предположим далее, что $\{a\} = \{c, d\} \wedge \{a, b\} = \{c, d\}$. Из первого равенства вытекает $a = c = d$, тогда из второго равенства получаем

$\{a, b\} = \{a\}$, поэтому $a = b = c = d$. Пусть теперь $\{a\} = \{c, d\} \wedge \{a, b\} = \{c\}$. Тогда $a = c = d$ и $c = a = b$, откуда вновь $a = b = c = d$.

Наконец, в последнем случае $\{a\} = \{c\} \wedge \{a, b\} = \{c\}$ получаем $a = c$ и $c = a = b$. Поэтому из $(a, b) = (c, d)$ следует $\{\{a\}\} = \{\{a\}, \{a, d\}\}$, откуда $\{a, d\} = \{a\}$, откуда $a = d$. В итоге вновь получим $a = b = c = d$. □

Определение 1.3. *Прямым (декартовым) произведением* множеств A и B называется терм

$$A \times B := \{z | \exists u \in A : \exists v \in B : z = (u, v)\},$$

а множества A и B называются, соответственно, *левым* и *правым* сомножителями произведения $A \times B$

Теорема 1.5. *Прямое произведение множеств есть множество и определяется однозначно по множествам A и B.*

Доказательство. Пусть A и B множества. Если $a \in A$, $b \in B$, то $\{a\} \in \mathrm{Exp}(A \cup B)$, а также $\{a, b\} \in \mathrm{Exp}(A \cup B)$. Поэтому $(a, b) \subseteq \mathrm{Exp}(A \cup B)$, откуда следует $(a, b) \in \mathrm{Exp}(\mathrm{Exp}(A \cup B))$. Тогда

$$A \times B = \{x \in \mathrm{Exp}(\mathrm{Exp}(A \cup B)) | \exists a \in A : \exists b \in B : x = (a, b)\}.$$

Поэтому в силу аксиомы степенного множества и аксиомы содержательности прямое произведение $A \times B$ есть множество.

Однозначность построения $A \times B$ по множествам A и B вполне очевидна. □

§ 1.3 Определяемые отображения и функции

Пусть имеется некоторая формула $\varphi(x, y)$ языка ZF, в которой переменные x, y входят свободно.

Определение 1.4. Мы говорим, что формула φ *определяет* $(x \mapsto y)$*—отображение*, если, во-первых, существуют x, y такие, что $\varphi(x, y)$, во-вторых, всякий раз из того, что $\varphi(x, y) \wedge \varphi(x, z)$ следует $y = z$.

Значок $(x \mapsto y)$, являющийся, вообще говоря, термом со свободными переменными x, y, мы будем употреблять по мере необходимости, точнее, тогда, когда нам будет важно указать данные переменные в данном порядке, например, при формальном выводе некоторых формул.

Пусть $\varphi(x, y)$ определяет отображение, и пусть A — множество. Язык теории множеств, описанный нами во введении, позволяет нам определить терм

$$ran\,(\varphi|A) := \{z|\ \exists x \in A:\ \varphi(x, z)\}.$$

Можно ли определить такое множество в теории ZF? Чтобы ответить на этот вопрос, заметим для начала, что формула

$$\exists x \in A:\ \varphi(x, z)$$

эквивалентна формуле [3]

$$\exists x \in A:\ (\varphi(x, z) \wedge (\forall w\ \varphi(x, w) \to z = w)).$$

Теперь обратимся к аксиоме подстановки S8. Нетрудно видеть, что элементы множества u, существование которого нам гарантирует эта аксиома, определяются ровно таким же способом (учитывая показанную эквивалентность), как элементы $ran\,(\varphi|A)$. Поэтому

$$ran\,(\varphi|A) = \{z|\ \exists x \in A:\ (\varphi(x, z) \wedge \forall w\ (\varphi(x, w) \to z = w))\},$$

откуда $ran\,(\varphi|A)$ — множество. В этом, собственно, и заключается роль схемы аксиом подстановки, точнее, если у нас имеется некое множество и формула, определяющая отображение, то по этому множеству и формуле мы можем построить новое множество $ran\,(\varphi|A)$, которое мы впредь будем называть *областью значений* определяемого формулой φ отображения *относительно* множества A.

Приведем пример одного часто используемого в теории множеств определяемого отображения. Рассмотрим формулу $\varphi(x, y) := y = S(x)$, которая, как мы знаем, достаточно просто формализуется в ZF. Пусть $x' = \emptyset$, $y' = \{\emptyset\}$. Нетрудно убедиться в том, что $y' = S(x')$ при выбранных x', y'. Далее, предположим, что $y = S(x) \wedge z = S(x)$. Тогда, как легко проверить, $y = z$. Поэтому формула $y = S(x)$ определяет отображение. Назовем тогда букву S отображением, определяемым формулой $y = S(x)$. Тогда для каждого множества A область значений $ran\,(y = S(x)|A)$ отображения S относительно множества A будет множеством по аксиоме подстановки.

[3] Говоря точнее, из условия, что $\varphi(x, y)$ определяет $(x \mapsto y)$ — отображение, можно вывести эквивалентцию указанных формул, а значит, и показать их дедуктивное равенство [6].

Перейдем к определению функции. Обычно в математике под функцией принято понимать некоторое правило, по которому элементам одного множества ставятся в соответствие элементы другого множества так, что каждому элементу первого соответствует один и только один элемент второго. Поскольку мы хотим использовать теорию множеств для описания всех математических объектов, то такое определение функции нас, понятно, не устроит. Ведь объектами изучения аксиоматической теории множеств ZF являются множества и только множества. Поэтому нам нужно определить функцию именно как некоторое множество и никак иначе. Для этого мы воспользуемся понятием, также часто используемым математиками, — график функции. Ведь график функции, определенной на множестве A и принимающей значения из множества B, есть не что иное как подмножество прямого произведения $A \times B$ с некоторыми специфическими свойствами. На этом и основано определение функции в теории множеств Цермело—Френкеля.

Определение 1.5. Подмножество $f \subseteq A \times B$ прямого произведения множеств A и B называется *функцией* (из A в B), если:

1) для каждого $x \in A$ существует $y \in B$ такое, что $(x, y) \in f$;
2) из $(x, y) \in f \wedge (x, z) \in f$ следует $y = z$.

Тот факт, что f есть функция из A в B принято записывать в виде следующей сокращенной записи формулы: $f : A \to B$, при этом говорят, что множество A есть *область определения* функции f. Для обозначения области определения функции используют также терм $dom\,(f)$. Для каждого множества $x \in A$ мы можем рассмотреть единственное множество $y \in B$ такое, что $(x, y) \in f$. Условимся это множество, однозначно определяемое функцией f и множеством x, обозначать термом $f(x)$, который будем называть *значением функции f в точке x*. Тогда вместо формулы $(x, y) \in f$ мы можем записывать эквивалентную ей формулу $y = f(x)$, либо $f(x) = y$.

Множество

$$ran\,(f) := \{y \in B | \ \exists x \in A \ y = f(x)\}$$

называется *областью значений* функции f.

Функция $f : A \to B$ называется *сюръекцией*, если $ran\,(f) = B$, *инъекцией*, если для любых $x, y \in A$ из равенства $f(x) = f(y)$ вытекает $x = y$, *биекцией* (взаимно однозначным соответствием), если f инъекция и сюръекция одновременно. Для обозначения того факта, что f есть биекция из A в B, мы используем символ $f : A \leftrightarrow B$. Если же мы хотим выразить то, что существует биекция из A в B, то мы пишем $A \leftrightarrow B$.

Пусть $f : A \to B$ и $D \subseteq A$, $D \neq \emptyset$. Тогда функция

$$f|_D := \{(x, y) \in A \times B |\ x \in D \wedge (x, y) \in f\}$$

называется *сужением* функции f на множество D.

Пусть теперь $f : A \to B$, $g : B \to C$, тогда функция $h : A \to C$, определяемая как $h = \{(x, z) \in A \times C |\ z = g(f(x))\}$, называется *суперпозицией* функций f и g, для нее обычно используется обозначение $g \circ f$.

Функция $f : A \to A$ называется *тождественной* на A, если для каждого $x \in A$ имеем $f(x) = x$. В этом случае для f принято использовать обозначение id_A.

Мы говорим, что для функции $f : A \to B$ функция $g : B \to A$ является *обратной*, если их суперпозиция тождественна, т. е. $g \circ f = id_A$. Для обратной к f функции используется обычное обозначение f^{-1}.

Следующая теорема показывает некоторые тривиальные свойства обратных функций и биекций.

Теорема 1.6. *$f : A \to B$, тогда:*

1) *существует f^{-1} тогда и только тогда, когда f — биекция;*

2) *если существует f^{-1}, то f^{-1} — биекция;*

3) *если существует f^{-1}, то f суть обратная к f^{-1} функция.*

Введем теперь еще несколько полезных обозначений и понятия образа и прообраза множества относительно функции.

Если $f : A \to B$ и C есть подмножество в A, то множество

$$fC := \{y \in B |\ \exists x\ (x \in A \wedge y = f(x))\}$$

называется *образом множества C относительно функции f*.

Если $f : A \to B$ и $C \subseteq B$, то множество

$$f^{-1}C := \{x \in A |\ f(y) \in C\}$$

называется *прообразом множества C относительно функции f*. Следует обратить внимание на то, что множество C здесь вовсе не обязано быть подмножеством области значений функции f, а также вполне может быть пустым множеством (в этом случае, очевидно, образ и прообраз также будут пусты), и, кроме того, обратная функция к функции f может и не существовать.

Если множество C в том и другом случае записано в виде длинного многосимвольного терма, то удобнее заключать его в скобки, поэтому для обозначений образов и прообразов разрешим использовать и такие обозначения: [4]

$$f[C] \text{ — для образа,} \qquad f^{-1}[C] \text{ — для прообраза.}$$

Использование круглых скобок здесь недопустимо, ибо так мы обозначаем значение функции в данной точке.

Предположим далее, что формула $\varphi(x, y)$ определяет $(x \mapsto y)-$отображение, и рассмотрим множество A такое, что существует $x \in A$, для которого найдется y такой, что $\varphi(x, y)$. Как мы уже знаем, существует множество $ran\,(\varphi|A)$ — область значений определяемого формулой φ отображения относительно A. Рассмотрим подмножество f прямого произведения $A \times ran\,(\varphi|A)$, определяемое следующим образом:

$$f = \{(x, y) \in A \times ran\,(\varphi|A) \mid \varphi(x, y)\}.$$

Поскольку φ определяет отображение, то для f, очевидно, выполнено второе требование определения функции. Обозначим далее через D подмножество множества A, включающее все те $x \in A$, для которых $\varphi(x, y)$ истинно при каком-нибудь y. Тогда множество f будет функцией из множества D в множество $ran\,(\varphi|A)$, причем $ran\,(f) = ran\,(\varphi|A)$.

Итак, мы видим, что по всякой формуле, определяющей отображение, можно построить функцию (и даже далеко не одну). Для такой функции обычно используется термин *сужение отображения*. В наших обозначениях f есть сужение определяемого формулой φ отображения на множество D. Понятие функции позволяет нам рассматривать сужение отображения на некоторое (произвольно выбранное) множество и, таким образом, вместо формулы (объекта изучения метатеории) рассматривать вполне определенное множество (объект изучения теории ZF).

Отметим также, что для всякой функции f можно определить формулу $\varphi(x, y) := (x, y) \in f$, и эта формула, как нетрудно проверить, будет определять $(x \mapsto y)-$отображение. Поэтому функцию мы иногда будем называть *определяемым отображением* или просто *отображением*.

В математике часто используется такое понятие как индекс. Здесь мы намерены формализовать представление об индексе (хотя бы частично).

[4] Куратовский и Мостовский [9] используют символ $f^1(C)$ для обозначения образа множества C.

Пусть имеется сюръекция $f : I \to X$. В этом случае мы можем говорить, что *множество X проиндексировано множеством I*, при этом функцию f мы будем называть *индексацией*. С чем связана такая терминология? Понятно, что поскольку функция f является сюръекцией, то для множества X справедливо равенство $X = \{f(i) | \ i \in I\}$. Введем вместо терма $f(i)$ терм x_i. Тогда множество X можно записать в виде терма $\{x_i | \ i \in I\}$. Часто вместо такого терма используют обозначение $\{x_i\}_{i\in I}$. В таком виде обычно записываются последовательности (в анализе) и другие проиндексированные семейства множеств. Переменную i при этом принято называть *индексом*.

Еще раз отметим, что в силу аксиомы подстановки S8 $\{x_i\}_{i\in I}$ является множеством, если I — множество. Понятно, что переменные x и i могут быть заменены на другие, лишь бы только не возникало, как мы говорим, коллизий между переменными.

Индекс удобно использовать, например, для обозначения объединения элементов множества X: $\bigcup\limits_{i\in I} x_i$, или их пересечения: $\bigcap\limits_{i\in I} x_i$.

§ 1.4 Отношения и их свойства

Определение 1.6. Любое подмножество множества $A\times A$ называется *бинарным отношением* (или *отношением*) на A.

«Вырожденные» случаи отношений на A: пустое $\emptyset$ и полное $A \times A$.

Любая функция $f : A \to B$ есть подмножество в $A \times B$, а значит, и в $(A \cup B) \times (A \cup B)$, поэтому f есть отношение на $A \cup B$.

Если R есть отношение на A и $(a, b) \in R$, то это принято записывать так: aRb.

На любом множестве можно задать два также достаточно стандартных отношения: равенство и принадлежность. Для обозначения отношений используют, как правило, разные «экзотические» символы, например, $<, \sim, *, \prec$.

Рассмотрим теперь некоторые виды часто встречающихся в математике отношений.

Определение 1.7. (виды отношений) Отношение R на множестве A называется

а) *рефлексивным*, если для любого x из A имеем xRx.

б) *симметричным*, если для любых $x, y \in A$ из xRy следует yRx.

в) *транзитивным*, если для любых $x, y, z \in A$ из $xRy \wedge yRz$ следует xRz.

г) *отношением эквивалентности*, если оно рефлексивное, симметричное и транзитивное.

Прежде чем перейти к определению отношений порядка, рассмотрим некоторые свойства отношения эквивалентности. Для начала введем следующие обозначения. Чаще всего отношение эквивалентности обозначают символом $\sim$. Множество $[a]_\sim :=\{x \in A |\ x \sim a\}$ для каждого $a \in A$ будем называть *классом эквивалентности* элемента $a \in A$. В случае, когда из контекста очевидно, о каком отношении идет речь, вместо $[a]_\sim$ мы будем писать просто $[a]$. Классы эквивалентности обладают следующим свойством.

Теорема 1.7. *Два класса эквивалентности либо не пересекаются (пересечение пусто), либо совпадают.*

Доказательство. Пусть $\sim$ — отношение эквивалентности на множестве A, $a, b \in A$. Предположим, что $[a] \cap [b] \neq \emptyset$. Тогда существует $c \in [a] \cap [b]$. Тогда $c \sim a$ и $c \sim b$. Отсюда в силу симметричности и транзитивности отношения $\sim$ получаем $a \sim b$. Если $x \in [a]$, то $x \sim a$, откуда $x \sim b$, т. е. $x \in [b]$. Так что $[a] \subseteq [b]$. Аналогично получаем $[b] \subseteq [a]$. Итак, $[a] = [b]$. $\square$

Нетрудно показать (используя аксиому степенного множества), что для любого множества A и любого отношения эквивалентности на множестве A существует множество всех классов эквивалентности множества A. Для его обозначения используют символ $A/_\sim$ и называют *фактор-множеством* множества A. Итак,

$$A/_\sim :=\{x \in \mathrm{Exp}(A) |\ \exists a \in A :\ x = [a]_\sim\}.$$

Продолжим определение различных видов отношений. Отношение R на множестве A называется

д) *антирефлексивным*, если для любого $a \in A$ имеем $\rceil(aRa)$.

е) *частичным упорядочением* (или *частичным порядком*), если R антирефлексивно и транзитивно.

ж) частичное упорядочение называется *линейным порядком*, если для любых элементов $a, b \in A$ выполнено условие *связности*:

$$(aRb) \vee (a = b) \vee (bRa)$$

Чаще всего частичный порядок мы будем обозначать символом $<$ с индексами или без таковых. Если на множестве A задано частичное упорядочение $<$, то пара $(A, <)$ называется частично упорядоченным множеством. Если $<$ — линейный порядок, то $(A, <)$ —

линейно упорядоченное множество. Пусть далее $(A, <)$ — частично упорядоченное множество. Вместо формулы $(x < y) \vee (x = y)$ будем писать, как обычно, $x \leqslant y$. Пусть $B \subseteq A$. Элемент $x \in A$ называется *нижней* (*верхней*) *гранью* множества B, если для любого $b \in B$ имеем $x \leqslant b$ ($b \leqslant x$). Через $\inf B$ ($\sup B$) обозначают *точную* нижнюю (верхнюю) грань множества B, которая должна удовлетворять тому условию, что, во-первых, сама является нижней (верхней) гранью, а во-вторых, для всякой нижней (верхней) грани x множества B имеет место $x \leqslant \inf B$ ($\sup B \leqslant x$). Если $\inf B \in B$, то вместо символа $\inf$ пишут $\min$, в этом случае точная нижняя грань называется *минимумом*. Если $\sup B \in B$, то вместо символа $\sup$ пишут $\max$, и в этом случае точная верхняя грань называется *максимумом*.

Иногда под символами $\sup, \inf, \min, \max$ приписывают обозначение того частичного порядка, в котором они определены, например, $\sup\limits_{<} B$.

Кроме понятия максимума множества есть также понятие максимального элемента множества. Элемент $x \in B$ называется *максимальным* для множества B, если для любого элемента $b \in B$ не верно, что $x < b$. Заметим, что в случае частичного упорядочения формулы $\rceil(x < b)$ и $b \leqslant x$ не эквивалентны, т. к. частичное упорядочение, вообще говоря, не связно, но из второй формулы выводима первая. Поэтому максимум множества B всегда является максимальным элементом, но обратное в общем случае не верно. В случае линейного порядка указанные формулы равносильны. Точнее, справедлива следующая

Теорема 1.8. *Пусть $(A, <)$ — линейно упорядоченное множество и $B \subseteq A$, $B \neq \emptyset$. Тогда следующие утверждения равносильны:*

1) *$x = \max B$;*

2) *для любого $b \in B$ $b \leqslant x$ и $x \in B$;*

3) *x — максимальный элемент в B.*

Равносильными являются также и утверждения

1) *$x = \min B$;*

2) *для любого $b \in B$ $x \leqslant b$ и $x \in B$.*

Введем еще несколько терминов из теории упорядоченных множеств. Пусть по-прежнему $(A, <)$ — частично упорядоченное множество и $B \subseteq A$. Множество B называется *цепью* в A, если частичный порядок $<$ линейно упорядочивает множество B. Цепь называется *ограниченной* в A, если для нее существует верхняя грань в множестве A. Цепь называется *сквозной* в A, если у нее нет верхней грани, не принадлежащей ей самой (т. е. либо у нее вообще нет верхней грани, либо ее верхняя грань в A единственна и является максимумом этой цепи).

Отношение линейного порядка на A называется *вполне упорядочением* (или *полным упорядочением*), если каждое непустое подмножество $B \subseteq A$ имеет минимум. Пара $(A, <)$, где $<$ — вполне упорядочение на A, — называется вполне упорядоченным множеством.

Если $(A, <)$ — частично упорядоченное множество, $a, b \in A$, то множества

$$[a; b] := \{x \in A \mid a \leqslant x \leqslant b\}, \quad [a; b) := \{x \in A \mid a \leqslant x < b\},$$
$$(a; b] := \{x \in A \mid a < x \leqslant b\}, \quad (a; b) := \{x \in A \mid a < x < b\}$$

называются, соответственно, *отрезком* (или *$<$-отрезком*), *полуинтервалами* и *интервалом* (*$<$-интервалом*). В том случае, когда необходимо отметить, каким именно частичным порядком определен отрезок, полуинтервал или интервал, мы допускаем обозначения: $[a; b]_<$, $[a; b)_<$, $(a; b]_<$, $(a; b)_<$.

§ 1.5 Натуральные числа

В этом параграфе мы наконец воспользуемся девятой (последней) аксиомой Цермело—Френкеля из приведенных нами в первом параграфе аксиом S1 − S9 — аксиоматики формальной теории ZF.

Определение 1.8. Всякое множество ω, удовлетворяющее свойствам

1) $\emptyset \in \omega$;

2) $\forall x \in \omega : \ S(x) \in \omega$;

3) $\forall x \in \omega : \ (x \neq \emptyset \to \exists y \in \omega : \ x = S(y))$;

называется множеством (*порядковых*) *натуральных чисел*. Для обозначения такого множества мы всегда будем использовать букву ω. Элементы ω называются (порядковыми) натуральными числами, для их обозначения мы, как правило, будем использовать буквы n, m, l, p, q, s, если не оговорено противное. Условимся также, что пустое множество $\emptyset$ мы будем обозначать как 0 в том случае, если мы используем его как порядковое натуральное число.

Прежде, чем перейти к изучению свойств множества ω, нам необходимо доказать о нем следующий факт.

Теорема 1.9. *Множество ω существует и единственно.*

Доказательство. По аксиоме бесконечности S9 существует множество u, удовлетворяющее следующим свойствам: $\emptyset \in u$ и для всякого $x \in u$ имеем $S(x) \in u$. Таким образом, множество u удовлетворяет требованиям 1) и 2) определения множества ω. Будем называть такие множества *прогрессивными*. В качестве множества натуральных чисел ω мы хотим взять наименьшее из всех прогрессивных множеств, т. е. их пересечение. Точнее, положим

$$\omega = \{x \in u | \, \forall y \; (y \text{ — прогрессивное}) \to x \in y\}.$$

По аксиоме содержательности S6 ω будет множеством. Нетрудно установить, что ω будет прогрессивным множеством, т. е. удовлетворяет 1) и 2). Покажем, что ω удовлетворяет условию 3). Для этого выделим в ω подмножество X, определенное как

$$X = \{x \in \omega | \; x \neq \emptyset \to (\exists y \in \omega : \; x = S(y))\}.$$

Нетрудно показать, что X прогрессивно. Действительно, $\emptyset \in X$ и для каждого $y \in X$ имеем $y \in \omega$ и, поскольку ω прогрессивно, то $S(y) \in \omega$, но $S(y)$ удовлетворяет свойству элементов множества X, поэтому $S(y) \in X$. Итак, X прогрессивно. Тогда с одной стороны имеем $X \subseteq \omega$, с другой — $\omega \subseteq X$, поскольку ω содержится во всех прогрессивных множествах. Таким образом, $X = \omega$.

А это и означает, что для всякого $x \in \omega$ если $x \neq \emptyset$, то существует $y \in \omega$ такой, что $x = S(y)$, т. е. множество ω удовлетворяет 3).

Покажем теперь, что множество ω, удовлетворяющее свойствам 1) − 3), единственно. Пусть для ω' также выполнены условия 1) − 3). Допустим, что множество $\omega \setminus \omega'$ не пусто. Тогда в силу аксиомы регулярности S7 существует $x \in \omega \setminus \omega'$ такой, что $x \cap (\omega \setminus \omega') = \emptyset$. Поскольку $x \neq \emptyset$, то существует $y \in \omega$ такой, что $x = S(y)$. Нетрудно показать, что в этом случае $y \in \omega'$. Но тогда в силу прогрессивности множества ω' имеем $x \in \omega'$. Противоречие. Итак, $\omega \setminus \omega' = \emptyset$. Точно так же доказывается, что $\omega' \setminus \omega = \emptyset$. Таким образом, $\omega = \omega'$. Теорема доказана. □

Вместо символа $\in$ для натуральных чисел принято использовать символ $<$. Это правило будет еще обобщено нами в главе 2. По определению положим $n + 1 := S(n)$ для всякого $n \in \omega$. Далее мы займемся изучением структуры множества ω.

Теорема 1.10. *Множество ω удовлетворяет аксиомам Пеано:*

1) $0 \in \omega$;

2) *для любого* $n \in \omega$ *имеем* $n+1 \in \omega$;

3) *для любого* $n \in \omega$ *верно* $n+1 \neq 0$;

4) *для любых* $n, m \in \omega$ $n = m \Leftrightarrow n+1 = m+1$;

5) *если* $X \subseteq \omega$ *и* X *прогрессивно, то* $X = \omega$.

Доказательство этой теоремы несложно, и мы предлагаем провести его читателю самостоятельно. Следующая теорема выражает известный принцип *математической индукции*.

Пусть $\varphi(x)$ — произвольная формула языка ZF.

Теорема 1.11. *Если* $\varphi(0)$ *и для каждого* $n \in \omega$ *имеем* $\varphi(n) \to \varphi(n+1)$, *то тогда* $\forall n \in \omega : \ \varphi(n)$.

Доказательство. Пусть $X = \{x \in \omega | \ \varphi(x)\}$. Нетрудно убедиться в том, что X есть прогрессивное множество и $X \subseteq \omega$, поэтому $X = \omega$, откуда $\forall n \in \omega : \ \varphi(n)$. □

Определение 1.9. Множество X назовем *транзитивным*, если для каждого $x \in X$ имеем $x \subseteq X$.

Теорема 1.12. *ω и каждый его элемент транзитивны.*

Доказательство. Обозначим через X множество всех таких $n \in \omega$, для которых $n \subseteq \omega$. Понятно, что $X \neq \emptyset$, т. к. $0 \in X$. Пусть $n \in X$, отсюда следует, что $n \subseteq \omega$ и $\{n\} \subseteq \omega$. Поэтому и множество $n \cup \{n\} = n + 1$ содержится в ω. Таким образом, $n+1 \in X$. По принципу полной индукции получаем, что $X = \omega$. Таким образом, ω транзитивно.

Для доказательства транзитивности всех $n \in \omega$ снова воспользуемся индукцией по n. Очевидно, что 0 транзитивен. Предположим, что транзитивно n. Рассмотрим множество $n+1 = n \cup \{n\}$. Пусть $k \in n$. Тогда либо $k \in n$, либо $k = n$. В случае $k \in n$ имеем $k \subseteq n$, откуда $k \subseteq n+1$. В случае $k = n$ очевидно, что $k \subseteq n+1$. Итак, $n+1$ транзитивно. По принципу индукции заключаем, что каждое порядковое натуральное число транзитивно. □

Приведенная теорема позволяет описать нам натуральные числа следующим образом:

$$0=\emptyset,\quad 1=\{0\},\quad 2=\{0,1\},\quad 3=\{0,1,2\},$$
$$n+1=\{0,\dots,n\}:=\{m\in\omega|\ m\leqslant n\}$$

для каждого $n\in\omega$. Доказательство этого факта мы отложим пока до главы 2, в которой мы в общем виде (для всех ординалов) докажем ряд полезных свойств порядковых чисел (в частности натуральных) таких, как, например, вполне упорядочение их отношением принадлежности.

Об арифметических операциях (сложение и умножение) на натуральных числах речь пойдет в следующей главе (§ 2.3), когда мы будем заниматься построением арифметики ординалов.

Ранее мы уже рассматривали на произвольных множествах такие операции, как объединение, пересечение, разность, произведение двух множеств. Все эти операции мы относим к *арифметике множеств*. Теперь мы хотим пополнить список арифметических операций на множествах сложением и умножением.

§ 1.6 Суммы и произведения упорядоченных множеств

Пусть $\{L_x\}_{x\in C}$ — проиндексированное множество множеств.

Определение 1.10. Множество

$$\bigcup_{x\in C}\{x\}\times L_x$$

называется *прямой суммой* (или *дизъюнктным объединением*) *множеств* L_x по множеству C и обозначается $\sum\limits_C L_x$.

Пусть далее $(C,<_c)$ — линейно упорядоченное множество и $\{<_x \mid x\in C\}$ — множество линейных порядков на множествах L_x, так что для каждого $x\in C$ множество L_x линейно упорядочено отношением $<_x$.

На прямой сумме $\sum\limits_C L_x$ мы рассмотрим отношение $\prec$, удовлетворяющее следующим условиям:

$$(x,a)\prec(y,b)\Leftrightarrow\begin{cases}x<_c y \ \text{ или}\\ x=y\wedge a<_x b\ \ (a,b\in L_x)\end{cases}$$

для любых $(x, a), (y, b) \in \sum\limits_C L_x$.

Пара $\left(\sum\limits_C L_x, \prec\right)$ называется *канонической суммой* (или просто суммой) линейно упорядоченных множеств по линейно упорядоченному множеству, а отношение $\prec$ в этом случае называется *каноническим* (линейным) порядком. Несложно проверяется следующее утверждение о сумме линейно упорядоченных множеств.

Теорема 1.13. *Сумма линейно упорядоченных множеств по линейно упорядоченному множеству линейно упорядочена.*

Если мы теперь предположим, что все линейные порядки $<_x$ суть вполне упорядочения множеств L_x, а $<_c$ — вполне упорядочение множества C, то, введя аналогично термин суммы вполне упорядоченных множеств по вполне упорядоченному множеству, легко показать усиление предыдущей теоремы, а именно

Теорема 1.14. *Сумма вполне упорядоченных множеств по вполне упорядоченному множеству вполне упорядочена.*

Следующий вопрос, который мы здесь рассмотрим, — это произведения множеств. Ранее мы уже говорили о прямом произведении двух множеств. Теперь же мы хотим обобщить это понятие на произвольный набор (множество) множеств. Как определить, например, произведение множеств A, B и C? Можно воспользоваться понятием упорядоченной пары, и на ее основе построить упорядоченную тройку как $((a, b), c)$, где $a \in A$, $b \in B$, $c \in C$. Нетрудно показать, что существует множество всех таких троек (оно равно $(A \times B) \times C$). Однако уже в этом случае видно «неравноправное» вхождение компонентов тройки, ибо мы могли бы определить тройку как $(a, (b, c))$ и получить в итоге, вообще говоря, совершенно иное прямое произведение трех наших множеств. Для того, чтобы нам не приходилось выбирать и, кроме того, легко обобщить понятие упорядоченной пары до упорядоченного набора (кортежа), мы поступим следующим образом. Каждый упорядоченный набор элементов мы будем рассматривать как функцию, определенную на некотором упорядоченном множестве (например, числовая последовательность в анализе). Это позволит нам задавать сколь угодно большие упорядоченные наборы множеств. Перейдем к определению.

Вновь рассмотрим множество $\{L_x\}_{x \in C}$, проиндексированное множеством C.

Определение 1.11. Множество

$$\prod_C L_x := \left\{ f \,\Big|\, (f : C \to \bigcup_{x \in C} L_x) \wedge (\forall x \in C : \ f(x) \in L_x) \right\}$$

называется *прямым произведением* множеств L_x по множеству C.

На вопрос — пусто или нет это множество — мы не можем пока дать определенный ответ за исключением того случая, когда $C = n$, т. е. когда индексирующее множество является натуральным числом. При $C = n$ мы можем доказать существование хотя бы одной функции, являющейся элементом произведения, при бесконечных C — нет, и этот вопрос мы отложим до § 2.4 об аксиоме выбора. Теперь же мы предположим, что произведение не пусто, и перейдем к изучению его свойств.

Функции, являющиеся элементами прямого произведения множеств, называются *кортежами*. Если для любого $x \in C$ имеем $L_x = L$ при некотором множестве L, то вместо $\prod\limits_C L_x$ используют символ L^C (Йех в [10] предлагает символ ${}^C L$), который, в сущности, обозначает множество всех функций из C в L. Заметим, что поскольку все L_x одинаковы, то при любом сколь угодно большом множестве C мы можем доказать существование функции из C в L, т. е. что множество L^C не пусто.

В качестве примеров приведем следующие: $\mathbb{R}^n$ — множество всех n-ок вещественных чисел, $\mathbb{R}^\omega$ — множество всех последовательностей вещественных чисел, 2^ω, где $2 = \{0, 1\}$, — множество всех булевых (двоичных) последовательностей.

Предположим далее, что на каждом множестве L_x задан линейный порядок $<_x$, а на множестве C задано вполне упорядочение $<_c$. Определим на множестве $\prod\limits_C L_x$ отношение $\prec$ следующим образом: для любых $f, g \in \prod\limits_C L_x$ положим

$$f \prec g \Leftrightarrow \begin{cases} \exists x \in C : \ f(x) <_x g(x) \ \text{ и} \\ \forall z \in C : \ (z <_c x \to f(z) = g(z)). \end{cases} \tag{1.1}$$

Пара $\left(\prod\limits_C L_x, \prec\right)$ называется *каноническим произведением* (или просто произведением) линейно упорядоченных множеств по вполне упорядоченному множеству, а отношение $\prec$ — *каноническим* (линейным) порядком. Справедлива следующая

Теорема 1.15. *Произведение линейно упорядоченных множеств по вполне упорядоченному множеству линейно упорядочено.*

Доказательство. Для того, чтобы установить, что $\prec$ есть линейный порядок, очевидно, надо показать, что отношение $\prec$ антирефлексивно, транзитивно и связно.

1) Покажем антирефлексивность $\prec$. Если предположить $f \prec f$, то из (1.1) получим, что существует $x \in C$ такой, что $f(x) <_x f(x)$, что противоречит антирефлексивности линейного порядка $<_x$.

2) Покажем транзитивность $\prec$. Пусть $f \prec g$ и $g \prec h$. Тогда существуют $x, y \in C$ такие, что $f(x) <_x g(x)$, $g(y) <_y h(y)$ и для любого $z \in C$ из $z <_c x$ следует $f(z) = g(z)$ и из $z <_c y$ следует $g(z) = h(z)$. Обозначим через a минимум множества $\{x, y\}$, т. е. $a = \min\{x, y\}$. Нетрудно проверить, что в этом случае $f(a) <_a h(a)$, т. к. имеют место неравенства $f(a) \leqslant_a g(a)$ и $g(a) \leqslant_a h(a)$, причем по крайней мере одно из неравенств строгое. Для любого $z <_c a$ имеем $z <_c x$ и $z <_c y$ и, следовательно, $f(z) = g(z) = h(z)$. Итак, $f \prec h$.

Пункты 1) и 2), в доказательстве которых мы использовали только линейное упорядочение множества C и частичное упорядочение множеств L_x, показывают, что произведение частично упорядоченных множеств по линейно упорядоченному множеству есть частично упорядоченное множество. Можно также показать, что снятие условия связности с отношения $<_c$ не позволит нам доказать этот факт.

3) Покажем теперь связность отношения $\prec$. Пусть $f, g \in \prod\limits_C L_x$. Пусть также $f \neq g$. Нам необходимо показать, что либо $f \prec g$, либо $g \prec f$.

Выделим в множестве C множество B, составленное из всех таких $x \in C$, для которых $f(x) \neq g(x)$. Ясно, что $B \neq \emptyset$ (иначе бы функции f и g были бы равны). В силу того, что $<_c$ суть полное упорядочение, существует $x = \min B$. Понятно, что, во-первых, $f(x) \neq g(x)$, а во-вторых, для каждого $z <_c x$ имеем $f(z) = g(z)$. Теперь, в силу связности отношения $<_x$ получим: $f(x) <_x g(x)$ или $g(x) <_x f(x)$. Если $f(x) <_x g(x)$, то и $f \prec g$, если $g(x) <_x f(x)$, то $g \prec f$. Таким образом, отношение $\prec$ связно, и теорема доказана. □

Для того, чтобы добиться полного упорядочения прямого произведения множеств, не достаточно предположить дополнительно, что $<_x$ суть вполне упорядочения множеств L_x, как это было в случае суммы множеств. Необходимо также предположить, что множество C конечно, или, не теряя общности, что множество C есть натуральное число. Сформулируем этот результат в виде теоремы.

Теорема 1.16. *Произведение вполне упорядоченных множеств по на-*

туральному числу является вполне упорядоченным множеством.

Проверку этой теоремы мы предлагаем читателю.

В качестве примера скажем, что на основании этой теоремы нетрудно указать полное упорядочение такого множества, как ω^n. Для того, чтобы убедиться в том, что условие конечности множества C в общем случае мы снять не можем, приведем один простой пример. Рассмотрим произведение 2^ω (множество всех булевых последовательностей) с каноническим линейным порядком $\prec$. Выделим в этом множестве подмножество B последовательностей $f_k(n)$, определяемых формулами:

$$f_k(n) = \begin{cases} 0, & n \leqslant k \\ 1, & n > k \end{cases}$$

Нетрудно проверить, что $f_k \prec f_m$ тогда и только тогда, когда $m < k$ (здесь символ $<$ обозначает порядок на натуральных числах). Понятно, что в таком множестве нет наименьшего элемента (т. к. в ω нет наибольшего), а значит, 2^ω невозможно вполне упорядочить канонически.

§ 1.7 Классы множеств

В этом параграфе мы рассмотрим понятие класса, которое, вообще говоря, не принято формализовывать в ZF, но поскольку, как показано в [7], введение понятия класса в теорию множеств не приводит к противоречию, более того, обогащает теорию множеств, то мы намерены также воспользоваться и этим понятием. Образно говоря, *класс* — это произвольный определяемый набор множеств. Точнее говоря, если у нас имеется некая формула $\varphi(x)$ языка ZF, то терм $\{x|\ \varphi(x)\}$ является классом. Каждое множество является классом (т. к. $A = \{x|\ x \in A\}$ для любого множества A), но не каждый класс является множеством (об этом пойдет речь ниже). Классы, не являющиеся множествами, мы называем *собственно* классами. Для обозначения классов мы используем новый сорт переменных — каллиграфические латинские буквы $\mathcal{A}, \dots, \mathcal{Z}$, — и константы $\mathfrak{V}$ и $\mathfrak{U}$. Мы также оставляем за собой право использовать некоторые специальные символы (например, Card, Card_τ или $\aleph$) для обозначения некоторых конкретных классов. Все эти символы будут определены нами в дальнейшем.

В связи с введением классов нам понадобятся еще несколько соглашений для записи формул, а именно:

$$z \in \{x|\ \varphi(x)\} := \varphi(z),$$
$$\{x|\ \varphi(x)\} = \{x|\ \psi(x)\} := \forall x\ \varphi(x) \Leftrightarrow \psi(x),$$
$$A = \{x|\ \varphi(x)\} := \forall x\ x \in A \Leftrightarrow \varphi(x),$$
$$\{x|\ \varphi(x)\} = A := \forall x\ \varphi(x) \Leftrightarrow x \in A,$$

где переменная A не входит в формулу $\varphi(x)$. Эти соглашения позволяют нам распространять стандартные теоретико-множественные отношения $\in$ и $=$ на классы, правда, с некоторыми ограничениями. Так, мы никогда не можем использовать запись $\{x|\ \varphi(x)\} \in X$, поскольку в общем случае класс не является множеством; мы никогда не можем ставить символ класса под квантор или в качестве аргумента формулы, поскольку все эти подстановки возможны лишь для множеств.

Ранее, когда мы использовали во введении терм $\{x|\ \varphi(x)\}$, мы не определяли для него никаких правил, находясь в рамках наивной теории множеств, и считали его как обозначение множества. Однако с появлением аксиом **ZF** нам пришлось отказаться от использования этого терма в общем виде, а пользоваться только его частным случаем $\{x|\ x \in A \wedge \varphi(x)\}$. Теперь же мы вновь намерены использовать это обозначение, но уже не для множеств, а для классов, а приведенные правила, собственно, показывают, что все наши рассуждения, содержащие понятие класса, мы можем без труда формализовать в **ZF**.

Другими словами, классы нам потребовались для упрощения записи утверждений на языке **ZF**, точно так же, как сокращения формул типа $x \subseteq y$ или $x \notin y$. Если, например, у нас имеется достаточно большая формула $\varphi(x) := (x \in A) \wedge (x \in B) \vee (x \in C)$ и т. п., то мы можем определить класс $\mathcal{K} := \{x|\ \varphi(x)\}$, и в дальнейшем вместо этой длинной формулы писать коротко $x \in \mathcal{K}$.

Рассмотрим примеры собственно классов. Пусть $\mathfrak{V} := \{x|\ x = x\}$. Класс $\mathfrak{V}$ — это класс всех множеств, и множеством он быть не может, т. к., предполагая что $\mathfrak{V}$ есть множество, мы придем в противоречие с теоремой 1.3, из которой следует, что $\mathfrak{V} \notin \mathfrak{V}$. Аналогично класс Расселла $\{x|\ x \notin x\}$ не является множеством по той простой причине, что он совпадает с $\mathfrak{V}$ в силу аксиомы регулярности S7. Нетривиальным примером собственно класса является класс всех транзитивных множеств. Пусть $\mathcal{T} := \{x|\ x$ — транзитивно$\}$. Предположим, что $\mathcal{T}$ является множеством. Тогда существует множество

$p = \cup\mathcal{T}$. Покажем, что множество $S(p)$ транзитивно. Действительно, из того, что $x \in S(p)$ следует $x \in p$ или $x = p$. Если $x \in p$, то существует транзитивное множество t такое, что $x \in t$, тогда $x \subseteq t$, откуда $x \subseteq p$ и, следовательно, $x \subseteq S(p)$. Если же $x = p$, то очевидно, что $x \subseteq S(p)$. Итак, $S(p)$ транзитивно, поэтому $S(p) \in \mathcal{T}$ и $S(p) \subseteq p$. Противоречие. Таким образом, $\mathcal{T}$ не является множеством.

Подклассом класса $\mathcal{K}$ называется любой такой класс $\mathcal{L}$, что для каждого множества $x \in \mathcal{L}$ имеем $x \in \mathcal{K}$. Если подкласс $\mathcal{L}$ является множеством, то его мы называем *подмножеством* класса $\mathcal{K}$. Для классов, как и для множеств, мы используем все сокращения для формул, определенные нами во введении, и почти все сокращения для термов, а именно: $\mathcal{K} \cap \mathcal{L}$, $\mathcal{K} \cup \mathcal{L}$, $\mathcal{K} \setminus \mathcal{L}$, $\cup\mathcal{K}$, $\mathrm{Exp}(\mathcal{K})$, причем под классом $\mathrm{Exp}(\mathcal{K})$ мы понимаем класс всех подмножеств класса $\mathcal{K}$.

Понятия последующего класса и пары классов уже некорректны в случае собственно классов, ибо элементами класса могут быть множества и только множества.

На классах мы также можем рассматривать отношения как классы пар множеств, в частности мы можем ввести в рассмотрение прямое произведение классов. Поэтому в дальнейшем (см. главу 2), когда мы будем доказывать, например, вполне упорядочение некоторого класса, мы фактически будем проверять следующие свойства. Пусть $\mathcal{K}$ — класс, и на этом классе задано отношение $\mathcal{R} := \{(x,y) :\ \varphi(x,y)\}$. Тогда отношение $\mathcal{R}$ называется вполне упорядочением, если:

1) $\forall x \in \mathcal{K} : \rceil x\mathcal{R}x$ (антирефлексивность);

2) $\forall x, y, z \in \mathcal{K} :\ x\mathcal{R}y \wedge y\mathcal{R}z \to x\mathcal{R}z$ (транзитивность);

3) $\forall x, y \in \mathcal{K} :\ x = y \vee x\mathcal{R}y \vee y\mathcal{R}x$ (связность);

4) для любого подмножества $A \subseteq \mathcal{K}$, $A \neq \emptyset$, существует такой $x \in A$, что для любого $y \in A$ имеем $x\mathcal{R}y$ или $x = y$.

Аналогичные определения можно привести и для всех остальных видов отношений, какие мы рассматривали в § 1.4.

Под *отображением* $\mathcal{F} : \mathcal{K} \to \mathcal{L}$ класса $\mathcal{K}$ в класс $\mathcal{L}$ мы понимаем класс $\mathcal{F} \subseteq \mathcal{K} \times \mathcal{L}$ такой, что для каждого $x \in \mathcal{K}$ существует $y \in \mathcal{L}$ такой, что $(x,y) \in \mathcal{F}$, и всякий раз из $(x,y), (x,z) \in \mathcal{F}$ следует $y = z$. Понятие отображения — это естественное представление понятий функции и определяемого отображения в терминах теории множеств с классами. Действительно, если формула $\varphi(x,y)$ определяет $(x \mapsto y)$—отображение, то класс $\mathcal{F} = \{(x,y) |\ \varphi(x,y)\}$ является отображением из класса $\mathcal{K} = \{x |\ \exists y\ \varphi(x,y)\}$ в класс $\mathcal{L} = \{y |\ \exists x\ \varphi(x,y)\}$. Если же f есть функция из A в B, то полагая $\mathcal{K} = A$, $\mathcal{L} = B$, $\mathcal{F} = f$, получаем, что $\mathcal{F}$ есть отображение из $\mathcal{K}$ в $\mathcal{L}$.

Для отображения $\mathcal{F}$ формулы $\mathcal{F}(x) = y$ или $y = \mathcal{F}(x)$, как и в случае функции, означают попросту, что $(x, y) \in \mathcal{F}$.

Для отображений так же, как и для функций, вводятся понятия инъективного, сюръективного и биективного отображения, суперпозиции отображений, обратного отображения, образа и прообраза, сужения отображения на подкласс или на подмножество.

Покажем одно фундаментальное свойство, которое мы будем впоследствии неоднократно использовать при доказательстве теорем.

Пусть $\mathcal{K}$ — некоторый класс, Y — множество.

Теорема 1.17. *Если $\mathcal{F}$ есть инъективное отображение класса $\mathcal{K}$ в множество Y, то класс $\mathcal{K}$ есть множество.*

Доказательство. Выделим в множестве Y подмножество Z как область значений $\mathcal{F}$, т. е. положим $Z = \{y \in Y |\ \exists x \in \mathcal{K} : \ \mathcal{F}(x) = y\}$. Тогда отображение $\mathcal{F} : \mathcal{K} \to Z$ биективно и, следовательно, обратимо. Отображение $\mathcal{F}^{-1} : Z \to \mathcal{K}$, обратное к $\mathcal{F}$, сюръективно, откуда в силу аксиомы подстановки S8 получаем, что класс $\mathcal{K}$ есть множество. □

На этом мы завершаем рассмотрение оснований теории множеств. Подведем некоторые итоги наших построений. В этой главе мы попытались построить формальную аксиоматическую теорию множеств, в аксиомах которой мы зафиксировали все основные и вполне очевидные требования к множествам. Придерживаясь строгих правил языка ZF, мы сумели определить в рамках теории множеств практически все основные математические понятия такие, как отношение, функция, отображение, прямое произведение множеств, натуральные числа и прочее. Мы ввели в рассмотрение понятие класса, с помощью которого можно довольно компактно и интуитивно понятно записывать многие громоздкие формулы языка ZF.

Что дает нам такой подход? Во-первых, точность всех выводов теории и отсутствие всех известных парадоксов теории множеств. Во-вторых, объемность теории в том смысле, что в теорию множеств Цермело—Френкеля можно погрузить практически все математические рассуждения. В-третьих, за долгие годы тщательных исследований математикам не удалось обнаружить в ZF ни одного противоречия, что вселяет в нас большую уверенность в непротиворечивости этой теории.

Глава 2

ОРДИНАЛЫ

§ 2.1 Определение и свойства ординалов

Одно из самых часто используемых в теории множеств понятий — это порядок, или, точнее, полный порядок элементов некоторого множества. Представим себе множество некоторых элементов, отвлекаясь от их природы:

$$\underset{0}{\bigcirc}\quad \underset{1}{\bigcirc}\quad \underset{2}{\bigcirc}\quad \underset{3}{\bigcirc}\quad \cdots\quad \underset{n-2}{\bigcirc}\quad \underset{n-1}{\bigcirc}.$$

Натуральные числа, проставленные снизу, отмечают порядковый номер каждого элемента, устанавливая тем самым взаимно однозначное соответствие между натуральным числом n и нашим множеством. Если мы изменим порядок элементов, отвлекаясь опять же от их природы, то после перенумерации вновь получим ту же картину. Действительно, для конечных множеств при перестановке элементов их абстрактный порядок (или порядковый тип) не меняется. Но посмотрим, как обстоит дело с бесконечными множествами. Возьмем, к примеру, последовательность чисел $1 - 1/n$, упорядоченных по возрастанию, т. е. обычным способом, присвоив им в качестве номеров натуральные числа:

$$\underset{0}{\bigcirc}\qquad \underset{1}{\bigcirc}\quad \underset{2}{\bigcirc}\,\underset{3}{\bigcirc}\quad \cdots\quad .$$

Теперь перенесем нулевой элемент в «конец» этого ряда, и после перенумерации с нуля получим

$$\underset{0}{\bigcirc}\qquad \underset{1}{\bigcirc}\quad \underset{2}{\bigcirc}\,\cdots\quad \underset{\omega}{\bigcirc}.$$

Последнему элементу в качестве «номера» мы присвоили ω. Здесь уже имеется последний элемент, хотя количество элементов не изменилось, т. е. между тем и другим множеством можно установить взаимно однозначное соответствие. Чтобы быть более точными, вместо первого примера последовательности $\{1 - 1/n\}_{n=1}^{\infty}$ возьмем множество ω с обычным порядком, а вместо второго примера упорядоченного множества рассмотрим множество $S(\omega) = \omega \cup \{\omega\}$, где отношение принадлежности устанавливает вполне упорядочение, причем ω в этом множестве является наибольшим элементом. Биекцией между этими множествами будет, например,

$$f(n) = \begin{cases} n+1, & n \in \omega, \\ 0, & n = \omega, \end{cases} \qquad f : S(\omega) \leftrightarrow \omega.$$

Продолжая далее процесс «переброски» элементов из «начала» в «конец» в нашем примере, мы будем получать все новые и новые порядковые конструкции или, как мы далее будем говорить, *порядковые типы*.

Эта особенность бесконечных множеств была впервые подмечена Кантором (см. [1]) в его трудах по теории множеств. Тогда он ввел понятие порядкового типа вполне упорядоченного множества как некоего объекта, получаемого путем абстрагирования от природы элементов этого множества. Мы же воспользуемся методом фон Неймана для определения порядковых типов, который заключается в построении специальных полностью упорядоченных множеств, называемых нами ординалами и обладающих весьма привлекательными свойствами, причем для каждого полностью упорядоченного множества найдется и только один ординал, являющийся его порядковым типом.

Определение 2.1. *Ординалом* (или *порядковым числом*) называется всякое множество X, обладающее свойствами:

X транзитивно и любой элемент $x \in X$ транзитивен.

Для обозначения ординалов мы будем использовать, как правило, греческие буквы, поэтому условимся всюду в дальнейшем любую греческую букву, кроме φ и ψ, понимать как обозначение ординала, если не оговорено противное. Через Ord обозначим класс всех ординалов. Рассмотрим теперь основные свойства ординалов.

✓ **2.1.** Пустое множество $\emptyset$ есть ординал.

В дальнейшем, когда $\emptyset$ мы будем использовать как ординал, мы будем называть его нулевым ординалом, обозначая его 0.

✓ **2.2.** Каждый элемент ординала есть ординал.

Доказательство. Пусть $x \in \alpha$. Тогда x транзитивен. В силу транзитивности α получим $x \subseteq \alpha$, откуда и каждый элемент $y \in x$, будучи элементом α, также транзитивен. □

✓ **2.3.** Любое натуральное число $n \in \omega$, а также множество ω являются ординалами, что следует из теоремы 1.12 и предыдущего свойства.

✓ **2.4.** Если α — ненулевой ординал, то $0 \in \alpha$.

Доказательство. Из аксиомы регулярности (S7) следует, что существует $x \in \alpha$ такой, что $x \cap \alpha = \emptyset$. Так как $x \subseteq \alpha$, то $x \cap \alpha = x$, откуда $x = 0$ и, следовательно, $0 \in \alpha$. □

✓ **2.5.** Если α — ординал, то $S(\alpha)$ — ординал.

Доказательство. Пусть $x \in S(\alpha)$, тогда либо $x \in \alpha$, либо $x = \alpha$. В любом случае $x \subseteq \alpha$ в силу транзитивности α. Кроме того, для любого $x \in S(\alpha)$ множество x транзитивно, т. к. $x \in \alpha$ или $x = \alpha$. □

Ранее мы уже использовали принцип индукции для натуральных чисел, т. е. на множестве ω. Теперь мы докажем более общий принцип для всех ординалов.

Теорема 2.1. *Пусть $\varphi(x)$ — формула языка* ZF*. Если для любого α из того, что $\forall\beta \in \alpha : \ \varphi(\beta)$, следует $\varphi(\alpha)$, то тогда для любого α имеем $\varphi(\alpha)$.*

Доказательство. Предположим, существует α такой, что $\rceil\varphi(\alpha)$.

Рассмотрим множество $X = \{\beta \in \alpha |\ \rceil\varphi(\beta)\}$. Если это множество пусто, то $\forall\beta \in \alpha : \ \varphi(\beta)$, откуда $\varphi(\alpha)$. Противоречие.

Пусть $X \neq \emptyset$. Тогда по аксиоме регулярности S7 существует $\beta \in X$ такой, что $\beta \cap X = \emptyset$. Для ординала β верно следующее.

а) $\beta \subseteq \alpha$, т. к. $\beta \in \alpha$ и α транзитивен.

б) для любого $\gamma \in \beta$ имеем $\varphi(\gamma)$, т. к. $\beta \cap X = \emptyset$.

Но тогда по условию теоремы получаем $\varphi(\beta)$. Противоречие. □

Доказанную теорему называют обычно *трансфинитной индукцией* или просто *индукцией*. Индукция используется достаточно часто при доказательстве теоретико-множественных фактов и других теорем, лежащих в основаниях математики.

Замечание 1. Если у нас имеется некоторый непустой класс ординалов $\mathcal{K}$ (т. е. $\mathcal{K} \subseteq \mathrm{Ord}$), а формула φ, указанная в теореме имеет вид $x \in \mathcal{K} \to \psi(x)$, то мы говорим об *индукции на классе* ординалов. В этом случае для проверки условий теоремы, очевидно, достаточно брать ординалы α и β только из класса $\mathcal{K}$. Так мы поступаем, например, при доказательстве теоремы 3.19, используя индукцию на классе бесконечных кардиналов.

Проверка условия теоремы при $\alpha = 0$ (а в случае индукции по классу ординалов $\mathcal{K}$ при $\alpha = \min \mathcal{K}$) обычно осуществляется отдельно и называется базой индукции. Проверим, что условие теоремы при $\alpha = 0$ равносильно формуле $\varphi(0)$. [1] По условию мы имеем $(\forall \beta \in 0: \ \varphi(\beta)) \to \varphi(0)$. Воспользуемся нашими определениями сокращенной записи формул (см. введение), и перепишем условие иначе: $(\forall \beta: \ \ \beta \in 0 \to \varphi(\beta)) \to \varphi(0)$. Импликация $\beta \in 0 \to \varphi(\beta)$ истинна в силу ложности посылки при любом ординале β, поэтому исходная формула равносильна следующей $\psi \to \varphi(0)$, где ψ обозначает какую-либо истинную формулу, например, $\beta \notin \emptyset$. Ну а тогда наша исходная формула равносильна $\varphi(0)$, что вытекает уже из свойств импликации.

Заметим, что индукцию можно проводить не только на классе ординалов, но также на любом его подклассе или подмножестве, а также, в более общем виде, на любом вполне упорядоченном классе, только вместо ординала 0 надо брать минимум этого класса, а вместо ординалов брать исключительно элементы данного класса.

Докажем теперь одно из основных, на наш взгляд, свойств ординалов.

Теорема 2.2. *Класс* Ord *вполне упорядочен отношением принадлежности.*

Доказательство. Антирефлексивность $\in$ следует из аксиомы регулярности, и была уже нами не раз доказана.

Транзитивность $\in$ на ординалах вытекает из транзитивности ординалов.

Для доказательства связности $\in$ на ординалах рассмотрим формулу $\varphi(\alpha, \beta) := \alpha \in \beta \vee \alpha = \beta \vee \beta \in \alpha$.

Нам необходимо показать $\forall \alpha \forall \beta \ \varphi(\alpha, \beta)$. Для этого докажем истинность формулы $\psi(\alpha) := \forall \beta \ \varphi(\alpha, \beta)$ индукцией по α. Предположим, что для любого $\gamma \in \alpha$ истинно $\psi(\gamma)$. Теперь докажем индукцией по β истинность $\varphi(\alpha, \beta)$ (при фиксированном α). Предположим, что $\varphi(\alpha, \gamma)$ при любом $\gamma \in \beta$. Итак, фактически у нас имеется следующее пред-

[1] Часто в книгах по теории множеств (например, [13]) в условие теоремы об индукции добавляют требование $\varphi(0)$, которое, вообще говоря, излишне.

положение: $(\forall\gamma \in \alpha: \ \varphi(\gamma,\beta)) \wedge (\forall\gamma \in \beta: \ \varphi(\alpha,\gamma))$, из которого надо вывести $\varphi(\alpha,\beta)$.

Если $\alpha = \beta$, то все очевидно. Пусть $\alpha \neq \beta$. Тогда $\alpha \setminus \beta \neq \emptyset$ или $\beta \setminus \alpha \neq \emptyset$. Рассмотрим первый вариант. Пусть $\gamma \in \alpha \setminus \beta$. Тогда из предположения получаем: $\varphi(\gamma,\beta)$, т. е. $\gamma \in \beta \vee \gamma = \beta \vee \beta \in \gamma$. Случай $\gamma \in \beta$ исключается по выбору нашего γ. Таким образом, $\gamma = \beta \vee \beta \in \gamma$. Из транзитивности α и того, что $\gamma \in \alpha$, получаем $\beta \in \alpha$, т. е. $\varphi(\alpha,\beta)$.

Рассмотрим второй вариант. Пусть $\gamma \in \beta \setminus \alpha$. Из предположения получаем тогда $\varphi(\alpha,\gamma)$, причем случай $\gamma \in \alpha$ исключается. Поэтому имеем $\alpha \in \gamma \vee \alpha = \gamma$. Так или иначе, из $\gamma \in \beta$ в силу транзитивности β получим $\alpha \in \beta$, т. е. $\varphi(\alpha,\beta)$.

Тем самым мы доказали $\forall\beta\ \varphi(\alpha,\beta)$. Теперь индукцией по α заключаем, что $\forall\alpha\forall\beta\ \varphi(\alpha,\beta)$.

Итак, связность $\in$ на ординалах показана. Осталось показать, что в любом непустом множестве ординалов существует минимум. Пусть B — непустое множество ординалов. По аксиоме регулярности существует $\beta_0 \in B$ такой, что $\beta_0 \cap B = \emptyset$. Тогда для любого $\beta \in B$ получаем либо $\beta_0 = \beta$, либо $\beta_0 \in \beta$, т. к. вариант $\beta \in \beta_0$, очевидно, исключается. Итак, $\beta_0 = \min B$. □

✓ **2.6.** Из только что доказанной теоремы следует, что каждый ординал вполне упорядочен отношением принадлежности.

В дальнейшем, когда мы будем говорить о принадлежности как об отношении порядка на ординалах, вместо символа $\in$ мы будем писать $<$, а формула $\alpha > \beta$ будет равносильна по определению формуле $\beta < \alpha$. Как обычно, рассматриваются и равносильные формулы $\alpha \leqslant \beta$ и $\beta \geqslant \alpha$ нестрогого неравенства. В соответствии с определениями из § 1.4 пара $(\alpha, <)$, где α — ординал, $<$ — отношение принадлежности, называется вполне упорядоченным множеством. Условимся для ординалов вместо пары $(\alpha, <)$ писать просто сам ординал α, относя к нему понятие вполне упорядоченного множества.

✓ **2.7.** $\alpha < \beta \Leftrightarrow \alpha \subset \beta (\alpha \leqslant \beta \Leftrightarrow \alpha \subseteq \beta)$.

Доказательство. Если $\alpha < \beta$, то $\alpha \subset \beta$ в силу транзитивности β.

Пусть $\alpha \subset \beta$. Предположим, что $\rceil(\alpha < \beta)$. Тогда $\beta \leqslant \alpha$, откуда $\beta \subseteq \alpha$ в силу транзитивности α. Противоречие. □

✓ **2.8.** Если A — множество ординалов, то в классе Ord существует $\sup A$ и он равен $\cup A$.

Доказательство. Пусть $x = \cup A$. Множество x есть ординал, т. к. для каждого $z \in x$ существует $\alpha \in A$ такой, что $z \in \alpha$, поэтому, во-первых, z транзитивно, а во-вторых, $z \subseteq \alpha \subseteq x$, откуда x транзитивно.

Покажем, что $x = \sup A$.

а) Для любого $\alpha \in A$ имеем $\alpha \subseteq x$, откуда по свойству 2.7 $\alpha \leqslant x$, т. е. x является верхней гранью для A.

б) Пусть γ — верхняя грань для A. Так как для любого $\alpha \in A$ верно или $\alpha \leqslant \gamma$, то для любого $\alpha \in A$ по свойству 2.7 получим $\alpha \subseteq \gamma$, откуда $x \subseteq \gamma$, т. е. по свойству 2.7 или $x \leqslant \gamma$.

Итак, x — точная верхняя грань A. □

✓ **2.9.** Не существует наибольшего ординала.

Доказательство. Если $\alpha = \max \mathrm{Ord}$, то $S(\alpha) \subseteq \alpha$. Противоречие. □

✓ **2.10.** Класс Ord не является множеством.

Доказательство. Если Ord — множество, то $\cup\,\mathrm{Ord}$ есть ординал по свойству 2.8, причем, очевидно, $\cup\,\mathrm{Ord} = \max \mathrm{Ord}$, что противоречит свойству 2.9. □

Определим два основных типа ординалов.

Определение 2.2. Ординал α называется *последующим*, если существует множество x такое, что $\alpha = S(x)$. В противном случае ординал α называется *предельным*, если только $\alpha > 0$.

Несложно показать, что класс предельных ординалов и класс последующих ординалов не ограничены в Ord, т. е. не являются множествами.

✓ **2.11.** α есть последующий ординал тогда и только тогда, когда $\sup \alpha < \alpha$.

Доказательство. Во-первых, ссылаясь на свойство 2.8, заметим, что для любого ненулевого ординала α

$$\sup \alpha = \cup \alpha = \bigcup_{x \in \alpha} x,$$

причем $\sup \alpha$ есть ординал.

Во-вторых, покажем, что утверждение $\alpha < \sup \alpha$ ложно при любом ненулевом ординале α. Пользуясь свойством 2.7, получим

$$\sup \alpha = \bigcup_{x \in \alpha} x \subseteq \bigcup_{x \subset \alpha} x \subseteq \alpha. \tag{2.1}$$

Итак, пусть α есть последующий ординал. Тогда существует ординал β, такой, что $\alpha = S(\beta)$.

Тогда $\sup\alpha = \cup\alpha = (\cup\beta) \cup \beta = \beta$ по (2.1). Следовательно, $\sup\alpha < \alpha$.

Обратно, пусть $\sup\alpha < \alpha$. Рассмотрим ординал $S(\sup\alpha)$. Имеем

$$S(\sup\alpha) = (\cup\alpha) \cup \{\cup\alpha\} \subseteq \alpha \tag{2.2}$$

по неравенству (2.1) и по предположению.

По определению $\sup\alpha$ для любого $\beta < \alpha$: $\beta < (\sup\alpha) \cup \{\sup\alpha\} = S(\sup\alpha)$.

Поэтому

$$\alpha \subseteq S(\sup\alpha). \tag{2.3}$$

Окончательно из (2.2) и (2.3) имеем $\alpha = S(\sup\alpha)$, то есть α — последующий ординал. □

Из доказательства этого свойства вытекают следующие два критерия последующего и предельного ординалов.

✓ **2.12.** α есть последующий ординал тогда и только тогда, когда $\alpha = S(\sup\alpha)$; α есть предельный ординал тогда и только тогда, когда $\alpha = \sup\alpha$.

§ 2.2 Рекурсивные определения. Порядковые типы

Одна из часто встречающихся в математике конструкций — рекурсия. Например, выбрав определенным образом вещественную функцию f и число a, мы можем рассматривать последовательность $\{x_n\}_{n=0}^{\infty}$, определяемую равенствами: $x_0 = a$, $x_{n+1} = f(x_n)$, $n \in \omega$. Последнее равенство принято называть рекурсивным. Вообще, всякая рекурсия подразумевает построение последовательности путем указания зависимости элементов данной последовательности от элементов с меньшими номерами. При этом (в общем случае) «номера» не обязаны быть исключительно натуральными числами, они могут быть и бесконечными ординалами.

Пусть $\mathcal{K}$ — класс, в котором мы хотим построить (рекурсивно) некоторую трансфинитную последовательность (т. е. отображение из Ord в $\mathcal{K}$). Пусть также задано отображение $\mathcal{F} : \mathrm{Exp}(\mathcal{K}) \to \mathcal{K}$. При помощи этого отображения мы и определим переход в рекурсии от элементов с номерами меньше α, где α — ординал, к элементу с номером α следующим образом:

$$x_\alpha = \mathcal{F}(\{x_\beta | \ \beta < \alpha\}), \quad x_0 = \mathcal{F}(\emptyset).$$

Корректно ли такое определение? Ответ на этот вопрос дает следующая

Теорема 2.3. (О рекурсивных определениях).
Пусть $\mathcal{K}$ есть класс и задано отображение $\mathcal{F} : \operatorname{Exp}(\mathcal{K}) \to \mathcal{K}$. Тогда можно определить отображение $\mathcal{G} : \mathrm{Ord} \to \mathcal{K}$ такое, что

$$\forall \Delta \in \mathrm{Ord}: \ \mathcal{G}(\Delta) = \mathcal{F}\Big(\{\mathcal{G}(\delta) | \ \delta < \Delta\}\Big). \tag{2.4}$$

Доказательство. Для того, чтобы доказать теорему, нам необходимо сконструировать такую формулу φ, которая определяла бы отображение из Ord в $\mathcal{K}$, удовлетворяющее (2.4). Для этого мы сначала рассмотрим формулу

$$\psi(h) := \exists \alpha \in \mathrm{Ord}: \ (h : \alpha \to \mathcal{K}) \wedge \forall \beta < \alpha: \ h(\beta) = \mathcal{F}(h\beta).$$

Заметим, что всякое отображение $h : \alpha \to \mathcal{K}$ является функцией по аксиоме подстановки, поэтому формула ψ построена корректно. Полагая далее $\mathcal{H} = \{h | \ \psi(h)\}$, мы видим, что класс $\mathcal{H}$ не пуст, т. к., например, функция $h = \{(0, \mathcal{F}(\emptyset))\}$ является элементом $\mathcal{H}$. Более того, класс $\mathcal{H}$ линейно упорядочен отношением $\subset$. Действительно, пусть $h, h' \in \mathcal{H}$ и $\alpha = dom\,(h)$, $\alpha' = dom\,(h')$. Для определенности положим, что $\alpha \leqslant \alpha'$. Легко установить (по индукции), что $h'|_\alpha = h$, откуда следует $h \subseteq h'$.

Обозначим далее $\mathcal{G} = \cup\mathcal{H}$. Поскольку класс $\mathcal{H}$ линейно упорядочен отношением $\subset$ и состоит из функций, то $\mathcal{G}$ является отображением. Заметим также, что отображение $\mathcal{G}$ определено для всех ординалов. Именно, если предположить, что α — наименьший из ординалов, для которых $\mathcal{G}$ не определено, то $h = \mathcal{G} \in \mathcal{H}$. Полагая далее $h' = h \cup \{(\alpha, \mathcal{F}(h\alpha))\}$, замечаем, что $h' \in \mathcal{H}$, ибо h' удовлетворяет формуле ψ. Таким образом, $\mathcal{G} \subset h'$. Противоречие.

Теперь определим формулу $\varphi(\alpha, x)$ так:

$$\varphi(\alpha, x) := \exists h \in \mathcal{H}: \ h(\alpha) = x.$$

Нетрудно проверить, что $\mathcal{G} = \{(\alpha, x) | \ \varphi(\alpha, x)\}$. Итак, формула $\varphi(\alpha, x)$ определяет отображение $\mathcal{G} : \mathrm{Ord} \to \mathcal{K}$, причем для каждого ординала α имеем $\mathcal{G}(\alpha) = \mathcal{F}(\mathcal{G}\alpha)$, поскольку для каждого α существует функция $h \in \mathcal{H}$ такая, что $\mathcal{G}|_{S(\alpha)} = h$ и $h(\alpha) = \mathcal{F}(h\alpha)$. $\square$

Теперь мы видим, что наш пример с вещественной последовательностью $\{x_n\}$, приведенный в начале параграфа, есть частный случай трансфинитной рекурсии. Действительно, рассмотрим класс $\mathcal{K} = \mathbb{R} \times \omega$. Построим $\mathcal{F} : \mathrm{Exp}(\mathcal{K}) \to \mathcal{K}$ так: для каждого подмножества $A \subseteq \mathbb{R} \times \omega$, являющегося функцией $A : S(n) \to \mathbb{R}$ при некотором $n \in \omega$, положим $\mathcal{F}(A) = (f(A(n)), S(n))$, для всех прочих $A \subseteq \mathbb{R} \times \omega$ положим $\mathcal{F}(A) = (a, 0)$. Здесь функция f и число a те, которые были упомянуты в начале параграфа. Теперь нетрудно проверить, что отображение $\mathcal{G} : \mathrm{Ord} \to \mathcal{K}$, существование которого доказано в теореме, обладает следующими свойствами:

$$\mathcal{G}(n) = (x_n, n) \text{ при } n < \omega, \quad \mathcal{G}(\alpha) = (a, 0) \text{ при } \alpha \geqslant \omega.$$

Построение рекурсивных определений (точнее, рекурсивно определяемых отображений) — одна из самых часто возникающих задач не только в теории множеств, но также в арифметике, топологии и т. д. Чаще всего эту теорему применяют ко множествам, т. е. в случае, когда класс $\mathcal{K}$ является множеством, но иногда (см., например, главу 3, теорему 3.8, где $\mathcal{K} = \mathrm{Card}_\omega$) приходится использовать и более общий ее вариант, который был только что доказан. В текущей главе мы еще неоднократно возвратимся к данной теореме.

Определение 2.3. Пусть $(X, <_X)$ — вполне упорядоченное множество. Если между X и некоторым ординалом Δ существует порядковый изоморфизм, т. е. такая биекция $f : \Delta \to X$, что при любых $\alpha < \beta < \Delta$ имеем $f(\alpha) <_X f(\beta)$, то ординал Δ называется *порядковым типом* $(X, <_X)$, и для него в этом случае используется обозначение $|(X, <_X)|$ или $\mathrm{Ord}(X, <_X)$.

Поскольку $\emptyset \times \emptyset = \emptyset$, то любое отношение на $\emptyset$ совпадает с $\emptyset$. Поэтому по определению также положим $|(\emptyset, \emptyset)| = 0$.

Теорема 2.4. *Любое вполне упорядоченное множество имеет единственный порядковый тип.*

Доказательство. Пусть непустое множество X вполне упорядочено отношением $<_X$. Построим функцию $F : \mathrm{Exp}(X) \to X$ по следующему правилу: для любого собственного подмножества $A \subset X$ положим $F(A) = \min X \setminus A$, в случае $A = X$ положим $F(A) = \min X$.

По теореме о рекурсивных определениях существует отображение $\mathcal{G}$ из Ord в X такое, что $\mathcal{G}(\alpha) = F(\mathcal{G}\alpha)$ при любом $\alpha \in \mathrm{Ord}$.[2]

[2]Напомним, что символ $\mathcal{G}\alpha$ обозначает образ ординала α относительно отображения $\mathcal{G}$.

I *Покажем существование порядкового типа X.*

Пусть $\alpha \in \mathrm{Ord}$ и $\mathcal{G}\alpha \subset X$. Пусть также $\beta < \alpha$.

Ia) Покажем, что в этом случае $\mathcal{G}(\beta) < \mathcal{G}(\alpha)$.

Действительно, $\mathcal{G}\beta \subseteq \mathcal{G}\alpha$, откуда $X \setminus \mathcal{G}\alpha \subseteq X \setminus \mathcal{G}\beta$, откуда $\mathcal{G}(\beta) \leqslant \mathcal{G}(\alpha)$, а поскольку $\mathcal{G}(\beta) \in \mathcal{G}\alpha$, то $\mathcal{G}(\beta) \neq \mathcal{G}(\alpha)$, откуда $\mathcal{G}(\beta) < \mathcal{G}(\alpha)$.

Iб) Покажем, что существует ординал Δ такой, что $\mathcal{G}\Delta = X$.

В самом деле, если предположить, что это не верно, то из Ia) следует, что $\mathcal{G}$ есть инъективное отображение из Ord в X, откуда по теореме 1.17 получаем, что Ord будет множеством. Противоречие.

Через Δ обозначим наименьший из таких ординалов.

Iв) Покажем, что $\mathcal{G}$ действует инъективно с Δ в X.

Действительно, по определению Δ при любом $\alpha < \Delta$ имеем $\mathcal{G}\alpha \subset X$, откуда в силу Ia) для любых $\beta < \alpha < \Delta$ получим $\mathcal{G}(\beta) < \mathcal{G}(\alpha)$, т. е. $\mathcal{G}|_\Delta$ — инъекция.

Iг) Из Ia), Iб) и Iв) следует, что $\mathcal{G}|_\Delta$ осуществляет порядковый изоморфизм ординала Δ и множества X. Итак, $\Delta = |(X, <_X)|$.

II *Покажем, что порядковый тип вполне упорядоченного множества определяется единственным образом.*

Пусть ординалы $\Delta \leqslant \Gamma$ являются порядковыми типами $(X, <_X)$. Легко показать, что в этом случае существует порядковый изоморфизм $f : \Delta \to \Gamma$.

Предположим, что f не является тождественной функцией, и через α обозначим наименьший из таких ординалов, для которых $f(\alpha) \neq \alpha$. Если предположить, что $f(\alpha) < \alpha$, то существует $\delta < \alpha$ такое, что $f(\delta) = f(\alpha)$, что нарушает инъективность f. Итак, $f(\alpha) > \alpha$. Тогда для любого $\delta < \alpha$ имеем $f(\delta) < \alpha$, а для любого $\delta \geqslant \alpha$, $\delta \in \Delta$, получим $f(\delta) > \alpha$.

Итак, $\alpha \notin f\Delta = \Gamma$, что противоречит тому, что $\alpha < \Delta < \Gamma$, т. е. $\alpha \in \Gamma$. Следовательно, f есть тождественное отображение, откуда $\Delta = \Gamma$, и теорема доказана. □

О фундированности классов.

В § 1.7 нами было введено понятие класса как определяемой совокупности множеств. Классами, например, являются $\mathfrak{V}$ (класс всех множеств) и Ord (класс всех ординалов). Отметим, что аксиома регулярности (фундирования) S7, которая наводит достаточно строгий порядок на множествах, была нами сформулирована для множеств. Поэтому возникает вопрос: насколько справедливо подобное утверждение для классов, упорядочены ли они столь же строго как множества?

Ответ на этот вопрос содержится в следующей теореме.

Теорема 2.5. *Если* $\mathcal{K}$ *— непустой класс, то существует множество* $X \in \mathcal{K}$ *такое, что* $X \cap \mathcal{K} = \emptyset$.

Доказательство. Пусть $\mathcal{K}$ — непустой класс. Предположим, что для любого $X \in \mathcal{K}$ имеем $X \cap \mathcal{K} \neq \emptyset$. Для доказательства теоремы построим специальную последовательность множеств, которая сведет фундированность классов к фундированности множеств.

Так как $\mathcal{K} \neq \emptyset$, то существует $A_0 \in \mathcal{K}$, тогда множество $A_0 \cap \mathcal{K}$ непусто. Построим отображение $\mathcal{F}$ из класса $\mathrm{Exp}(\mathrm{Exp}(\mathcal{K}))$ в класс $\mathrm{Exp}(\mathcal{K})$ по правилу: для любого непустого множества $A \subseteq \mathrm{Exp}(\mathcal{K})$ положим

$$\mathcal{F}(A) = \bigcup_{a \in A} \bigcup_{x \in a} (x \cap \mathcal{K}),$$

для пустого множества: $\mathcal{F}(\emptyset) = A_0 \cap \mathcal{K}$.

По теореме о рекурсивных определениях существует отображение $\mathcal{G} : \mathrm{Ord} \to \mathrm{Exp}(\mathcal{K})$ такое, что для каждого ординала α имеем $\mathcal{G}(\alpha) = \mathcal{F}(\mathcal{G}\alpha)$. В силу нашего предположения о нефундированности класса $\mathcal{K}$ легко показать, что при любом $\alpha \in \mathrm{Ord}$ множество $\mathcal{G}(\alpha)$ непусто.

Рассмотрим сужение отображения $\mathcal{G}$ на множество ω. По аксиоме подстановки класс $\{\mathcal{G}(n) |\ n \in \omega\}$ есть множество. Обозначим через X_n множество $\mathcal{G}(n)$ при каждом $n \in \omega$. Тогда $X = \bigcup\limits_{n \in \omega} X_n$ есть множество по аксиоме объединения, кроме того, $X \subseteq \mathcal{K}$.

Для произвольно выбранного $x \in X$ существует n такое, что $x \in X_n$. По нашему предположению $x \cap \mathcal{K} \neq \emptyset$. Кроме того, легко проверить, что $x \cap \mathcal{K} \subseteq X_{n+1}$, т. е. $x \cap \mathcal{K} \subseteq X$, откуда $x \cap \mathcal{K} \subseteq x \cap X$, откуда $x \cap X \neq \emptyset$. Получено противоречие с аксиомой регулярности для множества X. □

§ 2.3 Арифметика ординалов

Когда мы даем определение некоторому объекту (множеству), называя его *числом*, то это накладывает определенные обязательства, ибо над числами принято осуществлять как минимум две операции: сложение и умножение. Следуя данной традиции, мы вводим вспомогательный инструментарий на классе ординалов, который будет рассмотрен в данном параграфе и который, опять же по традиции, будет назван *арифметикой ординалов*.

Пусть у нас имеется ненулевой ординал Δ, индексирующий множество ординалов $\{\alpha_\delta\}_{\delta\in\Delta}$. На всех ординалах мы рассматриваем одно и то же отношение полного упорядочения — отношение принадлежности. Тогда мы можем определить каноническую сумму ординалов α_δ по ординалу Δ так, как мы определяли каноническую сумму вполне упорядоченных множеств по вполне упорядоченному множеству в § 1.6. Из теоремы 1.14 вытекает, что каноническая сумма ординалов α_δ по ординалу Δ есть вполне упорядоченное множество. А это означает, что у канонической суммы ординалов существует единственный порядковый тип, который тоже является ординалом.

Определение 2.4. *Суммой ординалов* α_δ *в порядке* Δ называется порядковый тип их канонической суммы по ординалу Δ. Сумма ординалов α_δ в порядке Δ обозначается символом $\sum\limits_{\delta\in\Delta}\alpha_\delta$.

В том случае, когда ординал Δ является натуральным числом или ординалом ω, для обозначения суммы ординалов мы допускаем использование стандартных математических символов, например,

$$\alpha_0+\alpha_1+\dots+\alpha_n, \qquad \sum_{n=0}^{\infty}\alpha_n.$$

Для наглядного представления суммы ординалов можно воспользоваться картинкой:

$$[\circ\ \ \circ\ \ \underset{\alpha_0}{\circ}\ \dots)[\circ\ \ \circ\ \ \underset{\alpha_1}{\circ}\ \dots)[\circ\ \ \circ\ \ \underset{\alpha_2}{\circ}\ \dots)\dots$$

При сложении ординалы выстраиваются «друг за другом» и образуют новый порядковый тип. Нетрудно проверить, что в случае, когда α_0 и α_1 являются натуральными числами, их сумма, как сумма ординалов, совпадает с обычной суммой натуральных чисел.

Перейдем к определению произведения ординалов. Рассмотрим множество ординалов $\{\alpha_\delta\}_{\delta\in\Delta}$. Поскольку все ординалы вполне упорядочены, то мы можем определить каноническое произведение ординалов α_δ по ординалу Δ. В соответствии с теоремой 1.15 это произведение будет линейно упорядоченным множеством. Для его вполне упорядоченности приходится предполагать, что ординал Δ есть натуральное число. Поэтому положим далее $\Delta = n$. Тогда по теореме 1.16 каноническое произведение ординалов α_δ по ординалу n будет вполне упорядоченным множеством, для которого существует единственный порядковый тип, являющийся ординалом.

Определение 2.5. *Произведением ординалов* α_δ *в порядке* n называется порядковый тип их канонического произведения по ординалу n. Произведение ординалов α_δ в порядке n обозначается символом $\prod\limits_{\delta\in n}\alpha_\delta$, либо одним из следующих стандартных символов:

$$\prod_{i=0}^{n-1}\alpha_i, \qquad \alpha_0\alpha_1\ldots\alpha_{n-1}.$$

Здесь мы определили пока только конечное произведение ординалов. В дальнейшем мы определим и бесконечные произведения, пользуясь теоремой о рекурсивных определениях.

Произведение двух ординалов $\alpha_0\alpha_1$ (при $n=2$) можно представить так:

$$\underbrace{\Big[\;[\quad\alpha_1\quad)[\quad\alpha_1\quad)[\quad\alpha_1\quad)\quad\ldots\quad\Big)}_{\alpha_0}$$

При произведении ординалов α_0 и α_1 ординал α_1 последовательно повторяется в том порядке, который диктует ординал α_0. Если α_0 и α_1 есть натуральные числа, то их произведение совпадает с обычным произведением натуральных чисел.

Без доказательства приведем простейшие свойства суммы и конечного произведения ординалов.[3]

✓ **2.13.** Сложение вообще говоря не коммутативно, т. к., например, $\omega+1=S(\omega)$, а $1+\omega=\omega$.

✓ **2.14.** Сложение ассоциативно: $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$.

✓ **2.15.** Нулевой ординал есть нейтральный элемент по сложению: $\alpha+0=0+\alpha=\alpha$.

✓ **2.16.** Действует закон сокращения слева: если $\alpha+\beta=\alpha+\gamma$, то $\beta=\gamma$.

✓ **2.17.** Закон сокращения справа не действует. Например, $1+\omega=2+\omega$, но $1\neq 2$.

✓ **2.18.** Произведение ординалов вообще говоря не коммутативно. Так, например, $\omega\cdot 2=\omega$, но $2\cdot\omega\neq\omega$.

[3]Заметим, что для формальной проверки равенства порядковых типов двух множеств, на которой основаны доказательства этих свойств, достаточно установить порядковый изоморфизм между этими множествами, который как правило очевиден из структуры множества, определяющего результат сложения или умножения ординалов, интуитивно же эти свойства легко установить, пользуясь графическим представлением суммы и произведения,.

✓ **2.19.** Произведение ассоциативно: $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

✓ **2.20.** 1 есть нейтральный элемент по умножению: $1 \cdot \alpha = \alpha \cdot 1 = \alpha$.

✓ **2.21.** Действует правый дистрибутивный закон: $(\alpha+\beta)\gamma = \alpha\gamma+\beta\gamma$.

✓ **2.22.** Левый дистрибутивный закон не действует. Так, например, $2(\omega+1) = (\omega+1)+(\omega+1) = (\omega+(1+\omega))+1 = (\omega+\omega)+1$, но $2\omega+2 = (\omega+\omega)+2$.

✓ **2.23.** Монотонность: если $\alpha > 0$, то $\beta \leqslant \alpha\beta$ и $\beta \leqslant \beta\alpha$.

✓ **2.24.** Правая дистрибутивность в общем виде:

$$\left(\sum_{\delta\in\Delta} \alpha_\delta\right)\beta = \sum_{\delta\in\Delta}(\alpha_\delta\beta).$$

Если в этом равенстве положить $\alpha_\delta = 1$ при любом $\delta \in \Delta$, то легко доказать следующее утверждение.

Если для любого $\delta \in \Delta$ имеем $\alpha_\delta = \beta$, то $\sum\limits_{\delta\in\Delta} \alpha_\delta = \Delta \cdot \beta$.

Для определения произвольного произведения ординалов нам потребуется теорема о рекурсивных определениях 2.3 и, кроме того, несколько новых обозначений. Во-первых, через Ord_1 обозначим класс ненулевых ординалов. Во-вторых, для каждой упорядоченной пары (a, b) через $\mathrm{co}_1(a, b)$ будем обозначать левую ее координату, а через $\mathrm{co}_2(a, b)$ обозначим правую ее координату. Наконец в-третьих, для всякого подмножества B в прямом произведении классов $\mathcal{K} \times \mathcal{L}$ через $\pi_1 B$ обозначим множество $\{\mathrm{co}_1\, s|\ s \in B\}$, а через $\pi_2 B$ обозначим множество $\{\mathrm{co}_2\, s|\ s \in B\}$. $\pi_1 B$ и $\pi_2 B$ называются соответственно *левой* и *правой проекциями* множества B.

Теорема 2.6. *Для любого отображения* $\mathcal{I} : \mathrm{Ord} \to \mathrm{Ord}_1$ *существует отображение* $\mathcal{P} : \mathrm{Ord} \to \mathrm{Ord}_1$ *такое, что:*

1) $\mathcal{P}(0) = 1$;

2) $\mathcal{P}(\alpha+1) = \mathcal{P}(\alpha) \cdot \mathcal{I}(\alpha)$;

3) *если* α *— предельный, то* $\mathcal{P}(\alpha) = \sup\limits_{\gamma<\alpha} \mathcal{P}(\gamma)$.

Доказательство. Построим отображение $\mathcal{F} : \mathrm{Exp}(\mathrm{Ord}_1 \times \mathrm{Ord}_1) \to \mathrm{Ord}_1 \times \mathrm{Ord}_1$ по правилу: для множества $B \subseteq \mathrm{Ord}_1 \times \mathrm{Ord}_1$ положим:

$$\mathcal{F}(B) = \begin{cases} (1, 0), & B = \emptyset; \\ (\sup \pi_1 B, \sup \pi_2 B), & \sup \pi_2 B \notin \pi_2 B; \\ (\sup \pi_1 B \cdot \mathcal{I}(\sup \pi_2 B), \sup \pi_2 B + 1), & \sup \pi_2 B \in \pi_2 B. \end{cases}$$

Тогда по теореме о рекурсивных определениях существует отображение $\mathcal{G}$ из Ord в $\mathrm{Ord}_1 \times \mathrm{Ord}_1$ такое, что

$$\mathcal{G}(\alpha) = \mathcal{F}(\mathcal{G}\alpha), \quad \alpha \in \mathrm{Ord}\,.$$

Теперь введем отображение $\mathcal{P} : \mathrm{Ord} \to \mathrm{Ord}_1$ по правилу:

$$\forall \alpha \in \mathrm{Ord} :\ \mathcal{P}(\alpha) = \mathrm{co}_1\, \mathcal{G}(\alpha).$$

а) Из определения отображения $\mathcal{F}$ видно, что если определен $\sup \pi_2 B$, то $\mathrm{co}_1\, \mathcal{F}(B) \geqslant \sup \pi_1 B$. Пусть $\alpha < \beta$. Так как $\mathcal{G}(\alpha) \in \mathcal{G}\beta$, то $\sup \pi_1 \mathcal{G}\beta \geqslant \mathrm{co}_1\, \mathcal{G}(\alpha)$, откуда $\mathrm{co}_1\, \mathcal{G}(\beta) = \mathrm{co}_1\, \mathcal{F}(\mathcal{G}\beta) \geqslant \mathrm{co}_1\, \mathcal{G}(\alpha)$, т. е. отображение $\mathcal{P}$ монотонно возрастает.

б) Покажем индукцией, что при любом $\alpha \in \mathrm{Ord}$ имеем $\mathrm{co}_2\, \mathcal{G}(\alpha) = \alpha$. Предположим, что оно верно при любом $\beta < \alpha$.

Тогда $\pi_2 \mathcal{G}\alpha = \alpha$. Из определения $\mathcal{F}$ видно, что если $\sup \alpha \in \alpha$, то $\mathrm{co}_2\, \mathcal{F}(\mathcal{G}\alpha) = \sup \alpha + 1 = \alpha$, если же $\sup \alpha \notin \alpha$, то $\sup \alpha = \alpha$ и $\mathrm{co}_2\, \mathcal{F}(\mathcal{G}\alpha) = \sup \alpha = \alpha$. Здесь было использовано свойство 2.12 ординалов из § 2.1.

в) Докажем индукцией, что отображение $\mathcal{P}$ и есть искомое. Действительно, $\mathcal{G}(0) = \mathcal{F}(\emptyset) = (1, 0)$, т. е. $\mathcal{P}(0) = 1$. Пусть при любом $\gamma < \alpha$ отображение $\mathcal{P}$ удовлетворяет выводу теоремы. Покажем, что $\mathcal{P}$ будет искомым и для α.

Пусть $\alpha = \beta + 1$. Тогда в силу монотонности $\mathcal{P}$ получим $\sup \pi_1 \mathcal{G}\alpha = \mathcal{P}(\beta)$. В силу пункта б) $\pi_2 \mathcal{G}\alpha = \alpha$ и, следовательно, $\sup \pi_2 \mathcal{G}\alpha = \beta \in \pi_2 \mathcal{G}\alpha$. Тогда по определению отображения $\mathcal{F}$ получим $\mathcal{P}(\alpha) = \mathcal{P}(\beta) \cdot \mathcal{I}(\beta)$.

Пусть α — предельный ординал. Снова в силу монотонности $\mathcal{P}$ получим $\sup \pi_1 \mathcal{G}\alpha = \sup\limits_{\gamma < \alpha} \mathcal{P}(\gamma)$. Из б) следует, что $\pi_2 \mathcal{G}\alpha = \alpha$ и $\sup \pi_2 \mathcal{G}\alpha = \alpha \notin \pi_2 \mathcal{G}\alpha$. Тогда из определения $\mathcal{F}$ заключаем, что $\mathcal{P}(\alpha) = \sup\limits_{\gamma < \alpha} \mathcal{P}(\gamma)$.

Итак, $\mathcal{P}$ является искомым отображением. Теорема доказана. ☐

Определение 2.6. Отображение $\mathcal{P}$, зависящее от отображения $\mathcal{I}$ и существование которого только что было доказано, называется *продукционным отображением с порядком* $\mathcal{I}$.

Продукционное отображение служит для построения произведений ординалов.

Определение 2.7. Пусть есть множество ординалов A, проиндексированное ординалом Δ и функция I есть индексация. Если $0 \in A$, то 0 называется *произведением ординалов из A в порядке I*.

Если $0 \notin A$, то продолжим индексирующую функцию I (она действует сюръективно из Δ на A) до какого-либо отображения $\mathcal{I}$ из Ord в Ord_1 (например, положим $\mathcal{I}(\alpha) = 1$ при $\alpha \geqslant \Delta$). И пусть $\mathcal{P}$ обозначает продукционное отображение с порядком $\mathcal{I}$. Тогда ординал $\mathcal{P}(\Delta)$ называется *произведением ординалов из A в порядке* Δ.

В том и другом случае произведение обозначается

$$\prod_{\delta \in \Delta} I(\delta).$$

Произведение ненулевых элементов ординала $S(\Delta)$ в естественном порядке (т. е. в качестве индексирующего множества берется порядковый тип множества ненулевых ординалов из $S(\Delta)$, которым является сам ординал $S(\Delta)$ при $\Delta \geqslant \omega$, и n при $\Delta = n$) называют *факториалом* ординала Δ и обозначают $\Delta!$, т. е.

$$\Delta! = \prod_{\delta \in S(\Delta) \setminus \{0\}} \delta.$$

Легко проверить, что данное понятие факториала для натурального числа совпадает с обычным понятием факториала.

Замечание 2. В случае, когда $\Delta = 0$, т. е. множество A пусто и проиндексировано нулевым ординалом, по определению получим $\prod\limits_{\delta \in \Delta} I(\delta) = \mathcal{P}(0) = 1$.

Более наглядные правила для подсчета произведения ординалов таковы:

- произведение нуля сомножителей есть 1;
- если известно произведение α сомножителей, то умножив его на $(\alpha+1)$-й сомножитель, получим произведение $(\alpha+1)$-го сомножителя;
- если ординал α — предельный и известны произведения β сомножителей для каждого $\beta < \alpha$, то супремум этих произведений и есть произведение α сомножителей.

§ 2.4 Аксиома выбора

Аксиома выбора, о которой здесь пойдет речь, появилась в связи с одной не вполне очевидной проблемой. Представим себе, что у нас имеется несколько непустых множеств $X_1, \ldots, X_n$, и из каждого из этих множеств необходимо выбрать по одному элементу $x_1, \ldots, x_n$ ($x_i \in X_i$), образовав при этом новое множество $C = \{x_1, \ldots, x_n\}$, которое называется *сечением* множества множеств $\{X_1, \ldots, X_n\}$. Такой выбор, казалось бы, не представляет сложности. Но что если имеется *бесконечный* набор исходных множеств? Как построить функцию, которая каждому из этих множеств ставила бы в соответствие его собственный элемент? Как оказалось, это сделать невозможно, если мы находимся в рамках аксиом ZF! Сформулируем теперь *аксиому выбора* (AC):

> *Для любого множества X, если множество $\cup X$ не пусто, существует функция $f : X \to \cup X$ такая, что при любом $x \in X$ если $x \neq \emptyset$, то $f(x) \in x$, при этом f называют функцией выбора для множества X.*

На вопрос о том, почему AC называют именно аксиомой, отвечают следующие теоремы метаматематики.

Теорема 2.7. (Курт Гёдель, 1936). *Невозможно опровергнуть аксиому выбора (в символах:* $\mathrm{Con}(\mathsf{ZF}) \to \mathrm{Con}(\mathsf{ZF}+\mathsf{AC})$).

Теорема 2.8. (Поль Ко́эн, 1963). *Невозможно доказать аксиому выбора (в символах:* $\mathrm{Con}(\mathsf{ZF}) \to \mathrm{Con}(\mathsf{ZF}+\rceil\mathsf{AC})$).

Здесь символ Con обозначает совместность (непротиворечивость) аксиоматики, указанной в скобках, а выражение ZF+AC обозначает аксиоматику, полученную добавлением аксиомы выбора AC к аксиомам ZF, соответственно, ZF+$\rceil$AC обозначает аксиоматику, полученную добавлением отрицания аксиомы выбора к аксиомам ZF.

Таким образом, аксиома выбора не зависит от остальных аксиом теории множеств, и может быть принята как еще одна аксиома нашей теории. Но поскольку она встречает неодобрение многих математиков (в особенности с появлением в последнее время не менее привлекательной аксиомы детерминированности AD, противоречащей AC), мы не будем рассматривать ее как еще одну аксиому ZF, а для теории ZF+AC введем специальное обозначение ZFC. Следуя Куратовскому [9], все утверждения, которые мы будем доказывать в рамках теории ZFC, мы будем отмечать знаком $^\circ$, выставляя его перед ключевым словом утверждения, например, $^\circ$Теорема.

Кроме аксиомы выбора иногда используют разные ее частные случаи. Так, например, *аксиома счетного выбора* AC_ω гарантирует существование функции выбора $f : X \to \cup X$ лишь для счетных множеств X (т. е. таких множеств X, что $X \leftrightarrow \omega$, см. стр. 19). Эта аксиома хороша тем, что она выводима как из AC, так и из AD, и с ее помощью нельзя получить все те «парадоксальные» выводы, которые дает обычная аксиома выбора (некоторые из этих выводов мы рассмотрим в конце данного параграфа), но тем не менее можно получить большинство теорем анализа.[4]

Как оказалось, существует много эквивалентных аксиоме выбора весьма ценных утверждений (см. [9]). Здесь мы приведем только два, ибо они понадобятся нам в дальнейшем. Это теорема Цермело о полном упорядочении и лемма Цорна.

Теорема 2.9. *Следующие утверждения эквивалентны в рамках теории* ZF:

1) AC (*аксиома выбора*);

2) ZT (*теорема Цермело*)*: каждое непустое множество может быть вполне упорядочено;*

3) ZL (*лемма Цорна*)*: в любом частично упорядоченном непустом множестве, если любая его цепь ограничена, имеется максимальный элемент.*

Доказательство. Покажем, что $\mathsf{AC} \to \mathsf{ZT} \to \mathsf{ZL} \to \mathsf{AC}$.

I *Покажем, что из аксиомы выбора вытекает теорема Цермело.*

Пусть X — непустое множество, f — функция выбора на множестве $\mathrm{Exp}(X)$, а функция $F : \mathrm{Exp}(X) \to X$ действует по следующему правилу: для каждого $A \subseteq X$ $F(A) = f(X \setminus A)$.

Из теоремы о рекурсивных определениях (см. теорему 2.3) следует, что существует отображение $\mathcal{G} : \mathrm{Ord} \to X$ такое, что при любом ординале α $\mathcal{G}(\alpha) = F(\mathcal{G}\alpha)$.

Iа) Пусть $\mathcal{G}\beta \subset X$ (собственное подмножество) при некотором ординале β и ординал $\alpha < \beta$. Покажем, что в этом случае $\mathcal{G}(\alpha) \neq \mathcal{G}(\beta)$.

Действительно, $\mathcal{G}(\beta) = F(\mathcal{G}\beta) = f(X \setminus \mathcal{G}\beta)$ и множество $X \setminus \mathcal{G}\beta$ не пусто, поэтому $\mathcal{G}(\beta) \notin \mathcal{G}\beta$. С другой стороны, как легко видеть, $\mathcal{G}(\alpha) \in \mathcal{G}\beta$, откуда $\mathcal{G}(\alpha) \neq \mathcal{G}(\beta)$.

Iб) Покажем, что существует ординал Δ такой, что $\mathcal{G}|_\Delta$ действует из Δ на X сюръективно.

[4] Более подробно об аксиоме выбора и аксиоме детерминированности см. в [8, 11].

Допустим, что это не так, т. е. при любом ординале Δ имеем $\mathcal{G}\Delta \subset X$. Тогда, как видно из Iа), для ординалов $\Delta' \neq \Delta''$ получим $\mathcal{G}(\Delta') \neq = \mathcal{G}(\Delta'')$. Таким образом, имеется инъекция с класса ординалов в множество, откуда легко показать (по теореме 1.17), что Ord есть множество. Противоречие.

Итак, существует ординал Δ, с которого $\mathcal{G}$ действует сюръективно на X. В дальнейшем через Δ будем обозначать наименьший из таких ординалов.

Iв) Очевидно, $\Delta > 0$, т. к. X не пусто. Покажем, что функция $g = \mathcal{G}|_\Delta$ действует из Δ в X инъективно.

Действительно, пусть $\alpha < \beta < \Delta$, тогда $g\alpha$ и $g\beta$ есть собственные подмножества X (иначе Δ не был бы наименьшим из ординалов, с которых $\mathcal{G}$ действует сюръективно на X). Теперь, из Iа) легко получить, что $g(\alpha) \neq g(\beta)$, откуда следует инъективность g.

Iг) Из Iб) и Iв) заключаем, что функция g есть взаимно однозначное соответствие между X и Δ. Полагая теперь для любых $a, b \in X$: $a <_X b \Leftrightarrow g^{-1}(a) < g^{-1}(b)$, получаем полное упорядочение множества X, для которого $\mathrm{Ord}(X, <_X) = \Delta$.

II *Покажем, что из теоремы Цермело вытекает лемма Цорна.*

Пусть X — частично упорядоченное отношением $<$ непустое множество, в котором каждая цепь ограничена. Необходимо показать, что при выполнении теоремы Цермело в X есть максимальный элемент.

Из теоремы Цермело следует, что на X можно задать отношение полного порядка. Обозначим это отношение $\ll$. Пусть

$$\Omega_A = \{x \in X \,|\, \forall a \in A : \; a < x\} \text{ для всех } A \subseteq X.$$

Рассмотрим функцию $F : \mathrm{Exp}(X) \to X$ такую, что

$$F(A) = \begin{cases} \min\limits_{\ll} \Omega_A, & \Omega_A \neq \emptyset, \\ \min\limits_{\ll} X, & \Omega_A = \emptyset, \end{cases}$$

где символ $\min\limits_{\ll}$ обозначает минимум множества по отношению $\ll$. Это различие необходимо, т. к. у нас задано два отношения порядка на одном и том же множестве X.

По теореме о рекурсивных определениях (см. теорему 2.3) существует отображение $\mathcal{G}$ из Ord в X такое, что при любом ординале α имеем $\mathcal{G}(\alpha) = F(\mathcal{G}\alpha)$.

Легко видеть, что при ординалах $\Delta' < \Delta''$ имеем $\mathcal{G}\Delta' \subseteq \mathcal{G}\Delta''$ и, кроме того, $\Omega_{\mathcal{G}\Delta''} \subseteq \Omega_{\mathcal{G}\Delta'}$.

IIа) Покажем, что если $\Omega_{\mathcal{G}\Delta''} \neq \emptyset$, то $\mathcal{G}(\Delta') < \mathcal{G}(\Delta'')$.

Поскольку множество $\Omega_{\mathcal{G}\Delta''}$ не пусто, то из определения F видно, что $\mathcal{G}(\Delta'') \in \Omega_{\mathcal{G}\Delta''}$. Тогда для любого $a \in \mathcal{G}\Delta''$ имеем $a < \mathcal{G}(\Delta'')$, в частности, $\mathcal{G}(\Delta') < \mathcal{G}(\Delta'')$.

IIб) Покажем, что существует ординал Δ такой, что $\Omega_{\mathcal{G}\Delta} = \emptyset$.

Действительно, предположим, что это не так. Тогда для любых двух ординалов $\Delta' < \Delta''$ имеем $\mathcal{G}(\Delta') < \mathcal{G}(\Delta'')$ из IIа), т.е. $\mathcal{G}$ есть инъективное отображение из Ord в X, откуда по теореме 1.17 Ord будет множеством. Противоречие.

IIв) Через Δ обозначим теперь наименьший из тех ординалов, существование которых доказано в IIб). Покажем, что $\mathcal{G}\Delta$ есть цепь в X. Для этого достаточно показать связность отношения $<$ на множестве $\mathcal{G}\Delta$.

Пусть $x, y \in \mathcal{G}\Delta$. Тогда существуют ординалы $\alpha, \beta \in \Delta$ такие, что $x = \mathcal{G}(\alpha)$, $y = \mathcal{G}(\beta)$. Возможны только три варианта: $\alpha < \beta$ или $\alpha = \beta$ или $\beta < \alpha$. В случае $\alpha = \beta$ имеем $x = y$.

Пусть $\alpha < \beta$. Ясно, что множества $\Omega_{\mathcal{G}\alpha}$ и $\Omega_{\mathcal{G}\beta}$ не пусты, т.к. в противном случае Δ не был бы наименьшим из таких ординалов, для которых $\Omega_{\mathcal{G}\Delta} = \emptyset$. Тогда из IIа) $x < y$. Аналогично в случае $\beta < \alpha$ доказывается, что $y < x$.

Итак, $<$ есть отношение линейного порядка на $\mathcal{G}\Delta$, т.е. $\mathcal{G}\Delta$ — цепь в X.

IIг) Пусть элемент $c \in X$ ограничивает цепь $\mathcal{G}\Delta$. Покажем, что c есть максимальный элемент в X.

Предположим, что существует $c' \in X$ такой, что $c < c'$. Тогда для любого $a \in \mathcal{G}\Delta$ имеем $a \leqslant c < c'$, т.е. $a < c'$, откуда следует, что $c' \in \Omega_{\mathcal{G}\Delta}$, что противоречит тому, что $\Omega_{\mathcal{G}\Delta} = \emptyset$.

Итак, в X есть максимальный элемент.

III *Покажем теперь, что из леммы Цорна вытекает аксиома выбора.*

Пусть множество X таково, что $\cup X \neq \emptyset$. И пусть выполнена лемма Цорна. Построим для множества X функцию выбора.

Через $\mathbb{D}$ обозначим множество всех функций выбора $f : A \to \cup A$ таких, что $A \subseteq X$ и $\cup A \neq \emptyset$. Множество $\mathbb{D}$ не пусто, ибо для $A = \{x_0\}$, $x_0 \neq \emptyset$, функция выбора существует всегда. Множество $\mathbb{D}$ частично упорядочено отношением $\subset$ собственного вложения множеств.

IIIа) Покажем, что в $\mathbb{D}$ каждая цепь ограничена.

Пусть $\mathfrak{F}$ — цепь в $\mathbb{D}$. Через f_0 обозначим множество $\cup\mathfrak{F}$, а через A_0 обозначим объединение всех таких подмножеств $A \subseteq X$, что в $\mathfrak{F}$ существует функция выбора с областью определения A. Заметим, что для всякого $x \in A_0$ существует функция $f \in \mathfrak{F}$ такая, что f :

$A \to \cup A$, $x \in A$. При этом в случае $x \neq \emptyset$ имеем $f(x) \in x$, а значит, пара $(x, f(x))$ есть элемент множества f_0. Это означает, что если f_0 — функция, то она непременно будет и функцией выбора.

Пусть $(x, x'), (x, x'') \in f_0$. Из определения f_0 видно, что существуют функции $f', f'' \in \mathfrak{F}$ такие, что $f'(x) = x'$, $f''(x) = x''$. Так как $\mathfrak{F}$ — цепь, то мы можем выбрать наибольший из элементов f', f'', обозначив его f. Тогда $f(x) = x'$ и $f(x) = x''$, откуда $x' = x''$. Итак, f_0 — функция выбора для множества A_0.

Функция f_0 является элементом $\mathbb{D}$ и ограничивает цепь $\mathfrak{F}$.

IIIб) Найдем теперь функцию выбора для X.

Как видно из IIIа), множество $\mathbb{D}$ удовлетворяет условиям леммы Цорна. Тогда в $\mathbb{D}$ существует максимальный элемент. Обозначим его $\mathfrak{C}$. $\mathfrak{C}$ является функцией выбора с областью определения A, где $A \subseteq X$. Предположим, что существует $x_0 \in X \setminus A$, $x_0 \neq \emptyset$. Тогда функция $\mathfrak{C}$ не определена в точке x_0. Пусть $y_0 \in x_0$. Рассмотрим множество $\mathfrak{C} \cup \{(x_0, y_0)\}$. Легко показать, что это множество будет функцией выбора, большей (в смысле вложения), чем $\mathfrak{C}$. Получено противоречие с максимальностью $\mathfrak{C}$.

Итак, $\mathfrak{C}$ есть функция выбора для X, и теорема доказана полностью. □

Приложения аксиомы выбора

Здесь мы приведем несколько довольно интересных с нашей точки зрения следствий из аксиомы выбора, хотя тем самым мы покажем лишь ничтожную часть той роли, которую играет аксиома в современной математике.

Прежде всего надо вспомнить, что когда мы рассматривали прямое произведение множеств в § 1.6, мы не могли гарантировать существование хотя бы одного элемента в множестве $\prod\limits_C L_x$. Аксиома выбора позволяет это сделать. Действительно, пусть $I : C \to \{L_x\}_{x \in C}$ есть индексация, т. е. $I(x) = L_x$ для любого $x \in C$. Рассмотрим какую-нибудь функцию выбора $f : \{L_x\}_{x \in C} \to \bigcup\limits_{x \in C} L_x$. Тогда, очевидно, суперпозиция $f \circ I$ будет элементом прямого произведения $\prod\limits_C L_x$, т. к. $f \circ I : C \to \bigcup\limits_{x \in C} L_x$ и, кроме того, $(f \circ I)(x) \in L_x$ для каждого $x \in C$.

Рассмотрим еще несколько следствий аксиомы выбора.

°**Теорема 2.10.** *Пусть A — непустое множество, R_0 — отношение порядка на A. Тогда найдется отношение $R \supseteq R_0$, которое линейно упорядочивает A.*

Доказательство. Через $\mathcal{K}$ обозначим множество всех отношений порядка на A, содержащих R_0. Множество $\mathcal{K}$ частично упорядочено отношением $\subset$ собственного вложения.

Пусть $\mathcal{P}$ — цепь в $\mathcal{K}$. Покажем, что она ограничена в $\mathcal{K}$.

Пусть $Q = \cup\mathcal{P}$. Очевидно, для любого $S \in \mathcal{P}$ имеем $S \subseteq Q$. Легко проверить, что Q — отношение частичного порядка на A. Поэтому цепь $\mathcal{P}$ ограничена.

Тогда по лемме Цорна в $\mathcal{K}$ есть максимальный элемент, обозначим его R. Покажем, что это линейный порядок. Так как R — частичный порядок, то достаточно показать его связность. Предположим, что R не связно, т. е. существуют $a, b \in A$ такие, что $\rceil(aRb) \wedge (a \neq b) \wedge \rceil(bRa)$.

Пусть $S = \{(x, y) | \, (x, y \in A) \wedge ((xRa \wedge bRy) \vee (x = a \wedge bRy) \vee (xRa \wedge y = b) \vee (x = a \wedge y = b))\}$, $R' = R \cup S$. Покажем, что R' будет отношением частичного порядка на A.

1) антирефлексивность: пусть $xR'x$, т. к. R антирефлексивно, то xRa и bRx, или $x = a$ и bRx, или xRa и $x = b$, или $x = a$ и $x = b$. В любом случае получим противоречие с предположением.

2) транзитивность: пусть $xR'y$ и $yR'z$. Возможны только четыре варианта:

а) $(xRy) \wedge (yRz)$, откуда xRz и, следовательно, $xR'z$;

б) $(xRy) \wedge (ySz)$, откуда $(xRy) \wedge (yRa) \wedge (bRz)$, или $(xRy) \wedge (y = a) \wedge (bRz)$, или $(xRy) \wedge (yRa) \wedge (z = b)$, или $(xRy) \wedge (y = a) \wedge (z = b)$. В любом из этих случаев получим или $(xRa) \wedge (bRz)$, или $(xRa) \wedge (z = b)$, откуда xSz и, следовательно, $xR'z$;

в) $(xSy) \wedge (yRz)$. Так же, как в пункте б), можно показать, что xSz, откуда $xR'z$.

г) $(xSy) \wedge (ySz)$. Здесь легко показать, что в любом случае получим bRa, что невозможно по предположению.

Итак, R' — частичный порядок на A, причем $R \subset R'$, т. к. aSb (и значит, $aR'b$) и в то же время $\rceil(aRb)$. Получено противоречие с тем, что R — максимальный элемент в $\mathcal{K}$.

Окончательно имеем: R — линейный порядок на A. □

Определение 2.8. Множества X и Y назовем *равномощными*, если $X \leftrightarrow Y$, т. е. если существует биекция $f : X \to Y$

В теории ZFC будем называть множество *конечным*, если оно равномощно некоторому натуральному числу n, в противном случае назовем множество *бесконечным*. В главе 3 в рамках теории ZFC будет доказано, что множество бесконечно тогда и только тогда, когда оно равномощно некоторому своему собственному подмножеству.

Без доказательства приведем следующий факт.

°**Теорема 2.11.** *Пусть A — бесконечное множество, а $\mathcal{M}$ — некоторый набор его подмножеств (не обязательно всех), равномощных A. Тогда существует подмножество $Z \subseteq A$, равномощное A и своему дополнению $A \setminus Z$, обладающее тем свойством, что для любого $X \in \mathcal{M}$*

$$Z \cap X \neq \emptyset \quad \wedge \quad (Z \neq X \to X \setminus Z \neq \emptyset),$$

и такое, что его дополнение обладает этим же свойством.

°**Следствие 2.12.** *Если в теореме* 2.11 *положить $A = \mathbb{R}$, $\mathcal{M}$ — семейство непустых совершенных множеств*[5], *то получим, что существует множество $Z \subseteq \mathbb{R}$, имеющее с каждым совершенным множеством общую точку, и его дополнение обладает тем же свойством*[6].

Базис Гамеля.

Множество $X \subseteq \mathbb{R}$ называется *независимым*, если для любого конечного набора ненулевых элементов $x_1, \ldots, x_n \in X$ и любых рациональных чисел $r_1, \ldots, r_n$ сумма $\sum\limits_{i=1}^{n} x_i r_i$ обращается в нуль тогда и только тогда, когда все r_i равны нулю. Например, множество $\{\sqrt{2}, \sqrt{3}\}$ независимо.

Легко показать, что если B — цепь независимых множеств (по вложению), то ее предел $\cup B$ также есть независимое множество. Поэтому из леммы Цорна вытекает следующая

°**Теорема 2.13.** *В $\mathbb{R}$ существует максимальное независимое множество.*

Определение 2.9. Максимальное независимое множество называется *базисом Гамеля*.

Пусть H — базис Гамеля. Вполне очевидна

°**Теорема 2.14.** *Для любого $x \in \mathbb{R} \setminus \{0\}$ верно равенство $x = \sum\limits_{i=1}^{n} r_i b_i$, где $r_i \in \mathbb{Q} \setminus \{0\}$, $b_i \in H$, и это разложение единственно.*

Доказательство. Если x не представимо в таком виде, то множество $H \cup \{x\}$ независимо в противоречии с максимальностью H. Если же

$$x = \sum_{i=1}^{n} r_i b_i = \sum_{i=1}^{m} r'_i b'_i$$

[5] Такие множества равномощны $\mathbb{R}$, см. Куратовский Топология, т.1, «Мир», М., 1966, т.2, «Мир», М., 1969.

[6] Можно доказать, что это множество неизмеримо по Лебегу.

при различных наборах b_i и b'_i и не равных нулю r_i, r'_i, то множество

$$\{b_1, \ldots, b_n, b'_1, \ldots, b'_m\}$$

зависимо, откуда зависимо и множество H. Противоречие. □

Аксиома выбора вместе с привлекательными выводами, подобными только что приведенным фактам или тем теоремам, которые эквивалентны ей (в **ZF**), обладает и многими «странными» следствиями, доказывающими существование разного рода «экзотических» множеств. Некоторые из них мы сейчас покажем, а более богатый обзор следствий аксиомы выбора можно найти в [8, 11].

°**Теорема 2.15.** *Существует вещественная аддитивная не непрерывная функция.*

Доказательство. Пусть H — базис Гамеля, $x_0 \in H$. В силу теоремы 2.14 для каждого $x \in \mathbb{R} \setminus \{0\}$ существует единственное разложение по элементам базиса Гамеля. Естественно, элемент x_0 может как входить в это разложение, так и не входить.

Определим функцию $f : \mathbb{R} \to \mathbb{R}$ так: если x_0 входит в разложение x с коэффициентом r, то полагаем $f(x) = r$, если же $x = 0$ или x_0 не входит в разложение x, то полагаем $f(x) = 0$. Легко проверить, что для любых $x, y \in \mathbb{R}$ имеем $f(x+y) = f(x)+f(y)$ и в то же время функция f разрывна, т. к. принимает только рациональные значения. □

°**Теорема 2.16.** (Пример Виталú). *Существует неизмеримое по Лебегу множество в $\mathbb{R}$.*

Доказательство. На множестве $\mathbb{R}$ введем отношение $\sim$ следующим образом. Положим $x \sim y$ в том и только в том случае, когда $x - y$ есть рациональное число. Нетрудно проверить, что отношение $\sim$ есть отношение эквивалентности на $\mathbb{R}$. Каждый класс эквивалентности имеет вид $\alpha + \mathbb{Q}$, где $\alpha \in \mathbb{R}$, $\mathbb{Q}$ — множество рациональных чисел. Очевидно, что каждый класс содержит точки из отрезка $[0;1]$. Пользуясь аксиомой выбора, построим множество M, собрав в нем ровно по одной точке с отрезка $[0;1]$ из каждого класса эквивалентности. Покажем, что множество $M \subseteq [0;1]$ неизмеримо по Лебегу.

Обозначим $M_r = M + r$, где $r \in \mathbb{Q} \cap [-1;1]$, и пусть $S = \bigcup\{M_r |\ r \in \mathbb{Q} \cap [-1;1]\}$. Множества M_r попарно не пересекаются, поэтому в силу счетной аддитивности меры Лебега μ получим:

$$\mu S = \sum_{r \in \mathbb{Q} \cap [-1;1]} \mu M_r,$$

откуда следует, что при $\mu M = 0$ имеем $\mu S = 0$, а при $\mu M > 0$ получим $\mu S = \infty$, т. к. $\mu M_r = \mu M$ при любом $r \in \mathbb{Q} \cap [-1; 1]$.

Ясно, что для любой точки $\alpha \in [0; 1]$ существует рациональное r такое, что $\alpha + r \in M$, причем $r \in [-1; 1]$. Поэтому $[0; 1] \subseteq S$, откуда вытекает, что $\mu S > 0$, а значит, $\mu S = \infty$, т. е. $\mu M > 0$.

С другой стороны, объединение всех множеств M_r содержится в $[-1; 2]$, откуда вытекает, что $\mu S < \infty$, т. е. $\mu M = 0$. Противоречие.

Итак, множество M не измеримо по Лебегу. □

Одним из наиболее удивительных следствий аксиомы выбора является т. н. «парадоксальное» разбиение сферы, построенное Хаусдорфом.

°**Теорема 2.17.** (Хаусдорф). *Существует разбиение сферы S на попарно непересекающиеся множества X, Y, Z, Q, которые обладают следующими свойствами:*

(i) *X, Y, Z и $Y \cup Z$ переходят друг в друга вращением сферы;*

(ii) *множество Q счетно.*

Доказательство. Рассмотрим две оси a и b вращения сферы S. Рассмотрим группы вращений $\{1, p\}$ и $\{1, q, qq\}$, где p — вращение на 180^o вокруг оси a, q — вращение на 120^o вокруг оси b. Эти группы можно свободно перемножить и получить некоторую группу G вращений сферы.

Каждый элемент этой группы есть некторое слово, составленное из букв $1, p, q$. В записи слов мы, естественно, исключаем последовательности букв pp и qqq, поскольку они заменимы посредством тождественного вращения 1.

Оси a и b можно выбрать так, что разные слова описывают разные вращения. Действительно, допустим, что это не так и предположим, что для любых осей a и b найдутся два разных слова W и V, описывающих одно и то же вращение, тогда слово WV^{-1}, в котором мы удалим все последовательности букв pp и qqq, является тождественным вращением, но это слово, очевидно, не тривиально (поскольку $W \neq V$). Обозначим через t угол между осями a и b. Для данного нетривиального слова, являющегося тем не менее тождественным преобразованием сферы, существует лишь конечное множество допустимых значений угла t. Всего слов — счетное множество. Тогда всего значений угла t — счетное множество. Противоречие.

Далее считаем, что угол t между осями a и b выбран так, что никакое нетривиальное слово не может быть равно 1, т. е. что разные слова дают разные вращения.

Ключевой момент: разобьем группу G на три непересекающихся подмножества A, B, C таких, что

$$Ap = B \cup C, \ Aq = B, \ Aqq = C.$$

Очевидно, что можно в A собрать слова, оканчивающиеся на p, в B — оканчивающиеся на pq, в C — на pqq, и отдать 1 в А, q — в B, qq — в C.

На сфере S существует лишь счетное множество точек, остающихся неподвижными при некотором вращении $g \in G$, поскольку каждое вращение имеет ровно две неподвижные точки, а всего вращений в G счетное множество. Обозначим через Q множество всех таких точек.

Теперь введем отношение эквивалентности на множестве $S \setminus Q$ так, что каждый класс эквивалентности — это орбита, порожденная группой G, точнее, положим для $x, y \in S \setminus Q$ x эквивалентно y тогда и только тогда, когда $y = x * g$ при некотором вращении $g \in G$. Далее с помощью аксиомы выбора построим множество M, содержащее ровно по одной точке из каждого класса эквивалентности, и положим $X = M * A$, $Y = M * B$, $Z = M * C$.

Нетрудно видеть, что множества X, Y, Z, Q попарно не пересекаются и удовлетворяют (i) и (ii), поскольку

$$\begin{gathered}Y = M * B = M * (Aq) = (M * A)q = Xq, \quad Z = Xqq,\\ Y \cup Z = M * (B \cup C) = M * (Ap) = (M * A)p = Xp,\end{gathered}$$

Q счетно. □

В заключение сформулируем *парадокс Банаха—Тарского*. На подмножествах пространства $\mathbb{R}^3$ определим отношение $\sim$ следующим образом: положим $X \sim Y$ тогда и только тогда, когда существует такое разбиение $X = X_1 \cup \dots \cup X_n$ множества X на конечное число попарно непересекающихся множеств и такое разбиение $Y = Y_1 \cup \dots \cup Y_n$ на то же самое число попарно непересекающихся множеств, что X_i конгруэнтно Y_i для каждого $i = 1, \dots, n$.[7]

Нетрудно проверить, что отношение $\sim$ является отношением эквивалентности на $\mathrm{Exp}(\mathbb{R}^3)$, причем, если X не пересекается с X', Y не пересекается с Y', $X \sim Y$, $X' \sim Y'$, то $X \cup X' \sim Y \cup Y'$. Имея в распоряжении перечисленные свойства отношения $\sim$ и теорему

[7]Напомним, что два множества в арифметическом конечномерном пространстве *конгруэнтны*, если и только если они переходят друг в друга преобразованиями поворота и переноса.

Хаусдорфа, в рамках теории ZFC можно доказать следующее утверждение.

°**Теорема 2.18.** (Банах—Тарский, 1924). *Замкнутый шар B^3 может быть разбит на два непересекающихся множества $B^3 = X \cup Y$ так, что $B^3 \sim X$, $B^3 \sim Y$.*

Иными словами, пользуясь аксиомой выбора, замкнутый шар B^3 можно разбить на конечное число частей так, что после некоторой перестановки этих частей получим два шара того же радиуса. Понятно, что все части, на которые «разрезается» исходный шар B^3, не измеримы по Лебегу.

Глава 3

КАРДИНАЛЫ

В предыдущей главе мы занимались изучением различных видов вполне упорядочений множеств, точнее, мы рассмотрели некоторые свойства специальных множеств, моделирующих все возможные полные порядки элементов на множествах, отвлекаясь от их природы. Эти множества мы назвали ординалами.

Теперь же мы намерены пойти еще дальше, и рассмотреть такие модели множеств, которые отражают лишь «количество» элементов в множествах, отвлекаясь уже и от порядка этих элементов. Мы построим специальный класс множеств, называемых кардиналами, которые и будут нашими моделями «количеств», или, как принято говорить, мощностями.

Классы ординалов и кардиналов — это два уникальных класса множеств, предназначенных для отображения двух основных свойств абстрактных множеств: порядка и количества элементов.

Перейдем теперь непосредственно к изучению кардиналов.

§ 3.1 Мощность множества. Алефы

Для того, чтобы уметь сравнивать «количества» элементов в множествах, необходимо сначала научиться определять множества с одинаковым «количеством» элементов. Для этого мы пользуемся одним особым видом функции — взаимно однозначным соответствием (биекцией). Мы говорим, что два множества равномощны, если между ними существует взаимно однозначное соответствие (см. опр. 2.8). Для множеств с конечным (натуральным) количеством элементов это определение вполне естественно. Для всех прочих множеств мы принимаем точно такое же определение.

Следующая теорема является простым достаточным признаком равномощности двух множеств.

Поскольку в одних источниках (см., например, [12]) эта теорема называется теоремой Кантора—Бернштейна, а в других (например, [13]) — теоремой Шредера—Бернштейна, мы будем называть эту теорему теоремой Кантора—Бернштейна—Шредера, сокращенно обозначая CBS.

Теорема 3.1. (CBS) *Для любых двух непустых множеств A и B если существуют инъекции $f : A \to B$ и $g : B \to A$, то эти множества равномощны.*

Доказательство. Рассмотрим функцию $H : \mathrm{Exp}(A) \to \mathrm{Exp}(A)$, определяемую следующей формулой:

$$H(X) = A \setminus g[B \setminus fX] \text{ для всех } X \subseteq A.$$

Предположим, что существует корень уравнения $H(X) = X$ — некое множество X_0. Посмотрим, какими свойствами оно обладает. Обозначим через Y_0 множество $B \setminus fX_0$. Поскольку $H(X_0) = X_0$, то $gY_0 = A \setminus X_0$. Таким образом, сужения функций $f|_{X_0}$ и $g|_{Y_0}$ действуют на непересекающихся подмножествах множеств A и B, но тем не менее «покрывают» эти множества целиком.

Точнее, рассмотрим обратную к $g|_{Y_0}$ функцию, определенную на множестве $A \setminus X_0$, обозначив ее h. Имеем: $h : A \setminus X_0 \to Y_0$ — биекция, $f|_{X_0} : X_0 \to B \setminus Y_0$ — тоже биекция. Тогда объединение этих функций $h \cup f|_{X_0}$ есть биекция из A в B.

Итак, доказательство теоремы свелось к поиску корня уравнения $H(X) = X$. Назовем множество X *хорошим*, если $X \subseteq H(X)$, и через Z обозначим объединение всех хороших множеств.

Нетрудно проверить, что функция H монотонна по вложению множеств, т. е. если $X \subseteq Y$, то $H(X) \subseteq H(Y)$. Пусть $z \in Z$. Тогда существует хорошее множество X такое, что $z \in X$. Кроме того, имеем $H(X) \subseteq H(Z)$ и $X \subseteq H(X)$. Отсюда заключаем, что $z \in H(Z)$, и это верно для любого $z \in Z$. Таким образом, Z — хорошее множество.

Чтобы показать, что Z и есть корень нашего уравнения, надо проверить обратное вложение, т. е. что $H(Z) \subseteq Z$. Допустим, что это не так. Тогда существует $x \in H(Z) \setminus Z$. Рассмотрим множество $Z' = Z \cup \{x\}$. Это множество не может быть хорошим, т. к. иначе оно бы содержалось в Z. Поэтому $Z' \nsubseteq H(Z')$. Ясно, что $H(Z) \subseteq H(Z')$, поэтому $Z' \nsubseteq H(Z)$. С другой стороны, $Z \subseteq H(Z)$. Следовательно, точка x — единственная точка множества Z', не попадающая в $H(Z)$. Получено противоречие с тем, что $x \in H(Z)$.

Итак, $H(Z) \subseteq Z$, откуда $H(Z) = Z$, т. е. Z — искомое множество. □

Отметим без доказательства несколько полезных следствий этой теоремы.

Следствие 3.2. *Множества* $\mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}$ *и* $\mathbb{Q}$ *равномощны* ω.

Следствие 3.3. *Множество* $\mathbb{R}$, *отрезок* $[0; 1]$ *и полуинтервалы* $[0; 1)$, $(0; 1]$ *равномощны интервалу* $(0; 1)$.

Введем, наконец, понятие кардинала.

Определение 3.1. Ординал τ называется *кардиналом* (или *кардинальным числом*), если для любого ординала $\alpha < \tau$ не верно, что $\alpha \leftrightarrow \tau$.

Итак, мы видим, что кардинал — это в первую очередь порядковое число. Но из всех равномощных друг другу порядковых чисел кардинал является наименьшим таким числом, реализуя как бы наиболее «емкий» из всех возможных порядков для данного «количества» элементов. Выбор таких уникальных множеств в качестве кардиналов определяется, во-первых, замечательными свойствами самих ординалов (их транзитивностью и вполне упорядоченностью), а во-вторых, тем, что в качестве мощностей мы берем вполне конкретные объекты теории множеств, т. е. множества.

Теперь нам следует договориться об обозначениях кардинальных чисел, используемых на протяжении всей главы. Через Card мы будем обозначать класс всех кардиналов. Ясно, что $\mathrm{Card} \subseteq \mathrm{Ord}$, поэтому класс кардиналов также вполне упорядочен отношением принадлежности, как и класс ординалов. Знак $<$ для кардиналов будет использоваться в точности с той же целью, с какой он используется на классе ординалов. Итак, кардиналы мы можем сравнивать, и это сравнение есть отношение принадлежности, вполне упорядочивающее кардиналы.

Если τ есть какой-либо кардинал, то через Card_τ мы будем обозначать класс всех кардиналов, не меньших, чем τ.

Ранее мы условились «по умолчанию» использовать греческие буквы, кроме φ, ψ и ω, для обозначения произвольных ординалов. Теперь же мы условимся, что все греческие буквы, начиная с λ и до конца алфавита, исключая, как обычно, φ, ψ и ω, обозначают кардиналы, если не оговорено противное. Буквы φ и ψ, как и прежде, зарезервированы нами для обозначения формул, а ω есть символ-константа, обозначающий множество натуральных чисел.

Кардинал τ мы называем *бесконечным*, если $\tau \geqslant \omega$. В противном случае кардинал называется *конечным*, и его мы обозначаем точно так же, как натуральные числа.

Рассмотрим теперь некоторые свойства кардиналов.

✓ **3.1.** Бесконечный кардинал является предельным ординалом.

Доказательство. Предположим, что это не так, и пусть $\tau = S(\alpha)$, $\tau \geqslant \omega$. Покажем теперь, что ординалы α и $S(\alpha)$ равномощны. Если предположить, что $\alpha < \omega$, то отсюда получим $\tau < \omega$, т. е. кардинал τ конечен. Противоречие. Поэтому $\alpha \geqslant \omega$. Пусть $f : S(\alpha) \to \alpha$ и

$$f(\gamma) = \begin{cases} S(\gamma), & \gamma < \omega, \\ \gamma, & \omega \leqslant \gamma < \alpha, \\ 0, & \gamma = \alpha. \end{cases}$$

Нетрудно убедиться в том, что f есть взаимно однозначное соответствие между $S(\alpha)$ и α. Но $\alpha < \tau = S(\alpha)$. Тогда по определению кардиналов τ не является кардиналом. Противоречие. □

✓ **3.2.** Ординал ω и все натуральные числа являются кардиналами.

✓ **3.3.** Ординалы $S(\omega)$, $S(S(\omega))$, $S(S(S(\omega)))$, $\ldots$ не являются кардиналами.

Определение 3.2. Если между множеством X и кардиналом τ существует взаимно однозначное соответствие, то кардинал τ называется *мощностью* множества X. При этом мы используем для τ следующие обозначения: $||X||$, $\operatorname{Card} X$.

По определению положим также, что мощность пустого множества $\emptyset$ есть нулевой кардинал.

Очевидно, что для каждого кардинала τ имеем $||\tau|| = \tau$.

✓ **3.4.** Мощность множества определяется однозначно.

Доказательство. Если $\tau = ||X||$ и $\xi = ||X||$, то τ и ξ равномощны. Если предположить, что $\tau < \xi$, то ξ не есть кардинал (по определению). Аналогично исключается вариант $\xi < \tau$. Следовательно, $\xi = \tau$. □

✓ **3.5.** Если α — ординал, и τ — его мощность, то $\tau \leqslant \alpha$.

✓ **3.6.** Множество X можно вполне упорядочить тогда и только тогда, когда оно имеет мощность.

Доказательство. Пусть $(X, <)$ — вполне упорядоченное множество, тогда для него существует единственный порядковый тип α. Обозначим через A множество всех таких ординалов $\beta \leqslant \alpha$, что $\alpha \leftrightarrow \beta$. Пусть $\gamma = \min A$. Тогда, очевидно, $\gamma \leftrightarrow \alpha$ и для любого $\beta < \gamma$ не верно, что $\beta \leftrightarrow \gamma$. Поэтому γ — кардинал. Нетрудно видеть, что $||X|| = \gamma$.

Обратно. Если $||X|| = \tau$, то существует биекция $f : X \to \tau$. Тогда положим для любых $x, y \in X \quad x \prec y$ тогда и только тогда, когда $f(x) < f(y)$. Итак, $(X, \prec)$ — вполне упорядоченное множество. □

Используя это свойство и теорему 2.9, несложно доказать следующий факт.

Теорема 3.4. *Аксиома выбора* AC *эквивалентна утверждению: каждое множество имеет мощность.*

Следующая теорема показывает существование неравномощных бесконечных множеств, более того, с ее помощью можно построить бесконечно много попарно неравномощных множеств.

Теорема 3.5. (Георг Кантор). $\mathrm{Exp}(X) \not\leftrightarrow X$.

Доказательство. Для пустого множества X теорема очевидна. Пусть $X \neq \emptyset$. Предположим, что существует биекция $f : X \to \mathrm{Exp}(X)$. Пусть $A = \{x \in X | \ x \notin f(x)\}$. Очевидно, $A \in \mathrm{Exp}(X)$. Пусть $a = f^{-1}(A)$ (ведь f — биекция). Как связаны a и A? Здесь ситуация, аналогичная парадоксу Расселла.

Допустим, что $a \in A$. Тогда по определению множества A получим $a \notin f(a)$, но $f(a) = A$. Противоречие.

Предположим, что $a \notin A$. Тогда вновь по определению множества A имеем $a \in f(a)$, вновь противоречие. Итак, $\mathrm{Exp}(X) \not\leftrightarrow X$. □

Следствие 3.6. *Если существует мощность* $\mathrm{Exp}(X)$*, то существует мощность* X *и* $||X|| < ||\,\mathrm{Exp}(X)||$.

°**Следствие 3.7.** *Не существует наибольшего кардинала.*

Доказательство. Если τ — наибольший кардинал, то в силу AC существует мощность $\mathrm{Exp}(\tau)$, которая превосходит τ в противоречии с максимальностью кардинала τ. □

Заметим, что без аксиомы выбора утверждение о несуществовании наибольшего кардинала или равносильное утверждение о том, что Card — не множество, вообще говоря не доказуемы.

Пользуясь теоремой Кантора и известным фактом анализа о том, что $\mathbb{R} \leftrightarrow \mathrm{Exp}(\omega)$,[1] легко видеть, что $\omega \not\leftrightarrow \mathbb{R}$, более того, в рамках теории ZFC справедливо неравенство: $\omega < ||\mathbb{R}||$.

Нетрудно доказать следующий признак сравнения мощностей.

✓ **3.7.** Если у множеств A и B существуют мощности, то $||A|| \leqslant ||B||$, если выполнено хотя бы одно из условий:

1) существует инъекция $f : A \to B$;

2) существует сюръекция $f : B \to A$.

✓ **3.8.** Если A — множество кардиналов, то $\cup A$ — кардинал, причем $\cup A = \sup A$ в классе Card.

Доказательство. По аналогичному свойству ординалов получаем, что $\cup A$ — ординал, причем $\cup A = \sup A$. Осталось показать, что $\cup A$ — кардинал.

Пусть $\alpha < \cup A$ и α равномощен $\cup A$. Очевидно, существует $\tau \in A$ такой, что $\alpha < \tau$. Пусть $\xi = ||\alpha||$. Тогда $\xi \leqslant \alpha < \tau$. Кроме того, $\tau \subseteq \cup A$. Поскольку $\alpha \leftrightarrow \cup A$ и $\xi = ||\alpha||$, то существуют биекции из $\cup A$ в α и из α в ξ. Это означает, что существует биекция из $\cup A$ в ξ, а значит, существует инъекция из τ в ξ. С другой стороны, тождественная функция на ξ будет инъекцией из ξ в τ. Тогда по теореме CBS получим $\xi = \tau$. Противоречие. Итак, $\cup A$ — кардинал. □

Введем следующее обозначение. Через τ^+ будем обозначать наименьший из кардиналов, больших τ, если такой кардинал существует. В теории ZFC кардинал τ^+ существует для любого кардинала τ, кроме того, справедлива следующая

°**Теорема 3.8.** (Об áлефах[2]).

Существует и единственно отображение $\aleph : \mathrm{Ord} \to \mathrm{Card}_\omega$ *такое, что:*

1) $\aleph(0) = \omega$;

2) $\aleph(S(\alpha)) = \aleph(\alpha)^+$;

3) *если α — предельный, то* $\aleph(\alpha) = \sup\limits_{\gamma<\alpha} \aleph(\gamma)$.

[1] При доказательстве этого факта аксиома выбора не используется!

[2] Алеф — $\aleph$ — первая буква древнееврейского алфавита.

Доказательство. Пусть $\mathcal{F} : \mathrm{Exp}(\mathrm{Card}_\omega) \to \mathrm{Card}_\omega$ и $\mathcal{F}(A) = \sup A$, если $\sup A \notin A$, и $\mathcal{F}(A) = (\sup A)^+$, если $\sup A \in A$, для любого непустого подмножества $A \subset \mathrm{Card}_\omega$, $\mathcal{F}(\emptyset) = \omega$.

Тогда по теореме о рекурсивных определениях существует отображение $\aleph$ из Ord в Card_ω такое, что $\aleph(\alpha) = \mathcal{F}(\aleph\alpha)$.

а) Пусть $\alpha < \beta$, тогда $\aleph\alpha \subseteq \aleph\beta$, откуда $\aleph(\alpha) \leqslant \aleph(\beta)$. $\aleph(\alpha) \in \aleph\beta$. Предположим, $\aleph(\alpha) = \aleph(\beta)$, тогда $\aleph(\beta) \in \aleph\beta$, откуда $\mathcal{F}(\aleph\beta) \in \aleph\beta$, что противоречит определению $\mathcal{F}$. Итак, $\aleph(\alpha) < \aleph(\beta)$.

б) $\aleph(0) = \mathcal{F}(\emptyset) = \omega$.

в) Так как $\aleph[S(\alpha)]$ в силу монотонности $\aleph$, доказанной выше, имеет максимум, равный $\aleph(\alpha)$, то $\mathcal{F}(\aleph[S(\alpha)]) = \aleph(\alpha)^+$, откуда $\aleph(S(\alpha)) = \aleph(\alpha)^+$.

г) Для предельного ординала α имеем $\sup \alpha = \alpha$ (см. свойство ординалов 2.12). Если $\aleph\alpha$ имеет максимальный элемент, то в силу строгой монотонности $\aleph$, доказанной в а), α также имеет максимальный элемент, откуда $\sup \alpha \in \alpha$. Противоречие.

Итак, в $\aleph\alpha$ нет наибольшего элемента, следовательно, $\mathcal{F}(\aleph\alpha) = \sup \aleph\alpha$, откуда $\aleph(\alpha) = \sup\limits_{\gamma<\alpha} \aleph(\gamma)$.

д) Единственность отображения $\aleph$, удовлетворяющего 1) — 3), легко проверяется по индукции. □

Условимся везде далее вместо $\aleph(\alpha)$ для рассмотренного в теореме отображения $\aleph$ писать $\aleph_\alpha$, т. е. используем индекс. Такое обозначение бесконечных кардинальных чисел было введено еще Кантором. Этим, собственно, и объясняется название теоремы: об алефах.

°**Теорема 3.9.** *Отображение* $\aleph$, *существование которого доказано в теореме* 3.8, *биективно.*

Доказательство. 1) Инъективность $\aleph$ следует из пункта а) доказательства предыдущей теоремы.

2) Покажем сюръективность $\aleph$. Предположим, что $\aleph$ не сюръективно, и через τ обозначим наименьший из кардиналов, не принадлежащих образу $\aleph\,\mathrm{Ord}$. Очевидно, $\tau > \omega$.

Пусть $X = \{\xi \mid \omega \leqslant \xi < \tau\}$. В силу монотонности $\aleph$ легко показать, что множество $\Delta = \{\alpha \mid \aleph_\alpha \in X\}$ является ординалом. Тогда если Δ — предельный ординал, то $\sup X \notin X$ и в то же время $\sup X \leqslant \tau$, поэтому $\sup X = \tau$. Но $\sup X = \aleph_\Delta$ по теореме 3.8, поэтому $\tau \in \aleph\,\mathrm{Ord}$. Противоречие.

Если Δ — последующий ординал, то $\sup X \in X$, откуда $\tau = (\sup X)^+$ +. Но $\Delta = S(\sup \Delta)$ (по свойству 2.12 ординалов), откуда $\aleph_\Delta = (\aleph_{\sup \Delta})^+ = (\sup X)^+ = \tau$, откуда снова получаем $\tau \in \aleph\,\mathrm{Ord}$. Противоречие.

Следовательно, $\aleph$ сюръективно, и теорема доказана. □

Итак, любое бесконечное кардинальное число можно представить как $\aleph_\alpha$ при некотором ординале α, если мы принимаем аксиому выбора.

Как мы знаем, существуют предельные и последующие ординалы. Они составляют два достаточно богатых по свойствам подкласса класса Ord. Каждый кардинал является ординалом, поэтому и ненулевые кардиналы можно разделить на два класса, отнеся к первому классу кардиналы, являющиеся предельными ординалами, а ко второму — кардиналы, являющиеся последующими ординалами. Однако, как показывает свойство 3.1, такое разбиение кардиналов на классы весьма примитивно, ибо первый класс совпадет с классом Card_ω, а во второй войдут все конечные ненулевые кардиналы. Поэтому для кардиналов используют иной способ разбиения на специальные классы, а именно:

Определение 3.3. Кардинал τ называется *изолированным*, если существует кардинал ξ такой, что $\tau = \xi^+$, в противном случае ненулевой кардинал τ называется *предельным*.

Действуя по аналогии с доказательством только что приведенной теоремы, нетрудно установить следующий факт.

°**Теорема 3.10.** *Для любых ненулевого ординала α и непустого множества ординалов A справедливо следующее:*

1) *α — предельный ординал тогда и только тогда, когда $\aleph_\alpha$ — предельный кардинал;*

2) *α — последующий ординал тогда и только тогда, когда $\aleph_\alpha$ — изолированный кардинал;*

3) $\aleph_{\sup A} = \sup\limits_{\gamma\in A} \aleph_\gamma$.

Поэтому кардинал $\aleph_\omega$, как и кардинал ω, является предельным кардиналом, а все кардиналы $\aleph_n$ изолированы при $n > 0$.

Приведенные теоремы об отображении $\aleph$ из класса ординалов в класс кардиналов показывают, что если Card — не множество, то $\aleph$ есть порядковый изоморфизм между этими классами, т. е. взаимно однозначное соответствие, сохраняющее порядок. На самом деле существует гораздо более общая теорема об изоморфизме некоторых классов, не являющихся множествами, и класса ординалов, а теорема об алефах является лишь ее частным случаем благодаря аксиоме выбора.

Теорема 3.11. (Об изоморфизме классов).
Пусть собственно класс $\mathcal{K}$ вполне упорядочен отношением-классом $\prec$ и удовлетворяет условию:

$$\text{для каждого } y \in \mathcal{K} \text{ класс } \{x \in \mathcal{K} : x \prec y\} \text{ есть множество.}$$

Тогда классы $\mathcal{K}$ и Ord изоморфны (т. е. можно определить взаимно однозначное отображение из $\mathcal{K}$ в Ord, сохраняющее порядок).

В частности, *Любые два собственно класса ординалов порядково изоморфны.*

Мы не будем приводить здесь доказательство этой теоремы, т. к. оно практически повторяет доказательство теоремы об алефах и использует построение необходимого отображения по трансфинитной рекурсии. Мы предлагаем читателю попробовать доказать приведенную только что теорему.

§ 3.2 Конечные и бесконечные множества. Континуум-гипотеза

Мы уже довольно часто пользовались понятиями конечного и бесконечного множества, и даже определили конечные и бесконечные кардиналы. Введем теперь определение для произвольных множеств.

Определение 3.4. Множество X называется *бесконечным*, если оно обладает бесконечной мощностью, т. е. существует кардинал τ: $\tau = ||X||$, $\tau \geqslant \omega$. Множество X называется *конечным*, если оно обладает конечной мощностью, т. е. существует n: $n = ||X||$.

Множество X называется *счетным*, если $||X|| = \omega$.

Множество X называется *не более чем счетным*, если $||X|| \leqslant \omega$.

Каждое множество либо конечно, либо бесконечно, либо утверждение о существовании его мощности недоказуемо в ZF. Аксиома выбора позволяет исключить этот третий случай и говорить, что каждое множество либо конечно, либо бесконечно. Бесконечные множества обладают следующим свойством, отличающим их от конечных.

Теорема 3.12. *Если X — бесконечное множество, то для любого множества a мощности множеств $X \setminus \{a\}$, X и $X \cup \{a\}$ равны.*

Доказательство. Пусть $||X|| = \tau$, $\tau \geqslant \omega$, и пусть $a \notin X$. Нетрудно показать, что множество $X \cup \{a\}$ равномощно тогда ординалу $S(\tau)$. Между ординалом $S(\tau)$ и τ легко установить взаимно однозначное соответствие, как мы это уже делали при доказательстве свойства 3.1 кардиналов. Поэтому $||X \cap \{a\}|| = \tau$. Для $a \in X$ теорема очевидным образом справедлива.

Пусть теперь $Y = X \setminus \{a\}$, $a \in X$. Понятно, что используя полное упорядочение X, которое можно задать при помощи взаимно однозначного соответствия множества X и кардинала τ, можно вполне упорядочить и множество Y. Поэтому мощность Y существует. Если Y конечно, то понятно, что X тогда также конечно — противоречие. Если Y бесконечно, то по только что доказанному мы получим, что $||Y|| = ||Y \cup \{a\}||$, т. е. $||Y|| = ||X||$. При $a \notin X$ теорема также очевидна. □

Итак, мы видим, что при «выбрасывании» одной (или нескольких) точек из бесконечного множества мощность этого множества сохраняется. Таким образом, каждое бесконечное множество равномощно некоторому своему собственному подмножеству. На этом признаке базируется другое определение конечных и бесконечных множеств, принадлежащее Дедекинду.

Определение 3.5. Множество X называется *бесконечным по Дедекинду*, если оно равномощно некоторому своему собственному подмножеству, в противном случае множество X называется *конечным по Дедекинду*.

Определение Дедекинда не подразумевает наличия у множества мощности, и потому любое множество либо конечно по Дедекинду, либо бесконечно по Дедекинду. При выполнении аксиомы выбора оба определения совпадают, при отрицании AC могут существовать такие множества, которые не имеют мощности, но тем не менее бесконечны (или конечны) по Дедекинду. Оба эти факта вытекают из следующей теоремы.

Теорема 3.13. *Если множество X конечно, то оно конечно по Дедекинду. Если множество X бесконечно, то оно бесконечно по Дедекинду.*

Введем теперь обозначение: $\mathfrak{c} = ||\mathbb{R}||$, если существует мощность множества $\mathbb{R}$ всех вещественных чисел. Понятно, что $\mathbb{R}$ бесконечно по Дедекинду, ибо $\mathbb{R} \leftrightarrow [0,1]$, а если мы предполагаем существование мощности $\mathfrak{c}$ (мощности континуума), то $\mathbb{R}$ будет и просто бесконечно. В силу следствий к теореме Кантора мы можем сказать даже, что $\mathfrak{c} > \omega$, т. е. континуум несчетен. И здесь возникает новый вопрос: насколько вообще кардинал $\mathfrak{c}$ больше ω? Или: существуют ли множества мощности τ такой, что $\omega < \tau < \mathfrak{c}$?

Этот вопрос впервые был сформулирован Кантором в конце XIX века. Сам Кантор неоднократно пытался отыскать несчетное множество мощности меньше $\mathfrak{c}$, «прореживая» известные континуальные множества, строя нигде не плотные множества вещественных чисел. В результате появились канторовы совершенные множества, но все они оказались континуальными. На основании всех своих исследований Кантор предположил, что не существует такого множества. Его гипотеза в наших обозначениях формулируется в виде равенства $\omega^+ = \mathfrak{c}$, которое называется *гипотезой континуума* или *континуум-гипотезой* и обозначается CH.

Введем следующее обозначение: через 2^τ мы обозначим мощность множества $\mathrm{Exp}(\tau)$. Объясняется такое обозначение следующим образом. Когда мы определяли прямое произведение множеств в общем виде (см. § 1.6), мы ввели также понятие возведения множества A в степень-множество B, обозначая через A^B множество всех функций из B в A. Если мы теперь в качестве множества A рассмотрим ординал $2 = \{0, 1\}$, то 2^B будет множеством всех функций, определенных на B и принимающих значения 0 или 1. Нетрудно установить взаимно однозначное соответствие между 2^B и $\mathrm{Exp}(B)$, выбирая для каждой функции из 2^B прообраз единицы. Поэтому $||\,\mathrm{Exp}(B)|| = ||2^B||$, откуда и появилось обозначение: $2^{||B||} := ||\,\mathrm{Exp}(B)||$. В частном случае, когда $B = \tau$ получим, что мощность $\mathrm{Exp}(\tau)$ равна 2^τ.

Мы уже упоминали ранее, что мощность континуума такова же, как мощность множества всех подмножеств натурального ряда, т. е. $\mathfrak{c} = ||\,\mathrm{Exp}(\omega)||$ или, в силу наших обозначений, $\mathfrak{c} = 2^\omega$. Тогда континуум-гипотеза выражается равенством $\omega^+ = 2^\omega$.

Аналогично, рассматривая вместо кардинала ω произвольный бесконечный кардинал τ, сформулируем *обобщенную континуум-гипотезу* (GCH): $\tau^+ = 2^\tau$.

На сегодняшний день известно, что как континуум-гипотеза, так и обобщенная континуум-гипотеза не зависят как от аксиом ZF, так и от аксиом ZFC. Точнее, справедливы следующие теоремы.

Теорема 3.14. (Курт Гёдель, 1936).
$\mathrm{Con}(\mathsf{ZF}) \to \mathrm{Con}(\mathsf{ZF+CH})$, $\mathrm{Con}(\mathsf{ZF}) \to \mathrm{Con}(\mathsf{ZF+GCH})$,
$\mathrm{Con}(\mathsf{ZF}) \to \mathrm{Con}(\mathsf{ZFC+CH})$, $\mathrm{Con}(\mathsf{ZF}) \to \mathrm{Con}(\mathsf{ZFC+GCH})$.

Теорема 3.15. (Поль Коэн, 1963).

$\mathrm{Con}(\mathsf{ZF}) \to \mathrm{Con}(\mathsf{ZF}+\rceil\mathsf{CH})$, $\mathrm{Con}(\mathsf{ZF}) \to \mathrm{Con}(\mathsf{ZF}+\rceil\mathsf{GCH})$,
$\mathrm{Con}(\mathsf{ZF}) \to \mathrm{Con}(\mathsf{ZFC}+\rceil\mathsf{CH})$, $\mathrm{Con}(\mathsf{ZF}) \to \mathrm{Con}\,\mathsf{ZFC}+\rceil\mathsf{GCH})$.

Следует однако отметить, что GCH влечет аксиому выбора AC [7]. Отсюда следует, что теория ZF+GCH+$\rceil$AC противоречива. То есть мы не можем сказать, что AC не зависит от аксиом ZF+GCH. Более подробное рассмотрение проблем, связанных с доказательством непротиворечивости CH и GCH с аксиоматикой Цермело—Френкеля, можно найти у П. Коэна в [7] или в Справочной книге по математической логике [8].

Итак, кроме аксиомы выбора существуют и другие утверждения о свойствах множеств, которые можно сформулировать в рамках языка ZF, но невозможно ни доказать их, ни опровергнуть в ZF. На самом деле, в силу теоремы Гёделя о неполноте [4] таких утверждений можно найти бесконечно много. В § 3.5 мы рассмотрим еще несколько подобных утверждений.

§ 3.3 Предельные теоремы о мощностях. Теорема о квадрате

В этом параграфе все теоремы мы будем доказывать в теории ZFC. Первая теорема, которую мы здесь докажем, по сути является переформулировкой леммы Цорна.

$^\circ$**Теорема 3.16.** (Принцип сквозной цепи). *В любом частично упорядоченном множестве существует сквозная цепь.*

Доказательство. Пусть $(X,<)$ — частично упорядоченное множество. Предположим, что в X существует неограниченная непустая цепь C. Тогда эта цепь и будет сквозной, ибо для нее не существует элемента $a \in X$ такого, что при любом $c \in C$ имеем $c < a$.

Предположим теперь, что в X любая цепь ограничена. Тогда в силу леммы Цорна в X существует максимальный элемент a. Но тогда множество $\{a\}$ является сквозной цепью в X. □

Пусть C — цепь множеств по вложению, т. е. $(C,\subset)$ является линейно упорядоченным множеством. *Пределом* цепи C мы называем объединение $\cup C$ ее элементов. Ясно, что для любого $A \in C$ имеем $A \subseteq \cup C$, поэтому $||A|| \leqslant ||\cup C||$ для любого $A \in C$. Но как указать более точную оценку для мощности предела цепи C?

Следующая теорема позволяет нам ответить на этот вопрос.

°**Теорема 3.17.** (О мощности предела цепи). *Пусть C — цепь множеств по вложению и для каждого множества $A \in C$ имеем $||A|| < \tau$. Тогда $|| \cup C|| \leqslant \tau$.*

Доказательство. Пусть $X = \cup C$. Рассмотрим множество $\mathfrak{F}$ всех биекцией между множествами $A \in C$ и их мощностями $\xi < \tau$, а именно,

$$\mathfrak{F} = \{f : \ f : A \to \xi, \ A \in C, \ \xi < \tau, \ f \text{ — биекция}\}.$$

Ясно, что это множество не пусто. Кроме того, оно частично упорядочено отношением $\subset$. Так что в силу принципа сквозной цепи в $\mathfrak{F}$ существует сквозная цепь $\mathfrak{C}$. Обозначим $C' = \{\mathrm{dom}(f) : \ f \in \mathfrak{C}\}$. C' — непустая подцепь цепи C. Поскольку $\mathfrak{C}$ является цепью биекций, то ее предел $f_0 = \cup\mathfrak{C}$ также есть биекция между $\cup C' = \mathrm{dom}(f_0)$ и $\bigcup_{f\in\mathfrak{C}} \mathrm{ran}(f) = \mathrm{ran}(f_0)$. Ясно, что $\mathrm{dom}(f_0) \subseteq X$, $\mathrm{ran}(f_0) \subseteq \tau$.

Предположим теперь, что $\mathrm{dom}(f_0) \neq X$. Это означает, что в цепи C существует элемент A такой, что $A \not\subseteq \mathrm{dom}(f_0)$. Поскольку $\mathrm{dom}(f_0)$ — это предел цепи C', то очевидно также $A \not\subseteq B$ для каждого $B \in C'$. Но тогда в силу линейной упорядоченности C по вложению получаем, что для каждого $B \in C'$ имеет место $B \subset A$, откуда $\mathrm{dom}(f_0) \subseteq A$ и, более точно,

$$\mathrm{dom}(f_0) \subset A \tag{3.1}$$

ввиду предположения о том, что $A \not\subseteq \mathrm{dom}(f_0)$.

Покажем теперь, что $\mathrm{ran}(f_0)$ есть кардинал, меньший τ. Действительно, поскольку для каждого $f \in \mathfrak{C}$ имеем $\mathrm{ran}(f) \in \mathrm{Card}$, то $\mathrm{ran}(f_0) = \bigcup_{f\in\mathfrak{C}} \mathrm{ran}(f)$ также есть кардинал по свойству кардиналов 3.8. При этом

$$\mathrm{ran}(f_0) = ||\,\mathrm{dom}(f_0)|| \leqslant ||A|| < \tau. \tag{3.2}$$

Обозначим теперь $B = A \setminus \mathrm{dom}(f_0)$, $D = \tau \setminus \mathrm{ran}(f_0)$. Оба эти множества не пусты согласно (3.1) и (3.2). Если $||B|| \geqslant ||D||$, то существует инъекция из D в B. Тогда, используя биекцию f_0, нетрудно построить инъекцию из τ в A, откуда по теореме CBS получаем $||A|| = \tau$. Противоречие. Итак, $||B|| < ||D|| \leqslant \tau$. Пусть $h : B \to D$ — инъекция. Обозначим через α порядковый тип $\mathrm{ran}(h)$, $h_1 : \mathrm{ran}(h) \to [\mathrm{ran}(f_0); \mathrm{ran}(f_0) +_o \alpha)$ — порядковый изоморфизм, где через $+_o$ обозначена сумма ординалов. Индукцией нетрудно проверить, что для каждого $\beta \in \mathrm{ran}(h)$ имеет место $h_1(\beta) \leqslant \beta$. Тогда из того, что $\mathrm{ran}(h) \subseteq \tau$, следует, что $\mathrm{ran}(f_0) +_o \alpha \leqslant \tau$. Тогда, как нетрудно видеть, множество $f = f_0 \cup (h_1 \circ h)$ является биекцией между A и $\mathrm{ran}(f_0) +_o \alpha$.

Итак, $f \in \mathfrak{F}$ и f является верхней гранью для $\mathfrak{C}$, причем, $f \notin \mathfrak{C}$, т. к. $\mathrm{dom}(f) = A \supset \mathrm{dom}(f_0)$. Это противоречит тому, что цепь $\mathfrak{C}$ сквозная.

Итак, предположение о том, что $\mathrm{dom}(f_0) \neq X$, приводит к противоречию, следовательно, $\mathrm{dom}(f_0) = X$. Далее, поскольку f_0 — инъекция в τ, то $||X|| \leqslant \tau$, то и требовалось проверить. □

Условие теоремы $||A|| < \tau$ для каждого $A \in C$ существенно. Действительно, рассмотрим изолированный кардинал τ^+. Этот кардинал сам является цепью по вложению своих элементов-ординалов. Если кардинал τ бесконечный, то среди ординалов $\alpha \in \tau^+$, понятно, существуют ординалы мощности τ, причем, поскольку τ^+ является предельным ординалом, то τ^+ является пределом цепи своих элементов. Для каждого $\alpha \in \tau^+$ имеем $||\alpha|| \leqslant \tau$, но нестрого неравенства добиться нельзя, а мощность предела цепи τ^+ больше τ.

Следующая теорема позволяет представлять любое бесконечное множество в виде предела цепи его подмножеств меньшей мощности.

°**Теорема 3.18.** *Пусть X — бесконечное множество. Тогда найдется цепь C его подмножеств такая, что $\cup C = X$ и для любого $A \in C$ имеем $||A|| < ||X||$.*

Доказательство. Для бесконечного множества X рассмотрим множество $\mathcal{P}$ всех его подмножеств меньшей мощности, т. е.

$$\mathcal{P} = \{A \in \mathrm{Exp}(X) |\ ||A|| < ||X||\}.$$

Очевидно, что $\mathcal{P}$ не пусто и частично упорядочено отношением $\subset$. Тогда в $\mathcal{P}$ найдется сквозная цепь $\mathcal{E}$. Через A^* обозначим предел этой цепи. Очевидно, что $A^* \subseteq X$, поэтому $||A^*|| \leqslant ||X||$.

Предположим, что $||A^*|| < ||X||$. Тогда существует $a \in X \setminus A^*$. Рассмотрим множество $A_0 = A^* \cup \{a\}$. Если множество A^* конечное, то множество A_0 также конечное, откуда $||A_0|| < ||X||$. Если же множество A^* бесконечное, то $||A_0|| = ||A^*|| < ||X||$. Итак, в любом случае $A_0 \in \mathcal{P}$ и ограничивает цепь $\mathcal{E}$, не будучи элементом этой цепи, т. е. цепь $\mathcal{E}$ не может быть сквозной. Противоречие.

Поэтому $||A^*|| = ||X||$. Пусть $f : A^* \to X$ суть биекция. Построим цепь C как образ цепи $\mathcal{E}$ по функции f, т. е.

$$C = \{fA |\ A \in \mathcal{E}\}.$$

Нетрудно видеть, что в силу биективности f эти цепи порядково изоморфны по вложению. Кроме того, для любого $A \in \mathcal{E}$ имеем $||A|| = ||fA||$, поэтому все элементы цепи C имеют мощность меньше $||X||$. А поскольку $\cup C = f[\cup \mathcal{E}]$, то $\cup C = X$. Теорема доказана. □

Доказательство этой теоремы интересно тем, что его можно использовать в наивной теории множеств, т. к. мы не используем здесь определение кардинала и ординала по фон Нейману. С использованием теории ординалов и кардиналов в смысле фон Неймана эту теорему легко доказать, рассматривая биекцию между множеством X и кардиналом τ.

Из этой теоремы, в частности, следует, что отрезок $[0, 1] \subset \mathbb{R}$ можно представить как предел возрастающей цепи множеств мощности меньше $\mathfrak{c}$, а в случае принятия континуум-гипотезы, — счетных множеств. Эта цепь, разумеется, не может быть счетной, иначе мы бы пришли к противоречию, например, со счетной аддитивностью меры Лебега.

Следующая теорема позволяет нам вычислять мощности конечных прямых произведений бесконечных множеств.

°**Теорема 3.19.** (О квадрате). *Если τ — бесконечный кардинал, то $||\tau \times \tau|| = \tau$.*

Доказательство. Воспользуемся трансфинитной индукцией на классе бесконечных кардиналов.

Предположим, что для каждого бесконечного кардинала $\xi < \tau$, если таковой имеется, утверждение теоремы справедливо, т. е. $||\xi \times \xi|| = ||\xi||$, и покажем это равенство для τ.

Во-первых, отметим, что поскольку $||\alpha|| < \tau$ для любого ординала $\alpha < \tau$ (это следует из определения кардинала), то для каждого ординала $\alpha < \tau$ имеем $||\alpha \times \alpha|| = ||\alpha||$, если $\alpha \geqslant \omega$, и $||\alpha \times \alpha|| < \omega$, если α — натуральное число. В любом случае для $\alpha < \tau$ имеем $||\alpha \times \alpha|| < \tau$.

Во-вторых, кардинал τ есть предельный ординал, поэтому $\tau = \sup \tau = \bigcup\limits_{\alpha<\tau} \alpha$, откуда нетрудно получить, что

$$\tau \times \tau = \bigcup_{\alpha<\tau} \alpha \times \alpha,$$

т. е. множество $\tau \times \tau$ является пределом цепи множеств $\alpha \times \alpha$, где $\alpha < \tau$.

Теперь по теореме 3.17 о мощности предела цепи получаем, что $||\tau \times \tau|| \leqslant \tau$. С другой стороны, очевидно, что $||\tau \times \tau|| \geqslant \tau$, а значит, $\tau \times \tau$ имеет мощность τ. Теорема доказана. □

°**Следствие 3.20.** *Для любого бесконечного множества X имеем $||X \times X|| = ||X||$.*

°**Следствие 3.21.** *Если множество X бесконечно, а множество Y таково, что $||Y|| \leqslant ||X||$, то $||X \times Y|| = ||X||$.*

Доказательство. Поскольку $X \times Y \subseteq X \times X$, то очевидно, что $||X \times Y|| \leqslant ||X \times X|| = ||X||$. С другой стороны, $||X \times Y|| \geqslant ||X||$. □

°**Следствие 3.22.** *Если множество X бесконечно, $n \in \omega$, $n > 0$, то $||X^n|| = ||X||$, что несложно проверить математической индукцией по n.*

Как частный случай отметим, что $||\omega^n|| = \omega$, $||\mathbb{R}^n|| = \mathfrak{c}$, $n > 0$.

°**Теорема 3.23.** (О сумме). *Пусть имеется множество $\{X_i\}_{i\in I}$ и для каждого $i \in I$ имеем $||X_i|| \leqslant \tau$. Кроме того, $||I|| \leqslant \tau$, а кардинал τ бесконечный. Тогда*

$$\left\|\sum_I X_i\right\| \leqslant \tau, \quad \left\|\bigcup_{i\in I} X_i\right\| \leqslant \tau.$$

Доказательство. Поскольку $||X_i|| \leqslant \tau$ для каждого $i \in I$, то можно построить инъекции $f_i : X_i \to \tau$. Аналогично можно построить инъекцию $g : I \to \tau$. Теперь рассмотрим функцию $F : \sum\limits_I X_i \to \tau \times \tau$, определяемую следующей формулой: $F(i,x) = (g(i), f_i(x))$ для $(i,x) \in \{i\} \times X_i$. Нетрудно убедиться в том, что F есть инъекция из $\sum\limits_I X_i$ в $\tau \times \tau$. Поэтому

$$\left\|\sum_I X_i\right\| \leqslant ||\tau \times \tau|| = \tau.$$

Вторую часть утверждения теоремы легко доказать, построив сюръекцию из $\sum\limits_I X_i$ в $\bigcup\limits_{i\in I} X_i$. □

°**Следствие 3.24.** *Не более чем счетное объединение не более чем счетных множеств не более чем счетно.*

§ 3.4 Арифметика кардиналов

В § 2.3 мы изучали арифметику ординалов — сложение и умножение. Здесь мы намерены рассмотреть сложение, умножение и возведение в степень кардиналов. Поскольку для доказательства большинства равенств данного параграфа требуется существование мощностей рассматриваемых множеств, то все утверждения здесь мы будем считать теоремами ZFC, а не ZF, хотя некоторые свойства можно доказывать и без аксиомы выбора.

Пусть имеется множество кардиналов $\{\tau_i\}_{i\in A}$, проиндексированное множеством A.

Сложение.[3]

Через $\sum\limits_{i\in A}\tau_i$ обозначим мощность множества $\bigcup\limits_{i\in A}\{i\}\times\tau_i$.

Определение 3.6. Символ $\sum\limits_{i\in A}\tau_i$ называется *суммой кардиналов* τ_i по множеству A.

Для $A=\emptyset$ положим $\sum\limits_{i\in A}\tau_i=0$.

Для $||A||<\omega$ мы используем обычные математические обозначения суммы, например, $\sum\limits_{i=1}^{n}\tau_i$ или $\tau+\xi+\dots+\chi$.

Если мы обратим внимание на определение суммы ординалов, то увидим, что сумма кардиналов в смысле сложения ординалов (ведь кардиналы являются ординалами) вообще говоря отлична от суммы кардиналов, поэтому эти понятия следует различать. Кроме того, сумма кардиналов обладает гораздо бо́льшим числом обычных арифметических свойств сложения, чем сумма ординалов. Для натуральных чисел, как нетрудно проверить, сумма кардиналов совпадает с обычной суммой натуральных чисел. Рассмотрим некоторые свойства сложения кардиналов.

✓ **3.9.** (коммутативность) $\tau+\xi=\xi+\tau$.

✓ **3.10.** (обобщенная коммутативность) Если функция $f:A\to A$ является перестановкой множества A, т. е. биекцией из A в A, то

$$\sum_{i\in A}\tau_i=\sum_{i\in A}\xi_i,\ \text{где } \xi_i=\tau_{f(i)},$$

т. е. сумма кардиналов не зависит от перестановки слагаемых.

✓ **3.11.** (нейтральный элемент) $\tau+0=\tau$.

✓ **3.12.** (монотонность) Если $A\subseteq B$ и для $i\in A$ имеем $\tau_i\leqslant\xi_i$, то

$$\sum_{i\in A}\tau_i\leqslant\sum_{i\in B}\xi_i.$$

✓ **3.13.** (ассоциативность) $\tau+(\xi+\chi)=(\tau+\xi)+\chi$.

[3]Большинство свойств сложения, умножения и возведения в степень кардиналов приведены здесь без доказательств ввиду не особой их сложности. Эти доказательства можно найти, например, в [9, 14].

✓ **3.14.** (обобщенная ассоциативность) Если $A = \bigcup\limits_{j\in\lambda} B_j$ и для $j \neq j'$ имеем $B_j \cap B_{j'} = \emptyset$, то

$$\sum_{i\in A} \tau_i = \sum_{j\in\lambda} \left(\sum_{i\in B_j} \tau_i \right).$$

Из теоремы о сумме 3.23 нетрудно получить следующие свойства сложения кардиналов.

✓ **3.15.** $\tau + \xi = \max\{\tau, \xi\}$, если хотя бы один из кардиналов τ или ξ бесконечен.

✓ **3.16.** Если $\tau_i \leqslant \tau$ для любого $i \in A$ и $||A|| \leqslant \tau$, то $\sum\limits_{i\in A} \tau_i \leqslant \tau$.

✓ **3.17.** Если множество кардиналов $\{\tau_i\}_{i\in A}$ имеет максимум или $\tau_i \leqslant ||A||$ для любого $i \in A$ и, кроме того, хотя бы один из кардиналов $\sup_i \tau_i$ или $||A||$ бесконечен, то $\sum\limits_{i\in A} \tau_i = \max\{\sup\limits_i \tau_i, ||A||\}$.

Умножение.

Определение 3.7. *Произведением кардиналов* τ_i по множеству A при $A \neq \emptyset$ называется мощность прямого произведения кардиналов τ_i по множеству A:

$$\prod_{i\in A} \tau_i := \left\| \left\{ f \;\middle|\; (f : A \to \bigcup_{i\in A} \tau_i) \wedge (\forall i \in A : \; f(i) \in \tau_i) \right\} \right\|.$$

Для $A = \emptyset$ полагаем $\prod\limits_{i\in A} \tau_i = 1$.

Доопределение произведения в случае пустого множества A (как и суммы) производится лишь для единообразия записи формул арифметических равенств с кардиналами.

Произведение кардиналов, как и сумма, отличается от произведения ординалов как определением, так и свойствами. Для обозначения конечных произведений мы также будем использовать обычные математически символы такие, как $\prod\limits_{i=1}^{n} \tau_i$ или $\tau\xi\ldots\chi$.

Рассмотрим некоторые свойства произведения.

✓ **3.18.** (коммутативность) $\tau\xi = \xi\tau$.

✓ **3.19.** (обобщенная коммутативность) Если функция $f : A \to A$ является перестановкой множества A, то

$$\prod_{i\in A} \tau_i = \prod_{i\in A} \xi_i, \quad \xi_i = \tau_{f(i)},$$

т. е. произведение кардиналов не зависит от перестановки сомножителей.

✓ **3.20.** (нейтральный элемент) $\tau \cdot 1 = \tau$.

✓ **3.21.** (умножение на ноль) $\tau \cdot 0 = 0$ и, более общо, если при некотором $i \in A$ имеем $\tau_i = 0$, то $\prod\limits_{i\in A} \tau_i = 0$.

✓ **3.22.** (монотонность) Если $A \subseteq B$, для каждого $i \in A$ имеем $\tau_i \leqslant \xi_i$ и для $i \in B \setminus A$ имеем $\xi_i > 0$, то

$$\prod_{i\in A} \tau_i \leqslant \prod_{i\in B} \xi_i.$$

✓ **3.23.** (ассоциативность) $\tau(\xi\chi) = (\tau\xi)\chi$.

✓ **3.24.** (обобщенная ассоциативность) Если $A = \bigcup\limits_{j\in\lambda} B_j$ и для $j \neq j'$ имеем $B_j \cap B_{j'} = \emptyset$, то

$$\prod_{i\in A} \tau_i = \prod_{j\in\lambda} \left(\prod_{i\in B_j} \tau_i \right).$$

Из теоремы о квадрате 3.19 несложно получить следующее свойство.

✓ **3.25.** $\tau\xi \ldots \chi = \max\{\tau, \xi, \ldots, \chi\}$ для любого конечного набора кардиналов, если хотя бы один из них бесконечен и все они больше 0.

Следующие свойства отражают связь сложения и умножения кардиналов.

✓ **3.26.** Если для любого $i \in A$ $\tau_i = \tau$, то $\sum\limits_{i\in A} \tau_i = \tau \cdot ||A||$.

✓ **3.27.** (дистрибутивность) $(\tau + \xi)\chi = \tau\chi + \xi\chi$.

✓ **3.28.** (обобщенная дистрибутивность)

$$\left(\sum_{i\in A} \tau_i \right) \xi = \sum_{i\in A} (\tau_i \xi).$$

✓ **3.29.** (теорема Ю. Кенига) Если для $i \in A$ имеем $\tau_i < \xi_i$, то

$$\sum_{i\in A} \tau_i < \prod_{i\in A} \xi_i.$$

Доказательство. В соответствии с определениями суммы и произведения кардиналов рассмотрим множества

$$S = \bigcup_{i\in A} \{i\} \times \tau_i, \quad P = \left\{ f \;\middle|\; (f : A \to \bigcup_{i\in A} \xi_i) \wedge (\forall i \in A : \; f(i) \in \xi_i) \right\}.$$

Необходимо показать, что не верно $||S|| \geqslant ||P||$.

Для начала определим проектор $\pi_i : P \to \xi_i$, полагая $\pi_i(f) = f(i)$ для каждого $f \in P$. Рассмотрим произвольную функцию $t : S \to P$. Ее сужение $t|_{\{i\}\times\tau_i}$ есть функция из $\{i\} \times \tau_i$ в P, а суперпозиция $g_i = \pi_i \circ t|_{\{i\}\times\tau_i}$ является функцией из $\{i\} \times \tau_i$ в ξ_i. Поскольку $\tau_i < \xi_i$, то функция g_i не может быть сюръекцией, поэтому существует $x_i \in \xi_i$ такой, что для любого $z \in \tau_i$ не верно, что $g_i(i, z) = x_i$.

Рассмотрим функцию $f \in P$ такую, что для любого $i \in A \;\; f(i) = x_i$. Ясно, что при любых $(i, z) \in S$ не верно, что $t(i, z) = f$, т. к. иначе получилось бы, что $g_i(i, z) = x_i$ в противоречии с выбором x_i.

Итак, любая функция $t : S \to P$ не может быть сюръекцией, поэтому не верно, что $||S|| \geqslant ||P||$. Тогда $||S|| < ||P||$. □

Возведение в степень.

Определение 3.8. *Степенью* λ кардинала τ называется мощность множества всех функций из λ в τ, если кардиналы λ и τ отличны от нуля, обозначаемая τ^λ. Для остальных случаев полагаем: $\tau^0 = 1$, если $\tau > 0$, и $0^\lambda = 0$ при любом λ (в частности $0^0 = 0$).

Рассмотрим некоторые свойства степени.

✓ **3.30.** Если для любого $i \in A \;\; \tau_i = \tau$, то $\prod\limits_{i\in A} \tau_i = \tau^{||A||}$ при $A \neq \emptyset$.

✓ **3.31.** $\tau^{\lambda+\mu} = \tau^\lambda \cdot \tau^\mu$.

✓ **3.32.** $(\tau\xi)^\lambda = \tau^\lambda \cdot \xi^\lambda$.

✓ **3.33.** $(\tau^\lambda)^\mu = \tau^{\lambda\mu}$.

✓ **3.34.** Если $\tau \leqslant \xi$ и $\lambda \leqslant \mu$, то $\tau^\lambda \leqslant \xi^\mu$.

✓ **3.35.** $||\operatorname{Exp}(X)|| = 2^{||X||}$.

Это свойство свидетельствует о том, что введенное нами ранее обозначение 2^τ теперь приобрело арифметический смысл.

✓ **3.36.** По теореме Кантора $\tau < 2^\tau$.

✓ **3.37.** По теореме о квадрате $\tau^n = \tau$ для бесконечного τ.

✓ **3.38.** Если $2 \leqslant \tau \leqslant \lambda$ и $\omega \leqslant \lambda$, то $\tau^\lambda = 2^\lambda$.

Доказательство. $2^\lambda \leqslant \tau^\lambda \leqslant \lambda^\lambda \leqslant (2^\lambda)^\lambda = 2^{\lambda\cdot\lambda} = 2^\lambda$. □

Теперь мы вспомним про отображение $\aleph$, «нумерующее» ординалами кардиналы в порядке возрастания, и приведем следующие рекурсивные формулы.

°**Теорема 3.25.** (рекурсивная формула Хаусдорфа) *Для любых ординалов α, β и натурального числа n имеет место равенство:*

$$\aleph_{\alpha+n}^{\aleph_\beta} = \aleph_\alpha^{\aleph_\beta} \cdot \aleph_{\alpha+n},$$

где сумму $\alpha + n$ следует понимать как сумму ординалов.

Доказательство этой теоремы использует понятие конфинального характера кардинала (см. следующий параграф) и достаточно сложно, поэтому мы не приводим его здесь.[4]

Как следствие из этой теоремы (при $\alpha = 0$) нетрудно доказать рекурсивную формулу Бернштейна:

$$\aleph_n^{\aleph_\beta} = 2^{\aleph_\beta} \cdot \aleph_n.$$

§ 3.5 Типы кардиналов. Высшие аксиомы бесконечности

Ранее мы уже имели дело с двумя разновидностями (или типами) кардиналов — с изолированным кардиналом и предельным. В этом параграфе мы рассмотрим еще несколько типов кардиналов.

Пусть τ — бесконечный кардинал. Очевидно, что τ можно представить в виде суммы $\sum\limits_{i\in\lambda} \tau_i$, где кардиналы τ_i и λ не превосходят τ. При $\lambda = \tau$ можно даже положить $\tau_i = 1 < \tau$, а если при некотором i $\tau_i = \tau$, то можно положить $\lambda = 1 < \tau$. Более интересный случай возникает, когда мы хотим потребовать условие $\tau_i < \tau$ для любого $i \in \lambda$ и $\lambda < \tau$.

Определение 3.9. *Конфинальным характером* кардинала τ называется наименьший из кардиналов λ таких, что существует множество кардиналов $\{\tau_i\}_{i\in\lambda}$, $\tau_i < \tau$, удовлетворяющее равенству $\tau = \sum\limits_{i\in\lambda} \tau_i$.

Конфинальный характер кардинала τ обозначается $\mathrm{cf}(\tau)$.

Кардинал τ называется *регулярным*, если $\mathrm{cf}(\tau) = \tau$, в противном случае ($\mathrm{cf}(\tau) < \tau$) кардинал τ называется *сингулярным*.

Итак, мы разделили класс Card_ω бесконечных кардиналов на два подкласса — регулярных и сингулярных кардиналов. Например, кардинал ω регулярен, а кардинал $\aleph_\omega$ сингулярен.

°**Теорема 3.26.** *Если $\tau \geqslant \omega$, то τ^+ — регулярный.*

[4]Это доказательство можно найти в [9].

Доказательство. Предположим, что τ^+ сингулярен. Тогда $\tau^+ = \sum\limits_{i\in\lambda} \tau_i$, где $\tau_i < \tau^+$ и $\lambda < \tau^+$, $\lambda = \mathrm{cf}(\tau^+)$. Тогда $\tau_i \leqslant \tau$, $\lambda \leqslant \tau$, откуда $\sum\limits_{i\in\lambda} \tau_i \leqslant \tau^2 = \tau$. Противоречие. □

Если мы принимаем аксиому выбора, то благодаря этой теореме нетрудно показать, что класс регулярных кардиналов неограничен в классе Card, т. е. является собственно классом. Действительно, для каждого регулярного кардинала τ кардинал τ^+ также регулярен. Покажем, что и класс сингулярных кардиналов является собственно классом. Для произвольного кардинала $\aleph_\alpha$ мы можем рассмотреть последовательность кардиналов $\aleph_{\alpha+n}$ и кардинал $\aleph_{\alpha+\omega}$. Этот кардинал есть сумма всех кардиналов $\aleph_{\alpha+n}$, а потому $\mathrm{cf}(\aleph_{\alpha+\omega}) = \omega$, т. е. кардинал $\aleph_{\alpha+\omega}$ сингулярный. Это означает, что и класс сингулярных кардиналов неограничен в классе Card, и потому является собственно классом.

Из любого кардинала (и в частности сингулярного) можно довольно просто получить регулярный кардинал.

°**Теорема 3.27.** *Кардинал* $\mathrm{cf}(\tau)$ *регулярен при любом* $\tau \geqslant \omega$.

Доказательство. Очевидно, что $\mathrm{cf}(\tau) \geqslant \omega$, так что мы можем говорить о его регулярности.

Предположим, что $\mathrm{cf}(\tau)$ сингулярный. Введем обозначения: $\lambda = \mathrm{cf}(\tau)$, $\mu = \mathrm{cf}(\lambda)$. $\mu < \lambda \leqslant \tau$ по предположению. Тогда

$$\tau = \sum_{i\in\lambda} \tau_i, \quad \lambda = \sum_{j\in\mu} \lambda_j, \quad \tau_i < \tau, \quad \lambda_j < \lambda.$$

Используя закон обобщенной ассоциативности нетрудно проверить равенство

$$\tau = \sum_{j\in\mu} \sum_{k\in\lambda_j} \tau_{i(j,k)},$$

где $i(j,k)$ осуществляет взаимно однозначное соответствие между множеством $\bigcup\limits_{j\in\mu} \{j\} \times \lambda_j$ и кардиналом λ по определению суммы кардиналов.

Рассмотрим одно произвольное слагаемое $\xi_j = \sum\limits_{k\in\lambda_j} \tau_{i(j,k)}$. Очевидно, что $\xi_j \leqslant \tau$, т. к. $\tau_{i(j,k)} < \tau$ и $\lambda \leqslant \tau$. Если допустить $\xi_j = \tau$, то мы получим представление кардинала τ через меньшее, чем $\lambda = \mathrm{cf}(\tau)$, число слагаемых, что невозможно по определению $\mathrm{cf}(\tau)$. Поэтому $\xi_j < \tau$.

Но тогда имеем $\tau = \sum\limits_{j\in\mu}\xi_j$, т. е. вновь кардинал τ представлен в виде суммы с меньшим, чем $\lambda = \mathrm{cf}(\tau)$, числом слагаемых, ибо мы предположили, что $\mu < \lambda$. Противоречие.

Итак, $\mathrm{cf}(\mathrm{cf}(\tau)) = \mathrm{cf}(\tau)$, т. е. конфинальный характер регулярен. □

°**Теорема 3.28.** *Для любого* $\tau \in \mathrm{Card}_\omega$ *имеем* $\tau < \mathrm{cf}(2^\tau)$.

Доказательство. Пусть $\lambda = \mathrm{cf}(2^\tau)$, $2^\tau = \sum\limits_{i\in\lambda}\tau_i$, где $\tau_i < 2^\tau$ при любом $i \in \lambda$. Предположим, что $\lambda \leqslant \tau$.

Воспользуемся теперь теоремой Кенига, из которой следует, что

$$2^\tau = \sum_{i\in\lambda}\tau_i < (2^\tau)^\lambda = 2^{\tau\cdot\lambda} = 2^\tau,$$

что невозможно. Поэтому $\tau < \lambda$, т. е. $\tau < \mathrm{cf}(2^\tau)$. □

Из этой теоремы вытекает, что $\omega < \mathrm{cf}(\mathfrak{c})$, в частности множество $\mathbb{R}$ вещественных чисел невозможно представить как счетное объединение множеств мощности меньше $\mathfrak{c}$.

Если мы принимаем континуум-гипотезу, то $\mathrm{cf}(\mathfrak{c}) = \mathfrak{c}$, т. е. $\mathfrak{c}$ суть регулярный кардинал. Если мы принимаем обобщенную континуум-гипотезу, то каждый кардинал 2^τ регулярен.

Заметим, что конфинальный характер кардинала мы определяем через сумму кардиналов меньшей мощности. Это означает, что из существования кардинала τ мы можем доказать существование его конфинального характера, более того, все операции сложения кардиналов, не превосходящих τ, вполне определимы без аксиомы выбора лишь при условии существования кардинала τ. Поэтому наше определение регулярности и сингулярности кардинала допустимо формулировать в ZF.

Известно [8], что аксиоматике ZF не противоречат следующие утверждения:

а) $\mathfrak{c}$ — изолированный кардинал;

б) $\mathfrak{c}$ — сингулярный кардинал;

в) $\mathfrak{c}$ — предельный регулярный кардинал.

Рассмотрим еще несколько типов кардиналов.

Определение 3.10. Кардинал $\tau > \omega$ называется *слабо недостижимым*, если он предельный и регулярный.

Бесконечный кардинал τ называется *доминантным* (или *сильно предельным*), если для каждого кардинала $\xi < \tau$ имеем $2^\xi < \tau$.

Доминантный регулярный несчетный кардинал называется *сильно* (или *строго*) *недостижимым*.

Все сильно недостижимые кардиналы образуют подкласс класса ординалов, а потому могут быть «занумерованы» ординалами в порядке возрастания в силу теоремы 3.11. Эти кардиналы принято обозначать In_α, где α — ординал. Поскольку до сих пор не удалось доказать или опровергнуть существование строго недостижимых кардиналов, то утверждение о существовании In_0 называют аксиомой и обозначают SI (от Strong Inaccessibility). Кардинал In_0 мы будем называть далее первым строго недостижимым кардиналом.

Насколько безопасна SI в смысле непротиворечивости теории, полученной присоединением этой аксиомы к ZF или ZFC, не известно, однако справедлива следующая

Теорема 3.29. *Невозможно доказать, что аксиому* SI *невозможно опровергнуть* (*в символах:* $\mathrm{Con}(\mathsf{ZF}) \not\to \mathrm{Con}(\mathsf{ZF}+\mathsf{SI})$).

Но даже если принять аксиому существования первого строго недостижимого кардинала, то этого оказывается недостаточно для доказательства существования других строго недостижимых кардинальных чисел. Поэтому для каждого ординала α можно ввести свою аксиому SI_α о существовании α-го строго недостижимого кардинального числа.

Рассмотрим еще один тип кардиналов.

Определение 3.11. Кардинал τ называется *измеримым* (по У́ламу), если на нем можно определить *меру Улама*, т. е. такую функцию $\mathfrak{m} : \mathrm{Exp}(\tau) \to 2$, что

1) $\mathfrak{m}(\tau) = 1$;
2) для любого $\alpha < \tau$ имеем $\mathfrak{m}(\{\alpha\}) = 0$;
3) если $X = \{X_n\}_{n=0}^{\infty}$ — последовательность попарно непересекающихся подмножеств кардинала τ, то
$$\mathfrak{m}(\cup X) = \sum_{n=0}^{\infty} \mathfrak{m}(X_n).$$

На сегодняшний день не известно, противоречит ли утверждение о существовании измеримого кардинала аксиомам ZF. О величине первого измеримого кардинала, если таковой существует, можно судить по следующему результату Тарского.

Теорема 3.30. *Первое измеримое кардинальное число больше первого строго недостижимого.*

Существует еще несколько типов кардиналов.[5] Обо всех этих кардиналах известно только, что они намного больше всех тех кардиналов, существование которых можно доказать в ZF.

Аксиомы о существовании кардиналов таких специфических типов, как строго недостижимые или измеримые, возникшие в результате неудачных попыток доказать или опровергнуть существование таких кардиналов, называются *высшими аксиомами бесконечности*, т. к. постулируют существование очень больших кардиналов.

§ 3.6 Универсальные множества. Метод моделей

Подобно тому, как раньше, в главе 2 мы ввели класс специальных множеств — ординалов, заметно облегчивших понимание самой теории множеств, как позже мы вводили класс кардинальных чисел (в текущей главе), так теперь мы введем новый класс множеств, обладающих не менее интересными свойствами как с точки зрения теории множеств, так и с позиции математической логики.

Напомним обозначение из § 1.7: через $\mathfrak{V}$ мы обозначаем класс всех множеств.

Теорема 3.31. *Существует и единственно отображение $\mathcal{G}$ из Ord в $\mathfrak{V}$, удовлетворяющее свойствам:*

1) $\mathcal{G}(0) = \emptyset$;

2) $\mathcal{G}(\alpha) = \mathrm{Exp}(\mathcal{G}(\beta))$, *где* $\alpha = S(\beta)$;

3) $\mathcal{G}(\alpha) = \bigcup\limits_{\beta<\alpha} \mathcal{G}(\beta)$, *если* α *— предельный ординал.*

Доказательство. Построим отображение $\mathcal{F} : \mathrm{Exp}(\mathfrak{V}) \to \mathfrak{V}$ по следующему правилу: $\mathcal{F}(\emptyset) = \emptyset$ и для любого множества $A \neq \emptyset$

$$\mathcal{F}(A) = \begin{cases} \cup A, & \text{если } \cup A \notin A, \\ \mathrm{Exp}(\cup A), & \text{если } \cup A \in A. \end{cases}$$

По теореме о рекурсивных определениях существует отображение $\mathcal{G}$ из Ord в $\mathfrak{V}$ такое, что при любом $\alpha \in \mathrm{Ord}$

$$\mathcal{G}(\alpha) = \mathcal{F}(\mathcal{G}\alpha), \qquad \text{где} \quad \mathcal{G}\alpha = \{\mathcal{G}(\beta) |\ \beta < \alpha\}.$$

[5] См., например, [8].

Докажем трансфинитной индукцией, что для множеств $\mathcal{G}(\alpha)$ выполняются условия теоремы $1)-3)$. Действительно, $\mathcal{G}(0) = \mathcal{F}(\emptyset) = \emptyset$, так что при $\alpha = 0$ множество $\mathcal{G}(\alpha)$ удовлетворяет $1)-3)$.

Предположим, что условия $1)-3)$ выполнены для любого $\alpha < \Delta$. Теперь нам необходимо показать, что $\mathcal{G}(\Delta)$ также подчиняется этим условиям. В рамках нашего предположения докажем следующие свойства $\mathcal{G}(\alpha)$:

I. для любых множеств x, y и любого $\alpha < \Delta$ из $x \in y \in \mathcal{G}(\alpha)$ следует $x \in \mathcal{G}(\alpha)$;

II. для любых $\beta < \alpha < \Delta$ имеем $\mathcal{G}(\beta) \subseteq \mathcal{G}(\alpha)$.

Доказательство первого свойства проведем трансфинитной индукцией по $\alpha < \Delta$. Очевидно, что для $\alpha = 0$ это свойство справедливо. Предположим, что оно справедливо для любого $\beta < \alpha$.

Пусть $x \in y \in \mathcal{G}(\alpha)$. Возможны два случая:

а) $\alpha = S(\beta)$, откуда в силу нашего предположения $\mathcal{G}(\alpha) = \mathrm{Exp}(\mathcal{G}(\beta))$. Тогда $y \subseteq \mathcal{G}(\beta)$, откуда $x \in \mathcal{G}(\beta)$. Для любого $z \in x$ по предположению индукции имеем $z \in \mathcal{G}(\beta)$, откуда следует $x \subseteq \mathcal{G}(\beta)$, т.е. $x \in \mathcal{G}(\alpha)$.

б) α — предельный. Тогда $\mathcal{G}(\alpha) = \bigcup\limits_{\beta<\alpha} \mathcal{G}(\beta)$, откуда существует β такое, что $y \in \mathcal{G}(\beta)$. В силу предположения индукции получим $x \in \mathcal{G}(\beta)$, откуда $x \in \mathcal{G}(\alpha)$.

Итак, свойство I доказано. Теперь покажем справедливость свойства II. Доказательство также проведем трансфинитной индукцией по ненулевым $\alpha < \Delta$. Очевидно, что при $\alpha = 1$ утверждение истинно, т.к. $\mathcal{G}(0) = \emptyset \subseteq \mathcal{G}(1)$. Пусть оно истинно для всех $\alpha < \alpha_0$. Возможны два варианта:

а) $\alpha_0 = S(\alpha)$. Тогда $\mathcal{G}(\alpha_0) = \mathrm{Exp}(\mathcal{G}(\alpha))$, т.е. $\mathcal{G}(\alpha) \in \mathcal{G}(\alpha_0)$, откуда в силу свойства I $\mathcal{G}(\alpha) \subseteq \mathcal{G}(\alpha_0)$. А по предположению индукции $\mathcal{G}(\beta) \subseteq \mathcal{G}(\alpha)$ при любом $\beta < \alpha$. Тогда и при любом $\beta < \alpha_0$ получим $\mathcal{G}(\beta) \subseteq \mathcal{G}(\alpha_0)$.

б) α_0 — предельный. Тогда $\mathcal{G}(\alpha_0) = \bigcup\limits_{\beta<\alpha_0} \mathcal{G}(\beta)$, откуда очевидно $\mathcal{G}(\beta) \subseteq \mathcal{G}(\alpha_0)$ при любом $\beta < \alpha_0$.

Итак, свойство II доказано. Вернемся к доказательству свойств $1)-3)$ для ординала Δ. Здесь снова рассмотрим два возможных варианта:

а) $\Delta = S(\delta)$. В силу доказанного свойства II легко показать, что

$$\bigcup_{\gamma<\Delta} \mathcal{G}(\gamma) = \mathcal{G}(\delta),$$

откуда по определению отображения $\mathcal{F}$ имеем $\mathcal{G}(\Delta) = \mathrm{Exp}(\mathcal{G}(\delta))$.

б) Δ — предельный. Если предположить, что $\bigcup\limits_{\gamma<\Delta} \mathcal{G}(\gamma) \in \mathcal{G}\Delta$, то существует γ_0 такой, что $\bigcup\limits_{\gamma<\Delta} \mathcal{G}(\gamma) = \mathcal{G}(\gamma_0)$. Так как Δ суть предельный ординал, то $S(\gamma_0) < \Delta$. В то же время $\mathcal{G}(S(\gamma_0)) = \mathrm{Exp}(\mathcal{G}(\gamma_0))$ по предположению индукции, откуда заключаем, что $\mathrm{Exp}(\mathcal{G}(\gamma_0)) \subseteq \mathcal{G}(\gamma_0)$, что невозможно. Итак,

$$\bigcup_{\gamma<\Delta} \mathcal{G}(\gamma) \notin \mathcal{G}\Delta,$$

поэтому $\mathcal{G}(\Delta) = \mathcal{F}(\mathcal{G}\Delta) = \bigcup\limits_{\gamma<\Delta} \mathcal{G}(\gamma)$.

Итак, для $\alpha = \Delta$ условия $1)-3)$ также справедливы. Следовательно, $\mathcal{G}(\alpha)$ и есть искомое отображение.

Докажем его единственность. Допустим, что отображение $\mathcal{H}(\alpha)$ также удовлетворяет $1)-3)$. Найдем наименьший из ординалов, для которых $\mathcal{G}(\alpha) \neq \mathcal{H}(\alpha)$ и обозначим его Δ. Ясно, что $\Delta > 0$, т.к. $\mathcal{G}(0) = \emptyset = \mathcal{H}(0)$. Если $\Delta = S(\delta)$, то

$$\mathcal{G}(\Delta) = \mathrm{Exp}(\mathcal{G}(\delta)) = \mathrm{Exp}(\mathcal{H}(\delta)) = \mathcal{H}(\Delta).$$

Противоречие. Если Δ — предельный, то

$$\mathcal{G}(\Delta) = \bigcup_{\gamma<\Delta} \mathcal{G}(\gamma) = \bigcup_{\gamma<\Delta} \mathcal{H}(\gamma) = \mathcal{H}(\Delta).$$

Противоречие. Итак, отображение $\mathcal{G}(\alpha)$ единственно. Теорема доказана. □

Определение 3.12. В дальнейшем условимся вместо $\mathcal{G}(\alpha)$ писать $\mathfrak{V}_\alpha$. Всякое множество $\mathfrak{V}_\alpha$ мы будем называть *α-ым универсальным множеством* или, короче, *α-ым универсумом* или *универсумом*, а класс

$$\mathfrak{U} = \{\mathfrak{V}_\alpha |\ \alpha \in \mathrm{Ord}\}$$

всех универсумов будем называть *универсальным классом*.

Следствие 3.32. *Из приведенного доказательства теоремы легко видеть, что построенное отображение $\mathcal{G}(\alpha)$ строго монотонно, т. е. для любых $\alpha < \beta$ имеем $\mathcal{G}(\alpha) \subset \mathcal{G}(\beta)$ или, в силу наших обозначений, $\mathfrak{V}_\alpha \subset \mathfrak{V}_\beta$.*

Следствие 3.33. *Если $x \in \mathfrak{V}_\alpha$, то $x \subseteq \mathfrak{V}_\alpha$.*

Доказательство. Пусть $x \in \mathfrak{V}_\alpha$. В силу предыдущего следствия $x \in \mathfrak{V}_{S(\alpha)} = \mathrm{Exp}(\mathfrak{V}_\alpha)$. Тогда $x \subseteq \mathfrak{V}_\alpha$. □

Следующая теорема выражает одно из основных свойств универсумов и одновременно показывает, что класс $\mathfrak{U}$ не является множеством.

Теорема 3.34. *Для каждого множества X найдется такой ординал α, что $X \subseteq \mathfrak{V}_\alpha$.*

Доказательство. Допустим, что это не так, т. е. существует множество X, не содержащееся ни в одном универсуме. Очевидно, $X \neq = \emptyset$. Пользуясь теоремой о рекурсивных определениях, можно задать функцию $f : \omega \to \mathfrak{V}$, удовлетворяющую равенствам:

$$f(0) = X, \quad f(n+1) = \cup f(n), \quad n \in \omega.$$

Обозначим далее через $T(X)$ объединение области значений функции f. Понятно, что $T(X)$ есть множество (это множество называют *транзитивным замыканием множества* X). Поскольку из того, что $Y \in f(n)$, следует $Y \subseteq f(n+1)$, то для всякого множества $Y \in T(X)$ имеем $Y \subseteq T(X)$, т. е. множество $T(X)$ транзитивно (см. определение 1.9). Кроме того, очевидно, $X \subseteq T(X)$, откуда в частности следует, что множество $T(X)$ не пусто. Рассмотрим теперь множество

$$M = \{Y \in T(X) \cup \{X\} | \; \forall \alpha \in \mathrm{Ord} : \; Y \not\subseteq \mathfrak{V}_\alpha\}.$$

Понятно, что $X \in M$, поэтому M не пусто. Тогда по аксиоме регулярности существует $Z \in M$ такое, что $Z \cap M = \emptyset$. Из транзитивности $T(X)$ следует, что $Z \subseteq T(X)$. Очевидно, $Z \neq \emptyset$, ибо для пустого множества имеем $\emptyset \subseteq \mathfrak{V}_0$, а потому $\emptyset \notin M$. Нетрудно видеть, что для каждого $z \in Z$ существует ординал α такой, что $z \in \mathfrak{V}_\alpha$.[6]

На множестве Z зададим функцию $r(z)$, ставящую в соответствие элементу $z \in Z$ наименьший из таких ординалов α, что $z \in \mathfrak{V}_\alpha$. Теперь через β обозначим $\sup\limits_{z \in Z} r(z)$. Покажем, что $Z \subseteq \mathfrak{V}_\beta$. Действительно, пусть $z \in Z$. Тогда $r(z) \leqslant \beta$, откуда в силу монотонности универсумов по вложению (следствие 3.32) получим $\mathfrak{V}_{r(z)} \subseteq \mathfrak{V}_\beta$. Но тогда $z \in \mathfrak{V}_\beta$. Таким образом, $Z \subseteq \mathfrak{V}_\beta$, что противоречит тому, что $Z \in M$. □

В силу теоремы 3.34 корректно следующее

Определение 3.13. *Рангом множества* X называется наименьший ординал α такой, что $X \subseteq \mathfrak{V}_\alpha$. Ранг множества X обозначим $rank(X)$.

[6]Действительно, $z \in Z$, поэтому $z \in T(X)$, но тем не менее $z \notin M$, поэтому существует α такой, что $z \subseteq \mathfrak{V}_\alpha$, тогда $z \in \mathfrak{V}_{S(\alpha)}$.

В частности $\emptyset$ есть множество 0-го ранга, натуральное порядковое число n есть множество n-го ранга, ординал ω есть множество ранга ω. Вообще, для любого ординала α его рангом будет он сам.[7]

Теорема 3.35. *Если τ — строго недостижимый кардинал, то для любого $\alpha < \tau$ имеем $||\mathfrak{V}_\alpha|| < \tau$, если только указанная мощность существует.*

Доказательство. Допустим, что это не так, и через α обозначим наименьший ординал такой, что $||\mathfrak{V}_\alpha|| \geqslant \tau$, $\alpha < \tau$. Очевидно, что $\alpha > 0$, поэтому α либо последующий, либо предельный. Заметим также, что из существования мощности $\mathfrak{V}_\alpha$ следует существование мощностей всех универсумов $\mathfrak{V}_\beta$, $\beta < \alpha$, поскольку $\mathfrak{V}_\beta \subseteq \mathfrak{V}_\alpha$.

1) Пусть $\alpha = S(\beta)$. Но тогда $\mathfrak{V}_\alpha = \mathrm{Exp}(\mathfrak{V}_\beta)$, откуда нетрудно получить, что $||\mathfrak{V}_\alpha|| = 2^\xi$, где $\xi = ||\mathfrak{V}_\beta||$. В силу выбора ординала α мощность β-го универсума меньше τ, т. е. $\xi < \tau$. Но тогда из доминантности τ следует $2^\xi < \tau$ в противоречии с тем, что $||\mathfrak{V}_\alpha|| \geqslant \tau$.

2) Пусть теперь α предельный. Тогда $\mathfrak{V}_\alpha = \bigcup\limits_{\beta<\alpha} \mathfrak{V}_\beta$. Поскольку $||\mathfrak{V}_\alpha|| \geqslant \tau$, то существует инъекция $f : \tau \to \mathfrak{V}_\alpha$. Обозначим $X_\beta = \{\gamma \in \tau |\ f(\gamma) \in \mathfrak{V}_\beta\}$, $\beta < \alpha$, — прообраз универсума $\mathfrak{V}_\beta$ относительно функции f. Понятно, что $||X_\beta||$ существует и $||X_\beta|| \leqslant ||\mathfrak{V}_\beta|| < \tau$ в силу выбора α. Тогда $\tau = \bigcup\limits_{\beta<\alpha} X_\beta$. Отсюда и из теоремы о сумме мощностей вытекают неравенства:

$$\tau \leqslant \sum_{\beta<\alpha} ||X_\beta|| \leqslant \tau ||\alpha|| = \tau,$$

что противоречит регулярности кардинала τ. □

Теперь мы установим один немаловажный факт из математической логики, касающийся совместности теорий ZFC и ZFC+SI. Именно, методом построения модели мы докажем в следующей теореме, что совместность теории ZFC+SI влечет совместность ZFC. Этот пример приводится здесь не только как математический результат, он также является наглядной иллюстрацией метода доказательства относительной непротиворечивости формальных аксиоматических теорий путем построения модели.

Поясним коротко суть метода моделей. Пусть у нас имеется формальная аксиоматическая теория (далее просто теория) T в языке первого порядка (как, например, ZF), определенная своими атомар-

---

[7] Мы предлагаем читателю проверить этот факт, пользуясь трансфинитной индукцией.

ными формулами $\varphi_1(x_1,\ldots,x_{k_1})$, ..., $\varphi_n(x_1,\ldots,x_{k_n})$ (а в теории множеств есть лишь единственная атомарная формула — принадлежность), константами и переменными (в теории ZF, аксиомы которой мы рассматривали в § 1.1, существует лишь один сорт переменных, названных нами множествами), а также набором замкнутых формул, называемым аксиоматикой этой теории.[8]

Определение 3.14. Мы говорим, что множество M *является моделью теории* T, если на множестве M заданы такие отношения $R_1(x_1,\ldots,x_{k_1}),\ldots,R_n(x_1,\ldots,x_{k_n})$, что при замене атомарных формул $\varphi_1,\ldots,\varphi_n$ теории T на отношения $R_1,\ldots,R_n$ соответственно и констант теории T на некоторые множества, принадлежащие M, аксиомы теории T становятся истинными утверждениями на множестве M (то есть при том условии, что все переменные в полученных аксиомах пробегают исключительно множество M).

Формулы, полученные в результате указанной замены атомарных формул и констант, называются *интерпретациями* формул теории T на множестве M.

Замечание 1. Наше определение модели теории имеет несколько более упрощенный вид, чем это обычно принято в книгах по математической логике (см., например, [3, 4]). Мы намеренно приводим такое определение, поскольку нам этого будет достаточно для доказательства приводимой ниже теоремы и в то же время это дает представление читателю о методе моделей доказательства непротиворечивости аксиоматических теорий.

В том случае, когда T есть аксиоматическая теория множеств (например, ZFC+SI), для построения модели нам необходимо лишь указать множество-модель и некоторое бинарное отношение R на этом множестве, которое будет интерпретировать отношение принадлежности в теории T. Часто в качестве такого отношения R берут само отношение принадлежности. Для удобства восприятия мы будем различать переменные в исходной теории T и переменные в модели (то есть переменные, пробегающие исключительно множество-модель). Для переменных в модели мы будем использовать малые готические буквы, в то время как переменные теории T, следуя идеологии § 1.1, будут обозначаться малыми латинскими буквами. Таким образом, если в качестве отношения R, моделирующего отношение принадлежности, мы выбираем само же отношение принадлежности, то атомарной формуле $x \in y$ теории T соответствует

[8]Более подробное и строгое изложение см. в [3], глава 2.

формула $\mathfrak{x} \in \mathfrak{y}$, в которой переменные $\mathfrak{x}, \mathfrak{y}$ пробегают исключительно множество M.

Предположим теперь, что мы построили модель M теории T. Если теория T противоречива, то в ней можно найти такую формулу φ, которая выводима в теории T вместе с ее отрицанием (т. е. $\rceil\varphi$ также выводима в T). Очевидно, в этом случае интерпретации формул φ и $\rceil\varphi$ выводимы в рамках модели M. Тогда модель M приводит к противоречию. Таким образом, из совместности теории множеств (ZFC, ZF, ZFC+SI, ZFC+CH и т. п.), в которой мы строили модель, вытекает и совместность теории T. Поскольку здесь совместность теории множеств, в которой строится модель теории T, играет основную роль при доказательстве непротиворечивости T, то совместность теории T называют *относительной*.

На сегодняшний день большинство результатов по непротиворечивости теорий являются именно относительными. При этом непротиворечивость самой исходной теории множеств (как правило это ZF или ZFC) считается истиной, ибо на протяжении нескольких десятилетий интенсивных исследований в ней не было получено ни одного парадокса.

Перейдем, наконец, к упомянутой выше теореме, в которой мы построим модель для теории ZFC в некоторой более сильной теории — ZFC+SI. Данная модель, понятно, является также и моделью ZF, однако в совместности ZF мы все же более уверены, чем в совместности ZFC+SI, поэтому не стоит считать данную теорему надежным доказательством непротиворечивости теории Цермело—Френкеля. Эта теорема является не более чем красивой и наглядной иллюстрацией метода моделей, описанного в данном параграфе.

$^\circ$**Теорема 3.36.** *Если τ — первое строго недостижимое кардинальное число, то $\mathfrak{V}_\tau$ — модель* ZFC *(в символах:* Con(ZFC+SI)$\to$ Con(ZFC)).

Доказательство. Итак, в соответствии с изложенной выше идеологией, предположим, что атомарной формуле $x \in y$ теории ZFC соответствует формула $\mathfrak{x} \in \mathfrak{y}$ теории ZFC+SI, где переменные $\mathfrak{x}$ и $\mathfrak{y}$ пробегают исключительно множество $\mathfrak{V}_\tau$. Теперь нам необходимо проверить справедливость аксиом ZFC (точнее, их интерпретаций) в универсуме $\mathfrak{V}_\tau$. По мере надобности мы будем вводить и другие готические буквы в качестве переменных, пробегающих множество $\mathfrak{V}_\tau$.

1) *Аксиома экстенсиональности.* Здесь нам следует проверить, что

$$(\mathfrak{x} = \mathfrak{y}) \to ((\mathfrak{x} \in \mathfrak{z}) \to (\mathfrak{y} \in \mathfrak{z})).$$

Пусть $x, y, z \in \mathfrak{V}_\tau$. По аксиоме экстенсиональности теории ZFC +SI (а она, понятно, имеет тот же вид, что и одноименная аксиома теории ZFC), получаем

$$(x = y) \to ((x \in z) \to (y \in z)),$$

а поскольку $x, y, z \in \mathfrak{V}_\tau$, то их можно заменить на $\mathfrak{x}, \mathfrak{y}, \mathfrak{z}$ соответственно, и тем самым получить требуемое утверждение.

2) *Аксиома пустого множества.* Формально нам следует проверить формулу

$$\exists \mathfrak{u}\, \forall \mathfrak{z}\; \mathfrak{z} \notin \mathfrak{u},$$

а фактически нам надо указать множество, пустое в $\mathfrak{V}_\tau$. Поскольку множество $\emptyset$, определяемое аксиомой пустого множества теории ZFC+SI, является элементом универсума $\mathfrak{V}_\tau$ (т. к. $\emptyset = \mathfrak{V}_0 \in \mathfrak{V}_\tau$ по свойствам универсумов), то оно, очевидно, не имеет элементов, принадлежащих $\mathfrak{V}_\tau$. Таким образом, $\emptyset$ — пустое в $\mathfrak{V}_\tau$, что и требовалось.

3) *Аксиома пары.* Теперь мы уже не будем придерживаться строго формального доказательства, чтобы не поглотить обилием логической символики суть доказательства теоремы. Итак, теперь нам надо проверить, что для любых множеств $\mathfrak{x}, \mathfrak{y} \in \mathfrak{V}_\tau$ пара $\{\mathfrak{x}, \mathfrak{y}\}$ также есть элемент $\mathfrak{V}_\tau$.

Поскольку τ есть предельный ординал, то $\mathfrak{V}_\tau = \bigcup\limits_{\alpha<\tau} \mathfrak{V}_\alpha$. Поэтому существует $\alpha < \tau$ такой, что $\mathfrak{x}, \mathfrak{y} \in \mathfrak{V}_\alpha$, откуда $\{\mathfrak{x}, \mathfrak{y}\} \subseteq \mathfrak{V}_\alpha$, откуда $\{\mathfrak{x}, \mathfrak{y}\} \in \mathrm{Exp}(\mathfrak{V}_\alpha) = \mathfrak{V}_{S(\alpha)}$. А поскольку $S(\alpha) < \tau$, то $\{\mathfrak{x}, \mathfrak{y}\} \in \mathfrak{V}_\tau$.

4) *Аксиома объединения.* Пусть $\mathfrak{x} \in \mathfrak{V}_\tau$. Покажем, что $\cup\mathfrak{x} \in \mathfrak{V}_\tau$. Аналогично предыдущему получаем, что $\mathfrak{x} \in \mathfrak{V}_\alpha$ при некотором $\alpha < \tau$. Поскольку $\mathfrak{x} \subseteq \mathfrak{V}_\alpha$ по следствию 3.33, то для каждого $\mathfrak{v} \in \mathfrak{x}$ имеем $\mathfrak{v} \in \mathfrak{V}_\alpha$ и, значит, $\mathfrak{v} \subseteq \mathfrak{V}_\alpha$. Поэтому $\cup\mathfrak{x} \subseteq \mathfrak{V}_\alpha$. Тогда $\cup\mathfrak{x} \in \mathfrak{V}_{S(\alpha)}$, откуда $\cup\mathfrak{x} \in \mathfrak{V}_\tau$.

5) *Аксиома степенного множества.* Пусть $\mathfrak{x} \in \mathfrak{V}_\tau$. Проверим, что $\mathrm{Exp}(\mathfrak{x}) \in \mathfrak{V}_\tau$. Вновь существует $\alpha < \tau$ такой, что $\mathfrak{x} \subseteq \mathfrak{V}_\alpha$. Поэтому $\mathrm{Exp}(\mathfrak{x}) \subseteq \mathfrak{V}_\alpha$ и, следовательно, $\mathrm{Exp}(\mathfrak{x}) \in \mathfrak{V}_{S(\alpha)}$, откуда $\mathrm{Exp}(\mathfrak{x}) \in \mathfrak{V}_\tau$.

6) *Схема аксиом содержательности.* Пусть $\varphi(x)$ — формула языка ZF со свободной переменной x. Ее интерпретацией на множестве $\mathfrak{V}_\tau$ является формула $\varphi(\mathfrak{x})$.[9] Пусть $\mathfrak{A} \in \mathfrak{V}_\tau$. Покажем тогда, что множество $\mathfrak{B} = \{\mathfrak{x} \in \mathfrak{A} |\ \varphi(\mathfrak{x})\}$ суть элемент универсума $\mathfrak{V}_\tau$.

[9] Поскольку в языке ZF (см. § 1.1) нет констант и других термов, кроме переменных, а атомарные формулы как в ZFC, так и в ZFC+SI (в интерпретации на множестве) имеют одинаковый вид, то для получения интерпретаций формул нам, понятно, достаточно лишь произвести соответствующую замену переменных.

При некотором $\alpha < \tau$ имеем $\mathfrak{A} \subseteq \mathfrak{V}_\alpha$, откуда нетрудно видеть, что множество $\mathfrak{B}$ есть элемент $\mathfrak{V}_{S(\alpha)}$. Поэтому $\mathfrak{B} \in \mathfrak{V}_\tau$.

7) *Аксиома регулярности.* Проверка этой аксиомы аналогична предыдущим.

8) *Схема аксиом подстановки.*[10] Эта схема аксиом говорит о следующем. Если имеется некая формула $\varphi(x, y)$ с двумя свободными переменными x, y, и на некотором множестве A данная формула определяет $(x \mapsto y)$-отображение, т. е. задает функцию, то область значений этого отображения (функции) есть множество.

Для проверки этой аксиомы в нашей модели теории ZFC нам необходимо проделать следующее. Вместо формулы $\varphi(x, y)$ мы рассмотрим формулу $\varphi(\mathfrak{x}, \mathfrak{y})$, в качестве множества A мы возьмем элемент $\mathfrak{A}$ универсума $\mathfrak{V}_\tau$, на котором φ определяет $(\mathfrak{x} \mapsto \mathfrak{y})$-отображение, и докажем, что область значений полученного отображения также есть элемент $\mathfrak{V}_\tau$.

Обозначим далее отображение, определяемое формулой φ, через $\mathfrak{f}$. Понятно, что $\mathfrak{f} : \mathfrak{A} \to \mathfrak{V}_\tau$. Понятно также, что $ran\,(\mathfrak{f}) \subseteq \mathfrak{V}_\tau$.[11] Необходимо показать, что $ran\,(\mathfrak{f}) \in \mathfrak{V}_\tau$.

Как и раньше, нетрудно получить, что при некотором $\alpha < \tau$ имеем $\mathfrak{A} \subseteq \mathfrak{V}_\alpha$. Отсюда, а также из AC и теоремы 3.35 вытекает, что $||\mathfrak{A}|| < \tau$. Рассмотрим функцию $\mathfrak{g} : \mathfrak{A} \to \tau$ такую, что $\mathfrak{g}(\mathfrak{a}) = rank(\mathfrak{f}(\mathfrak{a}))$. Обозначим через γ супремум всех $\mathfrak{g}(\mathfrak{a})$, $\mathfrak{a} \in \mathfrak{A}$. Ясно, что $\gamma \leqslant \tau$. Предположим, что $\gamma = \tau$. Тогда кардинал τ представим как объединение меньших его ординалов в числе $||\mathfrak{A}||$. Отсюда нетрудно получить, что

$$\tau = \sum_{\mathfrak{a} \in \mathfrak{A}} ||\mathfrak{g}(\mathfrak{a})||, \quad ||\mathfrak{g}(\mathfrak{a})|| < \tau.$$

Получено противоречие с регулярностью кардинала τ. Поэтому $\gamma < \tau$. Теперь, поскольку для каждого $\mathfrak{a} \in \mathfrak{A}$ имеем $\mathfrak{f}(\mathfrak{a}) \subseteq \mathfrak{V}_{rank(\mathfrak{f}(\mathfrak{a}))}$, то для каждого $\mathfrak{a} \in \mathfrak{A}$ в силу монотонности $\mathfrak{V}_\beta$ по β получаем $\mathfrak{f}(\mathfrak{a}) \subseteq \mathfrak{V}_\gamma$ и, следовательно, $\mathfrak{f}(\mathfrak{a}) \in \mathfrak{V}_{S(\gamma)}$. Но тогда $ran\,(\mathfrak{f})$ принадлежит к универсуму $\mathfrak{V}_{S(S(\gamma))}$, который в силу предельности ординала τ, есть подмножество универсума $\mathfrak{V}_\tau$.

Итак, $ran\,(\mathfrak{f}) \in \mathfrak{V}_\tau$.

9) *Аксиома бесконечности.* Справедливость этой аксиомы в нашей модели вытекает из того, что $\omega \subseteq \mathfrak{V}_\omega$, т. е. $\omega \in \mathfrak{V}_{S(\omega)}$, а значит, $\omega \in \mathfrak{V}_\tau$.

10) Справедливость интерпретации аксиомы выбора на множестве $\mathfrak{V}_\tau$ очевидна в силу того, что аксиома выбора присутствует в

[10] Здесь и только здесь мы используем строгую недостижимость кардинала τ и аксиому выбора!

[11] Напомним, что через $ran\,(\mathfrak{f})$ обозначается область значений функции $\mathfrak{f}$.

теории ZFC+SI и тем самым обеспечивает существование функции выбора на любом элементе универсума $\mathfrak{V}_\tau$.

Итак, множество $\mathfrak{V}_\tau$ является моделью теории ZFC. Теорема доказана. □

Построенная модель теории ZFC примечательна по крайней мере по трем причинам. Во-первых, это модель на множестве. Ведь пользуясь определением построения модели мы могли бы получить импликацию Con(ZFC+SI)→Con(ZFC) более простым путем, а именно, указав тождественное соответствие формул в этих теориях (при этом моделью теории ZFC в ZFC+SI стало бы уже не множество, а класс всех множеств $\mathfrak{V}$, на вывод указанной импликации это ничуть не повлияло бы). Однако модель на множестве всегда более привлекательна с точки зрения математической логики, особенно, если множество-модель воспринимается в интуитивном смысле. Кроме того, эта же модель является, очевидно, моделью теории GB+AC,[12] поскольку в качестве интерпретации класса на данной модели достаточно брать некоторое подмножество множества $\mathfrak{V}_\tau$.

Во-вторых, аксиома выбора в ZFC+SI дает возможность построить функцию выбора на всем универсуме $\mathfrak{V}_\tau$. А это означает, что $\mathfrak{V}_\tau$ является моделью для более сильной теории, чем GB+AC, — для теории GB+GC, где посредством GC мы обозначаем *аксиому глобального выбора*, утверждающую, что существует отображение $\mathfrak{C}$ класса $\mathfrak{V}$ в класс $\mathfrak{V}$ такое, что для каждого непустого множества X имеем $\mathfrak{C}(X) \in X$. Таким образом, аксиома глобального выбора совместима с теорией множеств и классов (теорией GB), если только с ZF совместимы одновременно AC и SI (в символах: Con(ZFC+SI)→Con(GB +GC)).

В-третьих, поскольку $\tau \notin \mathfrak{V}_\tau$ ($\tau = \mathrm{In}_0$), в модели $\mathfrak{V}_\tau$ истинно отрицание SI. Следует также отметить, что определение строго недостижимого кардинального числа, принадлежащего универсуму, равносильно этому же определению с условием, что все переменные, участвующие в определении, пробегают исключительно данный универсум. Это нетрудно установить, пользуясь транзитивностью универсума. Таким образом, если аксиома SI совместна с ZFC, то и ее отрицание также совместно с ZFC (Con(ZFC+SI)→Con(ZFC+⌉SI)), т. е. SI в этом случае не зависит от аксиом ZFC.

[12]Теория GB — это теория Гёделя—Бернайса [7], являющаяся расширением теории ZF. GB включает конечное число аксиом (в отличие от ZF, в которой присутствуют схемы аксиом), но содержит два сорта переменных — множества и классы. Эта теория формализует понятие класса, описанное нами в § 1.7. Известно [7], что утверждение Con(ZF) равносильно утверждению Con(GB).

Литература

1. Кантор Г. *Труды по теории множеств*, М., «Наука», 1985.
2. Архангельский А. В. *Канторовская теория множеств*, МГУ, 1988.
3. Колмогоров А. Н., Драгалин А. Г. *Введение в математическую логику*, М., Изд-во Моск. ун-та, 1982.
4. Колмогоров А. Н., Драгалин А. Г. *Математическая логика. Дополнительные главы*, М., Изд-во Моск. ун-та, 1984.
5. Гильберт Д. *Основания геометрии*, М.-Л., Гостехиздат, 1948.
6. Гильберт Д., Бернайс П. *Основания математики*, пер. с нем., М., «Наука», 1982.
7. Коэн П. *Теория множеств и континуум-гипотеза*, пер. с англ., М., «Мир», 1969.
8. *Справочная книга по математической логике* в 4-х частях/Под ред. Дж. Барвайса, Ч.2 *Теория множеств*, М., «Наука», 1982.
9. Куратовский К., Мостовский А. *Теория множеств*, пер. с англ., М., 1970.
10. Йех Т. *Теория множеств и метод форсинга*, М., «Мир», 1973.
11. Кановей В. Г. *Аксиома выбора и аксиома детерминированности*, М., «Наука», 1984.
12. Колмогоров А. Н., Фомин С. В. *Элементы теории функций и функционального анализа*, М., «Наука», 1976.
13. Хенл Дж. *Введение в теорию множеств*, пер. с англ., М., «Радио и связь», 1993.
14. Александров П. С. *Введение в теорию множеств и общую топологию*, М., 1977.

Указатель обозначений

$\{x_i\}_{i\in I}$	множество, проиндексированное множеством I 22
$[a]_\sim, [a]$	класс эквивалентности элемента a 23
$A/_\sim$	фактор-множество множества A по отношению эквивалентности $\sim$ 23
$<$	частичное, линейное или вполне упорядочение на множестве или классе 23, 40, 65
$a \leqslant b$	то же, что $a < b \vee a = b$ 23
$(A, <)$	частично, линейно или вполне упорядоченное множество 23
$\sup B, \inf B$	точная верхняя и нижняя грани множества B 23
$\max B, \min B$	максимум и минимум множества B 23
$[a; b]$	отрезок 25
$[a; b), (a; b]$	полуинтервал 25
$(a; b)$	интервал 25
ω	множество натуральных чисел, наименьший бесконечный кардинал 25
$0, 1, 2, 3$	обозначения натуральных чисел 28
$n+1$	натуральное число, следующее за n 28
$\sum\limits_C L_x$	прямая сумма множеств L_x по множеству C 28
$\prec$	каноническое упорядочение на прямой сумме или прямом произведении множеств 28, 30
$\prod\limits_C L_x$	прямое произведение множеств L_x по множеству C 29
$\mathbb{R}$	множество вещественных чисел 30
$\mathbb{R}^n$	множество всех n-ок вещественных чисел 30
2^ω	множество всех булевых (двоичных) последовательностей 30
$\mathfrak{V}$	класс всех множеств 33
Ord	класс всех ординалов 37
$>, \geqslant$	симметричные обозначения для $<$ и $\leqslant$ 40
$\lvert(X, <)\rvert$	порядковый тип вполне упорядоченного множества $(X, <)$ 44
$\sum\limits_{\delta\in\Delta} \alpha_\delta$	сумма ординалов α_δ в порядке Δ 47
$\prod\limits_{\delta\in\Delta} \alpha_\delta$	произведение ординалов α_δ в порядке Δ 47, 51
$\mathrm{co}_1(a, b)$ $\mathrm{co}_2(a, b)$	левая и правая координаты упорядоченной пары множеств a и b 49
$\pi_1 B, \pi_2 B$	левая и правая проекции множества B в прямом произведении двух множеств 49
Ord_1	класс ненулевых ординалов 49
$\Delta!$	факториал ординала Δ 51
AC	аксиома выбора 52
$\mathrm{Con}(T)$	утверждение о совместности теории T 52
ZFC	теория Цермело—Френкеля с аксиомой выбора 52

Предметный указатель

Николай Игоревич Казимиров

ВВЕДЕНИЕ В АКСИОМАТИЧЕСКУЮ ТЕОРИЮ МНОЖЕСТВ

Редактор

Подписано к печати xx.xx.2000.
Формат $60 \times 90\frac{1}{16}$
Бумага типографская №1.
Гарнитура литературная. Высокая печать.
Усл. печ. л. 6.9   Уч.-изд. л. 7
Тираж xxx экз.

Издательство (не опр.)