ФИВТ МФТИ, весна 2014.

Краткие заметки по курсу *математическая логика.* Часть первая: трансфинитная индукция. Исправленный вариант[1].

А.Е. Ромащенко.

Заметки написаны для студентов, слушавших лекции курса и посещавших семинары на факультете ИВТ Физтеха. Текст непригоден для использования в качестве самостоятельного учебного пособия, независимого от занятий.

В начале заметок доказательства излагаются очень подробно. В последних главах окончание некоторых доказательств предоставляется читателям в качестве упражнений.

1 Фундированные множества.

Мы рассматриваем три эквивалентных определения *фундированных* множеств:

Определение 1. Частично упорядоченное множество $(A, \leq)$ называется фундированным, если в любом непустом подмножестве A есть минимальный элемент.

Напоминание: В частично упорядоченном множестве следует различать *минимальные* и *наименьшие* элементы.

Определение 2. Частично упорядоченное множество $(A, \leq)$ называется фундированным, если в нём нет бесконечных убывающих цепей, т.е., в A нельзя выбрать бесконечную последовательность элементов a_i такую, что

$$a_0 > a_1 > a_2 > \ldots > a_n > \ldots$$

Определение 3. Частично упорядоченное множество $(A, \leq)$ называется фундированным, если для него выполняется *принцип индукции*: для любого свойства $B(x)$ выполнено условие

$$[\forall a\,((\forall a' < a\ B(a')) \to B(a))] \to (\forall a\ B(a))$$

Комментарий к определению 3: Обычное рассуждение по индукции для натуральных чисел как правило разбивают на два шага – базу индукции и шаг индукции. Таким образом, классический принцип индукции гласит: пусть (1) некоторое свойство B верно для числа 0 [база индукции], и (2) если B верно для какого-то числа n, то оно верно и для числа $n + 1$ [шаг индукции]; тогда свойство $B(x)$ выполнено для всех натуральных чисел.

[1] С исправлением ошибок, замеченных Д. Колодзей

Принцип индукции, сформулированный в таком виде, можно представить в виде следующей формулы:

$$B(0)\ \&\ [\forall n > 0\,(B(n-1) \to B(n))] \to (\forall n \in \mathbb{N}\ B(n)).$$

Можно обобщить этот принцип и рассматривать *шаг индукции* более общего вида. Вместо условия "*если истинно* $B(n-1)$*, то истинно и* $B(n)$" будем допускать условие вида "*если для всех* $n' < n$ *истинно* $B(n')$*, то истинно и* $B(n)$". Такой обобщенный принцип индукции можно записать в виде формулы

$$B(0)\ \&\ [\forall n > 0\,((\forall n' < n\ B(n')) \to B(n))] \to (\forall n \in \mathbb{N}\ B(n)).$$

Теперь заметим, что требования *базы индукции* и *шага индукции* можно соединить в одно условие. В самом деле, применить утверждение

$$((\forall n' < n\ B(n')) \to B(n))$$

для $n = 0$, мы получим утверждение о том, что свойство $B(0)$ истинно. Таким образом, *база индукции* становится частным случаем *шага индукции*. Так что привычный нам принцип индукции для натуральных чисел можно переписать в виде

$$[\forall n \in \mathbb{N}\,((\forall n' < n\ B(n')) \to B(n))] \to (\forall n \in \mathbb{N}\ B(n)).$$

Именно этот принцип индукции и использован в Определении 3 (только уже не для стандартного линейного порядка на множестве натуральных чисел, а для произвольного частичного порядка на произвольном множестве A).

Комментарий ко всем трём определениям: Определения 1 и 2 имеют более наглядный комбинаторный смысл. Определение 3 выглядит более сложно, но оно объясняет, почему понятие фундированного множества может быть интересно. По существу, фундированные множества – это такие частично упорядоченные множества, на которые удаётся перенести привычный нам метод математической индукции.

Теорема 1 *Три определения фундированного множества эквивалентны друг другу.*

Прежде чем читать дальше, попытайтесь самостоятельно доказать Теорему 1, не заглядывая в конспекты лекций.

Доказательство теоремы 1. Определение 1 → Определение 2: Пусть для некоторого частично упорядоченного множества $(A, \leq)$ выполнено первое определение (в любом подмножестве есть минимальный элемент). Предположим, что второе определение для данного множества не выполнено, и в множестве есть бесконечная убывающая цепь $a_0 > a_1 > a_2 > \ldots$ Но тогда в множестве $B = \{a_0, a_1, a_2, \ldots\}$ нет минимального элемента, что противоречит первому определению.

Определение 2 $\rightarrow$ Определение 1: Теперь предположим, что для частично упорядоченного множества $(A, \leq)$ выполнено Определение 2, а Определение 1 не выполнено. Это значит, что в A есть непустое подмножество B, в котором нет минимального элемента. Поскольку B непусто, то в нем найдётся некоторый элемент $b_0 \in B$. Мы предположили, что в B нет минимальных элементов. В частности, b_0 не может быть минимальным элементом B. Это значит, что в B есть (хотя бы один) элемент b_1, который меньше b_0. Данный b_1 тоже не может быть минимальным в B. А значит, в B найдётся элемент b_2 меньший, чем b_1. Продолжая это рассуждение, мы выделим в B последовательность элементов

$$b_0 > b_1 > b_2 > \ldots,$$

которые образуют бесконечную убывающую цепь. Это противоречит Определению 2.

Определение 1 $\rightarrow$ Определение 3: Снова предположим, что для некоторого $(A, \leq)$ выполнено Определение 1. Нам нужно доказать, что для данного множества выполнен также и принцип индукции. Пусть для какого-то свойства $B(x)$ верен "шаг индукции"

$$(*) \qquad \forall a\, ((\forall a' < a\ B(a')) \rightarrow B(a))\, .$$

Мы хотим показать, что в таком случае свойство $B(a)$ верно для всех элементов $a \in A$. Предположим противное – пусть для некоторых a свойство $B(a)$ ложно. Выберем среди всех таких a минимальный (Определение 1 гарантирует, что среди всех элементов a, для которого $B(a)$ ложно, есть хотя бы один минимальный). Тогда для данного $a_{\min}$ свойство $B(a_{\min})$ ложно, а для всех элементов a' меньших $a_{\min}$ свойство $B(a')$ истинно. Получаем противоречие с (*).

Определение 3 $\rightarrow$ Определение 1: Теперь предполагаем, что для $(A, \leq)$ выполнен принцип индукции. Нам нужно проверить, что в любом непустом подмножестве B в A есть хотя бы один минимальный элемент. Пусть в некотором $B \subset A$ минимального элемента нет. Мы должны доказать, что данное B пусто. Для этого мы рассмотрим свойство $C(x)$:

$$C(x) \text{ истинно} \Leftrightarrow x \notin B$$

(свойство *не* лежать в B). Для данного свойства

$$\forall a\, ((\forall a' < a\ C(a')) \rightarrow C(a))$$

(если все элементы $a' < a$ не лежат в B, то и a не лежит в B; иначе a был бы минимальным элементом B). По принципу индукции заключаем, что свойство $C(a)$ истинно для всех $a \in A$. Это значит, что в B нет ни одного элемента — это подмножество пусто. Теорема доказана.

2 Определение вполне упорядоченного множества.

Определение. Частично упорядоченное множество $(A, \leq)$ называется *вполне упорядоченным*, если порядок является линейным и фундированным.

Отметим, что в каждом непустом подмножестве вполне упорядоченного множества есть *наименьший* элемент (свойство фундированности гарантирует существование *минимального* элемента, а из линейности порядка следует, что минимальный элемент является также и наименьшим).

Пример 1. Всякое конечное линейно упорядоченное множество является вполне упорядоченным.

Пример 2. Множество натуральных чисел со стандартным порядком на них $(\mathbb{N}, \leq)$ является вполне упорядоченным.

Пример 3. Сумма двух экземпляров натуральных чисел со стандартным порядком $(\mathbb{N}, \leq) + (\mathbb{N}, \leq)$ также является вполне упорядоченным. Элементы этого множества обычно обозначают

$$0, 1, 2, \ldots, n \ldots, \omega, \omega + 1, \omega + 2, \ldots, \omega + n, \ldots$$

Пример 4. Произведение двух экземпляров натуральных чисел со стандартным порядком $(\mathbb{N}, \leq) \cdot (\mathbb{N}, \leq)$ тоже является вполне упорядоченным. Опишите более подробно структуру данного вполне упорядоченного множества.

Во всяком непустом вполне упорядоченном множестве $(A, \leq)$ есть минимальный элемент. Этот элемент удобно обозначать 0_A. Далее, если множество A не исчерпывается единственным элементом, то разность $A \setminus \{0_A\}$ непуста, и в этой разности тоже есть минимальный элемент. Его удобного обозначить 1_A. если A не исчерпывается двумя элементами, то в разности $A \setminus \{0_A, 1_A\}$ найдётся минимум, который мы обозначим 2_A. Повторяя это рассуждение снова и снова, мы получаем, что начало множества $(A, \leq)$ устроено так же, как натуральный ряд. Если A не исчерпывается последовательностью элементов

$$0_A, 1_A, 2_A, \ldots, k_A, \ldots,$$

то и в разности $A \setminus \{0_A, 1_A, 2_A, \ldots, k_A, \ldots, \}$ найдется минимальный элемент, который мы будем обозначать ω_A. За ним следуют элементы $(\omega + 1)_A$, $(\omega + 2)_A$, и т.д.

Таким образом, начало любого вполне упорядоченного множества устроено тау же, как множество из Примера 1 или (если множество бесконечно) как множество из Примера 2 или как множество из Примера 3...

Определение. Элемент a называется (непосредственным) *предшественником* b, если $a < b$ и не существует такого c, что $a < c$ и $c < b$. Элемент

a называется (непосредственным) *последователем* b, если $a > b$ и не существует такого c, что $a > c$ и $c > b$.

Определение. Элемент a вполне упорядоченного множества $(A, \leq)$ называется *предельным*, если у него нет предшественника.

Заметим, что минимальный элемент согласно данному определению является предельным. Найдите все предельные элементы во вполне упорядоченных множествах из Примеров 1–4.

Утверждение 1 *Во вполне упорядоченном множестве $(A, \leq)$ у всякого элемента a кроме максимального (если в A есть максимальный элемент) имеется ровно один последователь. У всякого непредельного элемента есть ровно один предшественник.*

Докажите данное утверждение!

Утверждение 2 *Для всякого элемента a вполне упорядоченного множество $(A, \leq)$ найдется такой предельный элемент $b \leq a$, что между b и a есть лишь конечное число элементов c (таких, что $b \leq c$ и $c \leq a$). Другими словами, каждый элемент A получается из некоторого предельного элемента сдвигом вправо на конечное число шагов.*

Доказательство: Если элемент a предельный, то $b = a$, и доказывать нечего. Если же a не является предельным, то у него есть есть ровно один предшественник a'. Если a' предельный, то в качестве b нужно взять этот элемент a'. В противном случае у a' есть свой предшественник, который мы обозначим a''. Если и a'' не является предельным, то у него есть свой предшественник a''', и т.д. Так мы спускаемся к предшественнику предшественника, предшественнику предшественника предшественника, и т.д, пока не встретим предельный элемент. Его мы и возьмем в качестве b.

Объясните, почему между исходным элементом a и найденным элементом b нет других промежуточных элементов кроме $a', a'', a''', \ldots$

Описанный процесс не может продолжаться бесконечно, поскольку в $(A, \leq)$ нет бесконечных убывающих цепей.

3 Метод трансфинитной индукции.

Мы уже отмечали, что свойства вполне упорядоченных множеств можно доказывать методом индукции. Рассуждение по индукции для множеств более сложных, чем $\mathbb{N}$, называется *трансфинитной индукцией.* Рассмотрим простой пример такого рассуждения.

Теорема 2 *Пусть множество $(A, \leq)$ вполне упорядоченно, и отображение $f : A \to A$ монотонно, т.е.,*

$$x < y \to f(x) < f(y).$$

Тогда $f(x) \geq x$ для всех $x \in A$.

Прежде чем читать дальше, попробуйте доказать эту теорему самостоятельно, не заглядывая в конспект.

Доказательство: Мы воспользуемся этой простой теоремой, чтобы поупражняться в применении метода трансфинитной индукции. У нас есть три эквивалентных определения фундированности, мы рассмотрим три разных доказательства, по одному доказательству для каждого определения.

Первый вариант доказательства. Предположим, что $f(x) < x$ для некоторых x из A. Рассмотрим множество всех таких "патологических" элементов x. В этом множестве найдется минимальный элемент – минимальный a, для которого $f(a) < a$. Обозначим $b = f(a)$.

По свойству монотонности отображения f, из условия $b < a$ мы получаем $f(b) < f(a)$, т.е., $f(b) < b$. Но с другой стороны, мы выбрали a так, что для всех b, меньших данного a, выполняется условие $f(b) \geq b$. Получено противоречие, и теорема доказана.

Второй вариант доказательства. Предположим, что для $f(a) < a$ для некоторого a из A. Тогда по свойству монотонности получаем $f(f(a)) < f(a)$, $f(f(f(a))) < f(f(a))$, и т.д. Это значит, что в A существует бесконечная убывающая цепь элементов

$$a > f(a) > f(f(a)) > f(f(f(a))) > \dots,$$

что противоречит фундированности.

Третий вариант доказательства. Воспользуемся принципом индукции. Мы хотим доказать, что $\forall x\ f(x) \geq x$. Для этого достаточно обосновать "шаг индукции", т.е., доказать для каждого a свойство

$$(**) \qquad [\forall a' < a\ (f(a') \geq a')] \to (f(a) \geq a).$$

Предположим, что для некоторого a условие (**) нарушено. Это значит, что $\forall a' < a\ (f(a') \geq a')$, но при этом $f(a) < a$. Обозначим $b = f(a)$. С одной стороны, $f(b) \geq b$ (как и для всех элементов a', меньших a). С другой стороны, $f(b) = f(f(a)) < f(a) = b$ всилу монотонности f. Получено противоречие, и теорема доказана.

4 Начальные отрезки вполне упорядоченного множества

Мы уже обращали внимание на то, что начальные куски всех известных нам вполне упорядоченных множеств устроены одинаково. Чтобы придать точный смысл этому утверждению, мы введем формальное определение *начального отрезка*.

Определение. Множество B называется *начальным отрезком* вполне упорядоченного множества $(A, \leq)$, если для каждого $x \in B$ и каждого $y \in A$ такого, что $y < x$, выполняется $y \in B$ (другими словами, вместе с каждым своим элементом x множество B содержит и все меньшие элементы).

Примеры:

- Пустое подмножество является начальным отрезком $(A, \leq)$.
- Всё множество A является своим начальным отрезком.
- Если a_0 есть минимальный элемент A, элемент a_1 минимален в $A \backslash \{a_0\}$, и a_2 минимален в $A \backslash \{a_0, a_1\}$, то тройка элементов $\{a_0, a_1, a_2\}$ является начальным отрезком в A.
- В Примере 3 на странице 4 множество $\{0, 1, 2, \ldots, \omega\}$ является начальным отрезком во всём множестве $(A, \leq) = (\mathbb{N}, \leq) + (\mathbb{N}, \leq)$.

Утверждение 3 *Для начальных отрезков вполне упорядоченных множеств выполняются следующие свойства.*

- *Начальный отрезок вполне упорядоченного множества $(A, \leq)$ сам является вполне упорядоченным множеством (с порядком, унаследованным из $(A, \leq)$),*
- *начальный отрезок начального отрезка $(A, \leq)$ и сам является начальным отрезом $(A, \leq)$,*
- *объединение любого семейства начальных отрезков $(A, \leq)$ снова является начальным отрезком $(A, \leq)$.*

Попробуйте восстановить доказательства этого утверждения, не заглядывая в конспект лекций.

Для вполне упорядоченного множества $(A, \leq)$ и всякого его элемента a мы будем использовать обозначения

$$[0, a)_A = \{x \in A \mid x < a\}$$

и

$$[0, a]_A = \{x \in A \mid x \leq a\}.$$

Докажите, что $[0, a)_A$ и $[0, a]_A$ являются начальными отрезками вполне упорядоченного множества.

Теорема 3 *Всякий начальный отрезок B в $(A, \leq)$ либо совпадает со всем A, либо равен $[0, b)_A$ для некоторого $b \in A$.*

Замечание: Напомним, что у всякого $a \in A$ (кроме максимального) есть непосредственный последователь. Поэтому всякий отрезок $[0, a]_A$ либо совпадает со всем множеством A, либо равен полуинтервалу $[0, a')_A$, где a' есть последователь a.

Доказательство теоремы: Когда начальный отрезок совпадает со всем A, доказывать нечего. Пусть B не совпадает с A. Возьмем в качестве b минимальный элемент в $A \setminus B$. Докажем, что $B = [0, b)_A$.

Доказательство включения $B \subset [0, b)_A$: Пусть $x \in B$. Мы должны доказать, что $x \in [0, b)_A$, т.е., что $x < b$. Предположим противное. Но тогда $b \leq x$, и по определению начального отрезка мы получаем $b \in B$. Это противоречит выбору элемента b.

Доказательство включения $B \supset [0, b)_A$: Пусть $x \in [0, b)_A$. Нам нужно доказать, что этот элемент лежит также и в B. Если это не так, то $x \in A \backslash B$ и при этом $x < b$. Это также противоречит выбору b (минимального элемента в $A \setminus B$). Теорема доказана.

5 Трансфинитная рекурсия и сравнимость любых двух вполне упорядоченных множеств

Мы продолжаем обсуждать наше замечание о том, что все известные нам вполне упорядоченные множества в начале устроены одинаково. Сейчас мы докажем, что любые два вполне упорядоченные множества сравнимы – одно из них обязательно является либо "началом", либо "продолжением" другого. Более строго, имеет место следующая теорема.

Теорема 4 *Для любых вполне упорядоченных множеств* $(A, \leq_A)$, $(B, \leq_B)$ *выполнено одно из двух условий:* $(A, \leq_A)$ *изоморфно (как линейно упорядоченное множество) некоторому начальному отрезку из* $(B, \leq_B)$ *или* $(B, \leq_B)$ *изоморфно некоторому начальному отрезку из* $(A, \leq_A)$.

Замечание: Могут выполняться одновременно оба условия: для некоторых вполне упорядоченных множеств $(A, \leq_A)$ изоморфно начальному отрезку $(B, \leq_B)$ и одновременно $(B, \leq_B)$ изоморфно начальному отрезку $(A, \leq_A)$. Докажите, что такое возможно, если и только если $(A, \leq_A)$ и $(B, \leq_B)$ изоморфны друг другу. *Указание:* используйте Теорему 2, стр. 5.

Неформальный план доказательства Теоремы 4: Будем строить требуемый изоморфизм шаг за шагом. Если одно из множеств $(A, \leq_A)$, $(B, \leq_B)$ пусто, то доказывать нечего. Пусть они оба непусты. Мы знаем, что в непустом вполне упорядоченном множестве есть минимальный элемент. Назовём минимальные элементы этих двух множеств 0_A и 0_B. Будущий изоморфизм будет сопоставлять эти элементы друг другу. Если одно из двух множеств исчерпывается одним элементом (скажем, A), то задача решена — мы установили соответствие между одноэлементным множеством A и одноэлементным начальным отрезком B. Если же оба множества содержат больше одного элемента, то найдем минимальные элементы среди ещё не рассмотренных:

$$1_A = \min_A (A \setminus \{0_A\})$$

и

$$1_B = \min_B (B \setminus \{0_A\}).$$

Будущий изоморфизм будет сопоставлять элемент 1_A из первого множества элементу 1_B из второго. Если и на этом оба множества не исчерпались, то

положим
$$2_A = \min_A(A \setminus \{0_A, 1_A\})$$
и
$$2_B = \min_B(B \setminus \{0_A, 1_A\}),$$
и так далее. Мы будем синхронно расширять начальные отрезки
$$\{0_A, 1_A, 2_A, \ldots, \omega_A, (\omega+1)_A, \ldots\}$$
и
$$\{0_B, 1_B, 2_B, \ldots, \omega_B, (\omega+1)_B, \ldots\}$$
в обоих наших вполне упорядоченных множествах, на каждом шаге продолжая построения изоморфизма. Если раньше закончатся элементы в множестве A, то мы получим изоморфизм между всем $(A, \leq_A)$ и некоторым начальным отрезком $(B, \leq_B)$. Если раньше исчерпается множество B, то мы получим изоморфизм между всем множеством $(B, \leq_B)$ и каким-то начальным отрезком $(A, \leq_A)$. Если же элементы в обоих множествах закончатся одновременно, то мы установим изоморфизм непосредственно между двумя исходными вполне упорядоченными множествами.

В приведенном рассуждении есть очевидный пробел: в ключевом месте мы использовали без объяснений слова *и так далее*. Чтобы придать этим словам смысл, нам потребуется изложить рассуждение более аккуратно, используя *трансфинитную индукцию*.

В конструкции, которую мы опишем ниже, мы будем строить требуемый изоморфизм шаг за шагом, опираясь на уже определенную ранее часть отображения. Такие конструкции иногда называют *трансфинитной рекурсией*. Подобно тому, как рекурсивное определение позволяет вычислять n-ое число Фибоначчи через предыдущие значения, мы будем определять значение нужного нам изоморфизма в очередной точке через значения этого же изоморфизма в *меньших* (в смысле порядка $\leq_A$) точках.

Доказательство Теоремы 4: Мы разделим доказательство на несколько шагов.

Шаг 1. По некоторым техническим причинам нам будет удобно расширить множество B, добавив к нему один новый элемент. Пусть некоторый элемент, который мы будем обозначать $*$, не принадлежит B (т.е., $* \notin B$). Далее мы будем рассматривать отображения из A в $B \cup \{*\}$. При этом нам будет полезен некоторый линейный порядок на $B \cup \{*\}$. Мы сохраним старый порядок на элементах B и будем считать, что $*$ больше всех элементов из B. Таким образом, элемент $*$ является максимальным в $B \cup \{*\}$. Проверьте, что множество $B \cup \{*\}$ с описанным порядком является вполне упорядоченным множеством.

Шаг 2. Мы будем строить отображение $f : A \to B \cup \{*\}$. В итоге f будет задавать требуемый изоморфизм. Мы будем определять это отображение индуктивно:
$$f(0_A) = 0_B,\ f(1_A) = 1_B,\ f(2_A) = 2_B,\ \text{и т.д.},$$

как мы и пытались сделать выше в *неформальном плане доказательства*. При этом будут возможны два случая: либо f отобразит всё множество A в какой-то начальный отрезок B (в этом случае элемент $*$ ни разу не встретится среди значений функции f), либо некоторый начальный отрезок A отобразится под действием f на всё множество B, а все остальные элементы A отобразятся в $*$.

Формально отображение f будет задаваться следующим рекурсивным определением:

Определение. Функция $f : [0, a]_A \to B'$ называется *регулярной*, если для каждого $x \in [0, a]_A$

$$(\mathcal{R}) \qquad f(x) = \begin{cases} \min(B \setminus \{f(x') \mid x' < x\}), & \text{если } B \setminus \{f(x') \mid x' < x\} \neq \emptyset, \\ *, & \text{если если } B \setminus \{f(x') \mid x' < x\} = \emptyset. \end{cases}$$

Интуитивный смысл этого определения: для каждого очередного $a \in A$ в качестве значения $f(a)$ мы берем минимальный ранее не использованный элемент B; если такого элемента не нашлось, то берем в качестве значения $*$. Далее мы покажем, что данное определение корректно.

Шаг 3. На этом шаге мы докажем осмысленность определения $(\mathcal{R})$ на каждом начальном отрезке A.

Лемма 1 *Для любого $a \in A$ существует и при том единственная функция $f : [0, a]_A \to B \cup \{*\}$, согласованная с $(\mathcal{R})$.*

Доказательство: Чтобы различать функции f с разными областями определения, будем обозначать f_a отображение $f_a : [0, a]_A \to B \cup \{*\}$, согласованное с $(\mathcal{R})$. Лемма утверждает, что для каждого a существует единственная такая функция f_a. Мы докажем это методом трансфинитной индукцией (индукцией по параметру a).

Обратите внимание, что мы будем доказывать по индукции сразу два свойства одновременно — *существование* и *единственность* требуемой f_a. Таким образом, в предположении индукции мы полагаем, что для всех меньших элементов уже установлены оба этих свойства: для всех $a' < a$ существует и единственное отображение $f_{a'} : [0, a']_A \to B \cup \{*\}$, согласованное с правилом $(\mathcal{R})$. Чтоб сделать шаг индукции, нам нужно показать существование и единственность такой же функции $f_a : [0, a]_A \to B \cup \{*\}$.

Начнем с доказательства существования. Заметим, что функции $f_{a'}$ для всех $a' < a$ согласованы друг с другом: если $a' < a'' < a$, то $f_{a'}$ является ограничением $f_{a''}$ на начальный отрезок $[0, a']$ (это следует из свойства *единственности* в предположении индукции). Поэтому мы можем рассмотреть объединение всех функций $f_{a'}$. Назовём это объединение $\hat{f}$:

$$\hat{f} := \cup_{a' < a} f_{a'}.$$

Данная функция $\hat{f}$ отображает $[0, a)_A$ в $B \cup \{*\}$; для каждого $x < a$ её значение определяется правилом $\hat{f}(x) = f_x(x)$.

Теперь мы готовы определить нужную нам функцию f_a. Положим

$$f_a(x) = \begin{cases} \hat{f}(x), & \text{если } x < a, \\ \min(B \setminus \{\hat{f}(a') \mid a' < a\} \cup \{*\}), & \text{если } x = a. \end{cases}$$

Проверьте, что построенная функция f_a согласована с правилом $(\mathcal{R})$, т.е., является регулярной.

Осталось доказать единственность требуемой функции f_a. Сначала заметим, что для всех $a' < a$ значение $f_a(a')$ определено однозначно: ограничение f_a на каждый начальный отрезок $[0, a']_A$ единственно по предположению индукции. Наконец, значение $f_a(a)$ однозначно определяется из

$$\{f_a(a') \mid a' < a\}$$

согласно $(\mathcal{R})$. Лемма доказана.

Шаг 4. Закончим нашу конструкцию отображения из A в B'.

Лемма 2 *Объединение (общее продолжение) функций f_a по всем $a \in A$ есть отображение $f : A \to B \cup \{*\}$, для которого правило $(\mathcal{R})$ выполняется для каждого $x \in A$.*

Доказательство леммы: По доказанной выше Лемме 1 для каждого $a \in A$ существует единственная функция $f_a : [0, a]_A \to B \cup \{*\}$, согласованная с $(\mathcal{R})$. Таким образом, эти функции согласованы друг с другом (одна является ограничением другой). Следовательно, мы можем объединить все эти функции (построить их общее продолжение), которое мы назовём f.

Замечание 1: Функцию f можно было бы формально определить в каждой точке $a \in A$ по правилу $f(a) = f_a(a)$.

Нетрудно проверить, что построенная функция f согласована с $(\mathcal{R})$.

Замечание 2: Из Леммы 1 легко получить *единственность* функции $f : A \to B \cup \{*\}$, согласованной с $(\mathcal{R})$. Таким образом, рекурсивное правило $(\mathcal{R})$ однозначно определяет некоторую функцию. Однако для доказательства теоремы нам не потребуется использовать единственность нужного нам отображения f, достаточно существования.

Шаг 5. Осталось убедиться, что построенная по правилу $(\mathcal{R})$ функция f задает нужный нам изоморфизм.

Лемма 3 *(а) Если согласованная с $(\mathcal{R})$ функция f отображает A в B (элемент $*$ не встречается среди значений f), то f изоморфно отображает A на некоторый начальный отрезок B.*

(б) Если элемент $*$ встречается среди значений f, то f изоморфно отображает некоторый начальный отрезок $[0, a)_A$ на всё множество B.

Доказательство леммы: (а) Прежде всего заметим, что отображение f строго монотонно. В самом деле, пусть $a_1 < a_2$. Тогда по правилу $(\mathcal{R})$

$$f(a_1) = \min(B \setminus \{f(a') \mid a' < a_1\})$$

и

$$f(a_2) = \min(B \setminus \{f(a') \mid a' < a_2\}).$$

В первом случае минимум выбирается из большего множества. Следовательно, $f(a_1) < f(a_2)$.

Далее, покажем, что образ функции f, т.е., множество $\{f(a) \mid a \in A\}$, есть начальный отрезок в B. Пусть некоторый элемент $b \in B$ лежит в образе f. Это значит, что $b = f(a)$ для некоторого $a \in A$. Согласно правилу $(\mathcal{R})$

$$b = \min(B \setminus \{f(a') \mid a' < a\}).$$

Тот факт, что минимумом оказался элемент b, означает, что все $b' < b$ уже встречаются среди значений $f(a')$ для каких-то a'. Другими словами, образ функции f вместе с каждым элементом b обязательно содержит и все меньшие элементы. Но это и есть определение начального отрезка в B.

(б) Пусть a минимальный элемент, отображаемый функцией f в $*$. Тогда все элементы из начального отрезка $[0, a)_A$ отображаются функцией f в B. Заметим, что среди значений функции f встречаются *все* элементы B (иначе по правилу $(\mathcal{R})$ не было бы необходимости отображать a в дополнительный элемент $*$). Наконец, строгая монотонность f на полуинтервале $[0, a)_A$ проверяется так же, как в пункте (а). Лемма доказана.

Из Леммы 3 мы немедленно получаем утверждение теоремы.

Подробно записанное доказательство Теоремы 4 кажется несколько громоздким. Но содержательная идея доказательства довольно проста: мы описываем нужный нам изоморфизм простым рекурсивным правилом, а затем по индукции докажем корректность этого рекурсивного определения. Для тренировки попробуйте воспроизвести доказательство, не заглядывая в конспект.

6 Ординалы

Множество x называется *транзитивным*, если для всякого $y \in x$ и всякого $z \in y$ выполнено $z \in x$ (все элементы множеств, являющихся элементами x, сами являются элементами x). Множество x называется *ординалом*, если

(1) множество x транзитивно,

(2) все элементы x являются транзитивными множествами.

Отметим, что из пункта (2) данного определения следует, в частности, что всякое $y \in x$ является *множеством* (все элементы x являются множествами, а не объектами какого-либо иного сорта).

Примеры транзитивных множеств: $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$.

Примеры ординалов: $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$.

Теорема 5 *(1) Всякий элемент ординала есть ординал.*

(2) Если на элементах ординала ввести порядок по правилу

$$(**) \qquad x \leq y \risingdotseq (x = y \text{ или } x \in y),$$

то мы получим частично упорядоченное множество.

(3) Порядок из пункта (2) является фундированным (нет бесконечных убывающих цепей.)

(4) Если α ординал, и $x, y \in \alpha$, то либо $x = y$, либо $x \in y$, либо $y \in x$. Другими словами, всякий ординал с отношением (**) на его элементах является вполне упорядоченным множеством.

Доказательство: Проведите самостоятельно доказательство пунктов (1) и (2).

(3) По существу в этом пункте теоремы утверждается, что не может существовать бесконечной последовательности множества $x_0, x_1, \ldots, x_n, \ldots$ такой, что

$$x_0 \ni x_1,\ x_1 \ni x_2,\ \ldots,\ x_n \ni x_{n+1},\ \ldots$$

Это утверждение самоочевидно и входит в формальную теорию множеств как одна из аксиом (*аксиома регулярности*).

Докажем (4) от противного. Предположим, что не все элементы ординала α сравнимы в указанном смысле. Пусть x — минимальный элемент α, для которого найдется хотя бы один несравнимый с ним y (тут мы используем уже доказанный пункт (3) — в каждом непустом подмножестве фундированного множества найдется хотя бы один минимальный элемент). Зафиксируем x и найдем для него минимальный несравнимый с ним y (мы второй раз используем фундированность порядка).

Поскольку x является минимальным «патологическим» элементом α, всякий $z \in x$ не является патологическим; в частности, всякий $z \in x$ сравним с y. Это значит, что $z = y$, $y \in z$, или $z \in y$. В случае $z = y$ мы сразу получаем, что y является элементом x, что противоречит несравнимости x и y. Далее, если $y \in z$, то из транзитивности x мы также получаем $y \in x$, что невозможно. Остаётся единственная возможность $z \in y$. Таким образом, каждый элемент множества x обязан лежать в y. Иначе говоря, мы доказали включение $x \subset y$.

Мы предположили, что x и y несравнимы. Это значит, в частности, что множества x и y не совпадают. Таким образом, найдется хотя бы один элемент $w \in y \setminus x$.

Поскольку y выбран минимальным элементом несравнимым с x, мы заключаем, что w сравнимо с x. Рассмотрим три возможных варианта:

(а) $w = x$ В этом случае $x \in y$, и мы сразу получаем противоречие с несравнимостью x и y.

(б) $x \in w$ Из транзитивности y следует, что $x \in y$, и мы снова получаем противоречие с несравнимостью x и y.

(в) $w \in x$ Это противоречит определению w — мы выбирали элемент из y, которые не лежит в x.

Теорема доказана.

Утверждение 4 *(1) Объединение любого множества ординалов есть ординал.*

(2) Начальный отрезок любого ординала (в смысле порядка (**) из Теоремы 5) также является ординалом.

(3) Если α ординал, то множество

$$S(\alpha){:=}\alpha \cup \{\alpha\}$$

тоже является ординалом.

Попробуйте доказать это утверждение, не заглядывая в конспект лекций.

В дальнейшем мы по умолчанию всегда будем считать каждый ординал вполне упорядоченным множеством с порядком (**).

Теорема 6 *Любые два ординала α, β сравнимы: либо $\alpha = \beta$, либо $\alpha \in \beta$, либо $\beta \in \alpha$.*

Доказательство: Рассмотрим множество $\gamma = S(\alpha) \cup S(\beta)$. Из Утверждения 4 следует, что множество γ тоже является ординалом. Следовательно, мы можем воспользоваться Теоремой 5 (4) и заключить, что α и β (как элементы ординала γ) должны быть сравнимы между собой (они либо совпадают, либо один является элементом другого).

Далее без дополнительных пояснений мы будем говорить, что ординал α *меньше* ординала β, если $\alpha \in \beta$. Согласно Теореме 6 любые два ординала сравнимы (они либо равны как множества, либо один из них меньше другого).

Следствие 1 *Всякий ординал является множеством всех меньших его ординалов.*

Объясните, как это следствие вытекает из Теоремы 6.

Теорема 7 *Не существует множества всех ординалов.*

Доказательство: Предположим, что существует множество X, состоящее из всех ординалов и только из них. Далее мы покажем, то это предположение ведет к противоречию (у этого противоречия есть собственное имя — это *парадокс Бурали-Форти*).

Рассмотрим объединение всех ординалов, лежащих в X. Согласно Утверждению 4 (1) это объединение (обозначим его Y) также является ординалом. Теперь рассмотрим множество

$$Y' = S(Y) = Y \cup \{Y\}.$$

С одной стороны, Y' является ординалом (Утверждение 4 (3)). С другой стороны, по предположению множество X содержит все ординалы, а значит и Y'. Это значит, что все элементы Y' должны лежать в Y. Получаем $Y \in Y$, что невозможно.

Теорема 8 *Всякое вполне упорядоченное множество $(A, \leq)$ изоморфно некоторому ординалу.*

Доказательство теоремы мы начнем со следующей леммы:

Лемма 4 *Для всякого $a \in A$ начальный отрезок $[0, a]_A$ изоморфен некоторому ординалу $\alpha(a)$.*

Доказательство леммы: Пусть утверждение леммы верно для всех $a' < a$. Рассмотрим объединение

$$\tilde{\alpha} := \bigcup_{a' < a} \alpha(a').$$

Нетрудно проверить (проверьте!), что ординал $S(\tilde{\alpha}) = \tilde{\alpha} \cup \{\tilde{\alpha}\}$ изоморфен $[0, a]_A$. Лемма доказана.

Теперь рассмотрим множество

$$\hat{\alpha} = \bigcup_{a \in A} \alpha(a).$$

Данное множество является ординалом (объединение ординалов и само является ординалом). Нетрудно проверить, что этот ординал $\hat{\alpha}$ изоморфен $(A, \leq)$. В самом деле, мы можем объединить все изоморфизмы между $\alpha(a)$ и $[0, a]_A$; в результате получим изоморфизм между $\hat{\alpha}$ и всем множеством $(A, \leq)$. (Сравните это рассуждение с доказательством Теоремы 4 и объясните, почему мы имеем право объединить все указанные изоморфизмы в одно отображение). Теорема доказана.

Теорема 9 *Для всякого множества A найдется такой ординал α, что $|\alpha| \not\leq |A|$.*

Комментарий: Содержательно эта теорема говорит, что существуют ординалы сколько угодно большой мощности. Нам бы хотелось сформулировать теорему как более понятный и более удобный для применений «положительный» факт: для всякого множества A найдется такой ординал α, что $|\alpha| > |A|$. Однако мы ещё не готовы доказать данное «положительное» утверждение. Трудность здесь в том, что мы ещё не доказали, что любые два множества сравнимы по мощности. Так что пока мы вынуждены довольствоваться несколько искусственным «отрицательным» свойством $|\alpha| \not\leq |A|$.

Доказательство теоремы: Пусть существует такое множество A, что всякий ординал α имеет мощность не больше мощности A. Это означает, что для всякого ординала α существует инъективное отображение $\varphi : \alpha \to A$.

Другими словами, всякий ординал α изоморфен некоторому вполне упорядоченному множеству $(B, \leq_B)$, для $B \subset A$ (и $\leq_B$ некоторый порядок на B).

Теперь мы за несколько шагов построим из A некоторое специальное множество, которое приведет нас к противоречию с Теоремой 7.

Шаг 1. Рассмотрим $A' = 2^A$ — множество всех подмножеств A.

Шаг 2. Рассмотрим бинарные отношения на всех множествах, являющихся элементами A' (более формально: мы рассматриваем декартов квадрат для каждого $B \in A'$ и берём *все* подмножества этого декартова квадрата). Обозначим множество всех таких отношений A''.

Шаг 3. Среди всех бинарных отношений, попавших в A'', выбираем только те, которые задают линйный и фундированный порядок — вполне упорядоченное множество (на некотором носителе $B \subset A$). Назовём множество всех прошедших отбор порядков A'''.

Шаг 4. Для каждого вполне упорядоченного множества из A''' найдём изоморфный ему ординал (это возможно по Теореме 8). Множество всех таких ординалов назовём A''''.

По нашему предположению *каждый* ординал α вкладывается в A. Это значит, что каждый ординал должен лежать в построенном множестве A''''. но это противоречит Теореме 7. Таким образом, теорема доказана.

7 Теорема Цермело

В этой главе нам придется явным образом использовать **аксиому выбора**: *Для любого множества X, состоящего из непустых множеств, существует такое отображение φ с областью определения X, что для любого $A \in X$*

$$\varphi(A) \in A.$$

Теорема 10 (Цермело) *Любое множество может быть вполне упорядочено: для любого множества A существует такое бинарное отношение $\leq_A$, что $(A, \leq_A)$ является линейно упорядоченным фундированным (т.е., вполне упорядоченным) множеством.*

Доказательство теоремы Цермело: Рассмотрим вполне упорядоченное множество $(B, \leq_B)$, для которого

$$|B| \not\leq |A|$$

(такое $(B, \leq_B)$ найдется согласно Теореме 9). Кроме того, нам удобно будет добавить к A дополнительный элемент $A' = A \cup \{*\}$; при этом мы будем считать $*$ максимальным элементом в A' (больше всех элементов A). Далее мы будем строить отображения из начальных отрезков B в A'.

В нашей конструкцией мы будем использовать отображение

$$\varphi : 2^A \setminus \{\emptyset\} \to A,$$

для которого $\varphi(X) \in X$ для каждого непустого $X \subset A$. Существование такой функции φ гарантируется аксиомой выбора.

Определение 1 *Отображение*

$$f_b \ : \ [0, b]_B \to A'$$

из начального отрезка $(B, \leq_B)$ *в* A' *называется* регулярной*, если для любой* $b' \leq_B b$

$$f(b') = \begin{cases} \varphi(A \setminus \{f(x) \mid x <_B b'\}), & \text{если } A \setminus \{f(x) \mid x <_B b'\} \neq \emptyset, \\ * & \text{иначе.} \end{cases}$$

Лемма 5 *Для любого* $b \in B$ *существует и притом единственная регулярная функция* f_b.

Докажите эту лемму самостоятельно.

Обозначим F объединение всех регулярных функций f_b,

$$F := \bigcup_{b \in B} f_b.$$

Такое объединение корректно определено, поскольку все функции f_b согласованы друг с другом (если f_{b_1} и f_{b_2} регулярны, то одна из этих функций является продолжением другой на большую область определения). Заметим, что у каждого $a \in A$ может быть не более одного прообраза $F^{-1}(a)$ (при этом у элемента $*$ может быть много прообразов).

Мы предположили, что $|B| \not\leq |A|$. Это значит, что F не может быть инъективным вложением B в A. Следовательно, некоторые элементы $b \in B$ под действием F отображаются в элемент $*$.

Пусть b_* — минимальный элемент $(B, \leq_B)$, который отображается в $*$. Тогда

$$F \ : \ [0, b_*)_B \to A$$

является биекцией (объясните, почему!). Теперь мы можем определить на A линейный фундированный порядок: для каждой пары элементов $x, y \in A$ мы полагаем

$$x \leq_A y \leftrightharpoons F^{-1}(x) \leq_B F^{-1}(y).$$

Проверьте, что $(A, \leq_A)$ является вполне упорядоченным множеством.

8 Следствия из теоремы Цермело

В этой главе мы применим теорему Цермело, чтобы доказать несколько полезных утверждений о мощностях бесконечных множеств.

Теорема 11 *Мощности любых двух множеств сравнимы: для любых множеств A, B выполнено $|A| \leq |B|$ или $|B| \leq |A|$.*

Доказательство: По Теореме Цермело всякое множество можно вполне упорядочить. Мы вводим на A и B порядки $\leq_A$ и $\leq_B$ и далее считаем, что множества $(A, \leq_A)$ и $(B, \leq_B)$ являются вполне упорядоченными.

По Теореме 4 любые два вполне упорядоченные множества сравнимы, т.е., одно из них изоморфно начальному отрезку другого. Для определенности будем считать, что множество $(A, \leq_A)$ изоморфно начальному отрезку $(B, \leq_B)$. Это означает, что существует отображение

$$f : A \to B,$$

которое обладает тремя свойствами:

- Значение $f(a)$ определено для каждого $a \in A$.
- Отображение монотонно: если $a_1 <_A a_2$, то $f(a_1) <_B f(a_2)$.
- Образ функции f есть начальный отрезок в $(B, \leq_B)$.

Из всех этих свойств f нам важно знать лишь то, что f есть инъективное вложение A в B. Это означает, что $|A| \leq |B|$. Теорема доказана.

Напомним несложное утверждение из первого семестра курса: если к бесконечному множеству A добавить конечное или счетное число элементов, то получится множество равномощное A.

Утверждение 5 *Если A произвольное бесконечное множество, а множество B конечно или счетно, то $|A \cup B| = |A|$.*

Вспомните доказательство Утверждения 5. Где в этом доказательстве используется аксиома выбора?

Итак, можность бесконечного множества не меняется при *объединении* со счетным множеством. Далее мы докажем, что мощность бесконечного множества не меняется и при *умножении* на счетное множество.

Теорема 12 *Если множество A бесконечно, а B счетно, то $|A \times B| = |A|$.*

Замечание: Мы уже знаем, как элементарными средствами доказать Теорему 12 для *счетных* множеств A — декартово произведение двух счетных множеств также счетно. Чтобы доказать эту теорему для произвольного бесконечного A, нам потребуется теорема Цермело.

Доказательство Теоремы 12:

Шаг 0: Прежде всего введем на A полный порядок (теорема Цермело) и далее будем полагать, что $(A, \leq)$ является вполне упорядоченным множеством.

Шаг 1: Если в $(A, \leq)$ есть максимальный элемент, то обозначим его a_{max}. Если этот элемент не является предельным, то обозначим a'_{max} его предшественника. Если и этот элемент не является предельным, то обозначим a''_{max}

предшественника предшественника максимального элемента, и т.д. Таким образом мы построим цепочку

$$a_{max} > a'_{max} > a''_{max} > \cdots > a^{(k)}_{max},$$

которая заканчивается некоторым предельным элементом $a^{(k)}_{max}$. Длина этой цепочки всегда конечна (Утверждение 2, стр. 5). Множество всех элементов A, которые не вошли в эту цепочку, мы обозначим A'. Таким образом, мы представили исходное множество A в виде объединения двух непересекающихся множеств

$$A = A' \cup \{a_{max}, a'_{max}, a''_{max}, \ldots, a^{(k)}_{max}\}.$$

Согласно Утверждению 5, множества A и A' равномощны. Поэтому вместо того, чтобы доказывать равномощность $A \times B$ и A, достаточно доказать равномощность $A' \times B$ и A'.

Шаг 2: Изучим более подробно структуру множества $(A', \leq)$ (мы сохранили на нём прежний полный порядок). Это множество бесконечно (выбрасывание конечной цепочки элементов не изменило мощности множества), и в этом множестве нет максимального элемента (именно для этого мы и выбросили цепочку элементов из A).

Поскольку в A' нет максимального элемента, то у каждого элемента есть свой последователь, последователь последователя, последователь последователя последователя, и т.д. Обозначим A'' множество всех предельных элементов из A'. Для каждого $a \in A''$ можно рассмотреть возрастающую счетную цепочку элементов

$$a < a' < a'' < a''' < \ldots,$$

состоящую из самого a, его последователя a', последователя последователя a'', и т.д. Заметим, что каждый элемент A' попадает ровно в одну такую цепочку (каждый элемент вполне упорядоченного множества получается из некоторого предельного элемента сдвигом вправо на конечное число шагов, мы снова пользуемся Утверждением 2, стр. 5). Таким образом, каждый $a \in A'$ можно однозначно задать парой “координат”

$$(\text{предельный элемент } a'', \text{целое число } k)$$

таких, что a получается из предельного элемента a'' сдвигом на k шагов вправо. Это означает, что A' равномощно $A'' \times \mathbb{N}$.

Шаг 3: Остается заметить, что для любого счетного множества B

$$A \times B \sim A' \times B \sim (A'' \times \mathbb{N}) \times B \sim A'' \times (\mathbb{N} \times B) \sim A'' \times \mathbb{N} \sim A' \sim A,$$

и теорема доказана.

Следствие 2 *Если множества A и B бесконечны, то* $|A \cup B| = \max\{|A|, |B|\}$.

9 Лемма Цорна

Многие доказательства, использующие трансфинитную рекурсию и трансфинитную индукцию, становятся короче и технически проще с использованием леммы Цорна. Чтобы сформулировать лемму Цорна, нам потребуется ввести два новых определения.

Определение. В частично упорядоченном множестве $(A, \leq)$ подмножество $B \subset A$ называется *цепью*, если любые два элемента из B сравнимы между собой.

Определение. В частично упорядоченном множестве $(A, \leq)$ элемент b называется верхней гранью подмножества $B \subset A$, если для любого $b' \in B$ выполнено $b' \leq b$. Заметим, что верхняя грань может принадлежать, а может и не принадлежать B.

Лемма 6 (Цорна) *Пусть $(A, \leq)$ такое частично упорядоченное множество, что для любой* цепи $B \subset A$ *существует некоторая* верхняя грань $b \in A$. *Тогда в $(A, \leq)$ есть максимальный элемент; более того, для любого $a \in A$ есть хотя бы один максимальный элемент a', больший или равный элемента a.*

Доказательство: Предположим, что для некоторого $a \in A$ не существует максимального элемента $a' \in A$ такого, что $a' \geq a$. Зафиксируем данный элемент a и приведем сделанное предположение к противоречию.

Возьмем некоторое множество S мощности большей, чем A, и введем на S полный порядок $(S, \leq)$. Построим инъективное отображение $f : S \to A$. Поскольку $|S| > |A|$, существование такого отображения будет противоречием. Нужную нам функцию мы определим с помощью трансфинитной рекурсии.

Поскольку $(S, \leq)$ является вполне упорядоченным, в этом множестве есть минимальный элемент. Назовём его s_0. Мы построим такую f, которая отображает s_0 в a. Каждый следующий элемент $s \in S$ будет отображаться в некоторый элемент A, который строго больше всех предыдущих значений функции f. Чтобы определить очередное значение функции f, мы будем пользоваться следующей леммой.

Лемма 7 *Для каждой цепи B в A, содержащей элемент a, найдется элемент b', который строго больше всех элементов B.*

Доказательство леммы: Поскольку B является цепью, условие Леммы Цорна гарантирует, что некоторый элемент b является верхней гранью B. Это значит, что для любого $x \in B$ выполнено $x \leq b$ (в частности, $a \leq b$). Однако это условие не требует, чтобы b был *строго* больше всех элементов B.

Теперь мы воспользуемся предположением: мы считаем, что в A нет макимальных элементов, больших или равных a. Это означает, что b (как верхняя грань для B) не может быть максимальным элементом в $(A, \leq)$.

Следовательно, найдется какой-то элемент b', строго больший b. Понятно, что этот b' будет строго больше и всех элементов цепи B. Лемма доказана.

Итак, Лемма 7 утверждает, что для всякой цепи B, содержащей a, есть элемент b', который строго больше всех элементов B (включая a). Для каждой цепи B таких элементов b' может быть много. Аксиома выбора позволяет зафиксировать выбор такого b' для каждой цепи $B \ni a$. Обозначим ψ такое отображение, которое сопоставляет каждой цепи B, содержащей a, некоторый элемент $\psi(B)$ из A, строго больший всех элементов B.

Теперь мы готовы построить инъективное отображение из S в A. Определим его рекурсивным правилом

$$f(s) = \begin{cases} a, & \text{если } s = s_0, \\ \psi(\{f(s') \mid s' < s\}), & \text{если } s > s_0. \end{cases} \qquad (\mathcal{R}')$$

Следующая лемма гласит, что данное рекурсивное определение корректно.

Лемма 8 *Для каждого $s \in S$*

(а) существует и единственно отображение $f_s : [0, s]_S \to A$, согласованное с правилом $(\mathcal{R}')$;

(б) множество значений данной функции $\{f_s(x) \mid x \in [0, s]_S\}$ является цепью в $(A, \leq_A)$ (все значения попарно сравнимы);

(в) f_s является инъекцией (все значения $f_s(x)$ для $x \leq_S s$ попарно различны).

Докажите Лемму 8. *Указание:* Воспользуйтесь трансфинитной индукцией. В предположении индукции должны содержаться все три утверждения (а), (б) и (в) (для всех s', меньших s).

Из Леммы 8 уже легко получить лемму Цорна. Объединим отображения $f_s : [0, s]_S \to A$ для всех $s \in S$ и получим инъективное отображение $f : S \to A$. Это противоречит тому, что мощность S больше мощности A.

Теорема 13 *Любое бесконечное множество A равномощно своему квадрату A^2.*

См. доказательство данной теоремы в [1, Теорема 34].

10 Аксиомы теории множеств

Стандартным способом формализовать рассуждения о множествах является формальная теория Цермело и Френкеля ZFC (буквы Z и F обозначают фамилии Цермело и Френкеля, а буква C обозначает аксиому выбора — axiom of choice).

Объектами ZFC являются множества и ничего кроме множеств. Однако выразительные средства этой теории очень велики; в терминах множеств можно описывать кортежи, отношения, функции, числа, геометрические фигуры , и т.д. — практически любые математические объекты можно «погрузить» в формальную теорию множеств. Скажем, упорядоченные пары $\langle x, y\rangle$ обычно описываются в ZFC как множества вида $\{x, \{x, y\}\}$ (пара по Куратовскому). Функция из множества X в множество Y — это некоторое множество F, состоящее из пар $\langle x, y\rangle$, где первая компонента пары есть элемент X, вторая компонента пар есть элемент Y, и выполнено свойство функциональности: для каждого $x \in X$ в F есть не более одной пары вида $\langle x, y\rangle$. Натуральные числа можно описывать как конечные ординалы; рациональные числа как обыкновенные дроби — пары натуральных чисел (точнее, как классы эквивалентности обыкновенных дробей), и т.д.

Формальная теория множеств ZFC использует язык первого порядка с равенством и единственным собственным предикатным символом $\in$ (который интерпретируется предикатом принадлежности). Свойства множеств описываются в ZFC набором аксиом, который мы приводим ниже.

1. Аксиома объёмности: *Два множества равны, если и только если они состоят их одних и тех же элементов.* Несколько более формально это можно сформулировать так:

$$x = y \leftrightarrow \forall z(z \in x \leftrightarrow z \in y).$$

2. Аксиома пустого множества: *Существует пустое множество.* Это свойство тоже легко записать в виде формулы языка первого порядка:

$$\exists x \forall y(y \notin x).$$

Отметим, что аксиому пустого множества можно было бы исключить из списка аксиом, поскольку её нетрудно вывести из других аксиом ZFC.

Ниже мы позволяем себе небольшую вольность речи и используем обычное обозначение пустого множества $\emptyset$, хотя обычно в теории ZFC специального символа (индивидной константы) для пустого множества не вводят.

3. Аксиома бесконечности: *Существует множество, включающее в себя пустое множество $\emptyset$, а также множества $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, и т.д.* Более формально это свойство можно описать так:

$$\textit{Существует такое } x, \textit{ что } \emptyset \in x, \textit{ и для всех } y \in x \textit{ множество } y \cup \{y\} \textit{ тоже является элементом } x.$$

4. Аксиома пары: *Из любых двух множеств x, y можно образовать неупорядоченную пару $\{x, y\}$*, т.е.,

$$\forall x \forall y \exists z(w \in z \leftrightarrow (w = x \vee w = y)).$$

5. Аксиома объединения: *Для любого семейства множеств x можно рассмотреть объединение всех множеств этого семейства.* Более формально,

$$\forall x \exists y \forall z(z \in y \leftrightarrow (\exists w(z \in w \ \& \ w \in x)))$$

6. Аксиома множества подмножеств: *Для всякого множества x существует множество y, элементами которого являются все подмножества x и только они.*

Попробуйте сформулировать аксиому 6 в виде формулы языка первого порядка.

7. Аксиома выделения подмножества: *Для всякого множества x и для всякого свойства (заданного некоторой формулой с параметром $\Phi(y)$) можно рассмотреть множество всех элементов из x, которые обладают указанным свойством.*

С точки зрения теории языков первого порядка аксиомы выделения — это целая серия аксиом, соответствующих всевозможным формулам Φ.

Перепишите аксиомы выделения в виде формул языка первого порядка.

8. Аксиома преобразования: *Пусть для некоторого множества x и некоторого свойства $\Psi(a, b)$ верно свойство «функциональности»: для любого $y \in x$ существует ровно одно z такое, что $\Psi(y, z)$ истинно. Тогда можно рассмотреть множество*

$$\{z \mid \text{существует элемент } y \in x \text{ такой, что } \Psi(y, z)\}.$$

Перепишите аксиому 8 в виде формулы языка первого порядка.

Строго говоря, аксиома преобразования также является не одной аксиомой, а целой серией аксиом, соответствующих всевозможным формулам Ψ.

9. Аксиома выделения регулярности: *Не существует бесконечной последовательности множеств $x_0, x_1, \ldots, x_n, \ldots$ такой, что $x_{n+1} \in x_n$ для каждого n.* Эквивалентная формулировка аксиомы регулярности:

$$\forall x(x \neq \emptyset(\exists y(y \in x \ \& \ \forall z(z \in y \to z \notin x))))$$

10. Аксиома выбора: *Для каждого множества x, все элементы которого сами являются непустыми множествами, существует такая функция φ, что для каждого $y \in x$ значение $\varphi(y)$ есть некоторый элемент в y.*

Аксиому 10 тоже можно записать в виде формулы языка первого порядка теории ZFC. Однако точная формулировка будет довольно громоздкой — придется описывать понятие функции как множество пар (по Куратовскому), обладающее свойством функциональности.

На лекции мы также обсуждали другой (эквивалентный) способ формализовать теорию множеств — теорию NBG (фон Нейман, Бернайс, Гёдель), см. подробности в [5].

Список литературы

[1] Верещагин Н., Шень А. Начала теории множеств - М.: МЦНМО, 1999.

[2] Лавров И.А., Максимова Л.Л. Задачи по теории множеств, математической логике и теории алгоритмов - М.: Физико-математическая литература, 1995.

[3] Йех Т. Теория множеств и метод форсинга. М.: Мир, 1973.

[4] Шёнфилд Дж. Математическая логика. М.: Наука, 1975.

[5] Мендельсон Э. Введение в математическую логику. М.: Наука, 1971.