ФИВТ МФТИ, весна 2013.

Краткие заметки по курсу *математическая логика*. Часть первая: трансфинитная индукция (4 лекции). (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 все доказательства излагаются очень подробно. В последних главах окончание некоторых доказательств предоставляется читателям в качестве упражнений.

Внимательные студенты заметят, что некоторые рассуждения записаны немного не так, как они были изложены на лекциях. Это связано с особенностями устной и письменной речи: одно и то же рассуждение может быть удобнее излагать по-разному у доски и на бумаге. Однако содержательные части всех доказательств в этих заметках достаточно точно повторяют рассказы на лекциях.

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. 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 → Определение 2: 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 → 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"

$$(*) \qquad \forall a \left((\forall a' < a \; B(a')) \to B(a) \right).$$

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 → 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

$$\forall a \left((\forall a' < a \; C(a')) \to C(a) \right)$$

(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.

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.

Проверьте, что между 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 $(A, \leq) = (\mathbb{N}, \leq) + (\mathbb{N}, \leq)$.

Простейшие свойства начальных отрезков:

- 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 $(A, \leq)$.

Докажите эти три свойства.

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

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

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

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, которое мы обозначим $(\mathcal{R})$.

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

Замечание: Два пункта этого рекурсивного определения можно объединить в одну строчку

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

(напомним, что $*$ является максимальным элементом в $B \cup \{*\}$). Интуитивный смысл этого определения прост: 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 g:

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

Данная функция g отображает $[0, a)_A$ в $B \cup \{*\}$; для каждого $x < a$ её значение определяется правилом $g(x) = f_x(x)$. Проверьте, что функция g согласована с правилом $(\mathcal{R})$!

Теперь мы готовы определить нужную нам функцию f_a. Положим

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

Проверьте, что построенная функция f_a согласована с правилом $(\mathcal{R})$!

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 доказательство корректности определения $(\mathcal{R})$.

Лемма 2 *Объединение (общее продолжение) функций f_a по всем $a \in A$ есть отображение $f : A \to B \cup \{*\}$, согласованное с $(\mathcal{R})$.*

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 $(\mathcal{R})$. 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 довольно громоздким, но содержательная идея во всём доказательстве ровно одна: опишем нужный нам изоморфизм простым рекурсивным правилом, а затем по индукции докажем корректность этого рекурсивного определения. Попробуйте воспроизвести доказательство, не заглядывая в конспект.

6 Теорема Цермело

В этой главе мы докажем, что любое множество (любой мощности!) можно вполне упорядочить. Этот важный результат называется теоремой Цермело. Для доказательства теоремы Цермело нам потребуется воспользоваться *аксиомой выбора*.

На самом деле в некоторых доказательствах мы неявно уже использовали аксиому выбора, но мы не акцентировали на этом внимания. Теперь же потребуется сформулировать и использовать эту аксиому явным образом.

Неформально аксиому выбора можно сформулировать следующим образом. Если задано некоторое семейство непустых множеств, то можно одновременно в каждом из этих множеств выбрать по элементу. Вот более точная формулировка.

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

Функция φ *выбирает* по одному элементу в каждом множестве семейства S. Разумеется, обычно такой "выбор" можно сделать огромным числом разных способов. Аксиома выбора ничего не говорит о конструкции и

каких-либо особых свойствах выбирающей функции φ, она лишь гарантирует существование хотя бы одной такой функции.

В некоторых случаях существование такой функции φ ясно и без специальной аксиомы, и выбор элемента из каждого множества в S можно описать явно. Рассмотрим несколько примеров.

- Если S состоит из всех непустых подмножеств $\mathbb{N}$, то для каждого $A \in S$ в качестве $\varphi(A)$ можно взять минимальное число в A.
- Если S состоит из всех непустых конечных подмножеств $\mathbb{R}$, то для каждого $A \in S$ в качестве $\varphi(A)$ можно взять минимальное число в A.
- Если S состоит из всех интервалов $(x, y) \subset \mathbb{R}$ (для всевозможных пар числе x, y, для которых $x < y$), то для каждого $A = (x, y)$ в качестве $\varphi(A)$ можно взять середину этого интервала $(x + y)/2$.

Однако в общем случае выбор элемента из каждого множества невозможно осуществить "конструктивно". Например, как описать выбор элемента в каждом непустом подмножестве $\mathbb{R}$? В таких случаях и приходиться пользоваться аксиомой выбора.

Теорема 5 (Цермело) *На любом множестве A можно ввести такой порядок $\leq$, что множество $(A, \leq)$ будет вполне упорядоченным.*

Очень неформальное доказательство теоремы Цермело: Выберем из множества A какой-нибудь элемент a_0 и объявим его минимальным элементом в будущем порядке. Далее выберем какой нибудь элемент $a_1 \neq a_0$ и объявим его следующим после минимального. Далее выберем в A элемент $a_1 \notin \{a_0, a_1\}$, и так далее. Повторяем эту процедуру, пока все элементы A не окажутся "пронумерованными".

Разумеется, пока это лишь грубый набросок доказательства, который ещё предстоит превратить в строгое рассуждение.

Первое уточнение неформальной идеи: Чтобы уточнить идею "очень неформального доказательства", приведенного выше, прежде всего следует конкретизировать, как именно мы будем выбирать очередной элемент a_i. Для этого нам и понадобится аксиома выбора.

Аксиома выбора гарантирует, что существует отображение

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

которая сопоставляет каждому непустому подмножеству $B \subset A$ некоторый элемент $b = \varphi(B) \in B$. Таких функций φ может быть очень много, мы зафиксируем какую-нибудь одну.

Технически нам будет удобно выбирать элемент не из самого подмножества B, а из его дополнения. Мы определим функцию ψ

$$\psi : 2^A \setminus \{A\} \to A$$

как $\psi(B) = \varphi(A \setminus B)$. Содержательно это означает, что для любого подмножества $B \subsetneq A$ функция $\psi(B)$ возвращает некоторый новый элемент из A, не лежащий в B.

Теперь можно пересказать неформальную идею доказательства теоремы Цермело чуть более точно. Мы выбираем в качестве самого первого элемента $a_0 = \psi(\emptyset)$ и объявим его минимальным элементом в будущем порядке. Следующим элементом будет $a_1 = \psi(\{a_0\})$, далее $a_2 = \psi(\{a_0, a_1\})$, $a_3 = \psi(\{a_0, a_1, a)2\})$, и так далее. Мы шаг за шагом строим на элементах A порядок, добавляя каждый новый элемент с помощью правила ψ. Мы повторяем эту процедуру, пока все элементы A не окажутся "пронумерованными".

Разумеется, выделенная красным цветом часть рассуждения остается неясной. Напомним, что мы хотим "пронумеровать" таким способом произвольное (возможно, несчетное!) множество. Так что для того, чтобы превратить описанный план в настоящее доказательство, требуется проделать ещё немалую работу.

На лекции мы получили строгое доказательство теоремы Цермело, введя понятие *корректного фрагмента* (согласованного с ψ) и построив максимальный корректный фрагмент, который и совпал со всем множеством A. Это рассуждение подробно описано в [1, Теорема 24].

7 Следствия из теоремы Цермело

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

Теорема 6 *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 $(A, \leq_A)$ 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 и 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 3 *Если A произвольное бесконечное множество, а множество B конечно или счетно, то $|A \cup B| = |A|$.*

Вспомните доказательство Утверждения 3. 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 7 *Если множество A бесконечно, а B счетно, то $|A \times B| = |A|$.*

Замечание: Мы уже знаем, как элементарными средствами доказать Теорему 7 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 7:

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 макисмальный элемент, то обозначим его a_{max}. Если этот элемент не является максимальным, 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 3, 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

$$a < a' < a'' < a''' < \dots,$$

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 1
(а) Если A и B равномощны, то $|A \cup B| = |A|$.
(б) Если A бесконечно, а B конечно, то $|A \times B| = |A|$.
(в) Если множества A и B бесконечны, то $|A \cup B| = \max\{|A|, |B|\}$.

Докажите данное следствие Теоремы 7, не заглядывая в конспекты лекций.

8 Ещё одно применение трансфинитной индукции

При первом чтении эту главу можно пропустить.

В этой главе мы приведем доказательство равномощности бесконечного множества A своему декартову квадрату. Эта теорема не доказывалась на лекциях, но обсуждалась на семинарах. Ниже мы приводим доказательство, не использующее лемму Цорна.

Теорема 8 *Любое бесконечное множество A равномощно своему квадрату A^2.*

Доказательство: Введём на A некоторый полный порядок (это возможно по теореме Цермело). Без ограничения общности можно считать, что в этом порядке есть максимальный элемент (если мы сначала получили порядок, в котором нет максимального элемента, то можно искусственно добавить недостающий максимальный элемент – добавление одного элемента не изменит мощность бесконечного множества A).

Обозначим a_0 минимальный элемент A такой, что начальный отрезок $[0, a_0)$ равномощен A (такой элемент обязательно найдется; именно для этого мы оговорились, что в $(A, \leq)$ есть максимальный элемент). Для доказательства теоремы нам нужно показать, что $[0, a_0)$ равномощно $[0, a_0) \times [0, a_0)$.

Отметим, что каждое множество $[0, a)$ заведомо имеет мощность не больше мощности $[0, a) \times [0, a)$. Так что если нам для какого-то a удаётся доказать обратное неравенсвто, т.е., $|[0, a)| \geq |[0, a) \times [0, a)|$, то с помощью теоремы Кантора–Бернштейна мы немедленно сможем заключить, что $[0, a)$ и $[0, a) \times [0, a)$ равномощны. Таким образом, для доказательства теоремы нам достаточно показать, что $|[0, a_0)| \geq |[0, a_0) \times [0, a_0)|$.

У нас уже есть полный порядок на множестве A; теперь мы введем полный порядок и на его декартовом квадрате $A \times A$. Для пар $(a, b), (a', b') \in A \times A$ будем считать, что (a, b) меньше (a', b'), если

- либо $\max\{a, b\} < \max\{a', b'\}$,
- либо $a = \max\{a, b\} = a' = \max\{a', b'\}$ и $b < b'$,
- либо $a = \max\{a, b\} = b' = \max\{a', b'\}$ и $a' < b'$,
- либо $b = \max\{a, b\} = b' = \max\{a', b'\}$ и $a < a'$.

Этот порядок легко представить себе наглядно. Разобьём $A \times A$ на ‘уголки’, состоящие из пары отрезков (‘вертикального’ и ‘горизонтального’):

$$\text{Уголок}_c = \{(x, c) \ : \ x \leq c\} \cup \{(c, x) \ : \ x \leq c\}$$

Пары (a, b) мы упорядочиваем так. Если (a, b) попадает в *Уголок* с меньшим значением c, нежели (a', b'), то считаем, что $(a, b) < (a', b')$. Если обе пары попадают в один и тот же уголок, то смотрим, лежат ли пары на вертикальной или горизонтальной линии; все точки вертикальной линии считаются меньше всех точек горизонтальной линии. А внутри вертикальной (соответственно, горизонтальной) линии точки упорядочены снизу вверх (соответственно, слева направо). Нетрудно понять, что введённый порядок является полным (проверьте это!).

Теперь определим функцию, которая (как мы докажем) будет задавать биекцию между $[0, a_0)$ и $[0, a_0) \times [0, a_0)$. Определим функцию $\varphi : [0, a_0) \to A \times A$ рекурсивно:

$$\varphi(a) = \min\{(b, c) \in A \times A \ : \ (b, c) \text{ не встречалось среди } \varphi(a') \text{ для } a' < a\}$$

Обычное рассуждение по трансфинитной индукции показывает, что такая функция φ существует (и единственна). (Проведите это рассуждение!) Кроме того, определённая таким образом функция φ обладает следующими свойствами:

1. φ инъективна,
2. φ монотонна,
3. для любого начального отрезка $[0, a)$ в A его образ $\varphi([0, a))$ является начальным отрезком в $A \times A$,
4. если $\varphi(a) \in$ Уголок$_b$, то для всех $c < b$ имеем Уголок$_c \subset \varphi([0, a))$.

(Объясните, почему эти свойства выполнены для данного отображения!)

Определение. Будем называть $b \in A$ *кардинальным*, если ни для какого $c < b$ начальные отрезки $[0, b)$ и $[0, c)$ равномощны. Кардинальные b делятся на *конечные* (такие, что множество $[0, b)$ конечно) и *бесконечные* (такие, что множество $[0, b)$ бесконечно).

В частности, элемент a_0 по определению является кардинальным.

Лемма 4 *Для каждого бесконечного кардинального $b \in A$ образ $[0, b)$ под действием φ содержит $[0, b) \times [0, b)$.*

Замечание: Если образ множества $[0, b)$ под действием φ содержит $[0, b) \times [0, b)$, то мощность $[0, b)$ не меньше мощности $[0, b) \times [0, b)$. Обратное неравенство очевидно, так что мы можем воспользоваться теоремой Кантора–Бернштейна. Таким образом, из леммы вытекает, что для каждого бесконечного кардинального b множество $[0, b)$ и его декартов квадрат $[0, b) \times [0, b)$ равномощны.

Доказательство леммы: Предположим, что утверждение леммы неверно, и для некоторых кардинальных b отображение φ переводит $[0, b)$ в собственное подмножество $[0, b) \times [0, b)$. Пусть b_0 – минимальный элемент A с таким свойством.

Прежде всего отметим, то для любого бесконечного кардинального $c < b_0$ условие леммы не нарушается, т.е., $[0, c)$ равномощно $[0, c) \times [0, c)$. Это значит, что и для некардинальных c' таких, что $c' < b_0$ и $[0, c')$ бесконечно, множество $[0, c')$ должно быть равномощно своему квадрату $[0, c') \times [0, c')$ (сначала заменяем c' на равномощное ему кардинальное c, а затем пользуемся тем, что для кардинального $c < b_0$ множества $[0, c)$ и $[0, c) \times [0, c)$ равномощны).

По предположению, множество $\varphi([0, b_0))$ не включает в себя подмножество $[0, b_0) \times [0, b_0)$. Из построения φ следует, что в таком случае, наоборот, $\varphi([0, b_0))$ содержится в $[0, b_0) \times [0, b_0)$ (см. выше свойство 4 функции φ). Обозначим c минимальный элемент, для которого $[0, c) \times [0, c)$ содержит целиком φ-образ $[0, \beta_0)$. Данный элемент c должен быть меньше b_0 (Объясните, почему!). Кроме того, $[0, c)$ должно быть бесконечным (иначе

$[0, c) \times [0, c)$, а значит и $[0, b_0)$ было бы конечным). Это значит, $[0, c)$ равномощно $[0, c) \times [0, c)$. Объединяя эти факты, мы заключаем, что $[0, b_0)$ имеет мощность не больше, чем $[0, c)$. Но это противоречит кардинальности b_0. Лемма доказана.

Итак, Лемма 4 показывают, что мощность $[0, a_0)$ не меньше мощности $[0, a_0) \times [0, a_0)$. Следовательно, $[0, a_0)$ и $[0, a_0) \times [0, a_0)$ равномощны. Теорема доказана.

Покажите, что построенное в доказательстве отображение φ является не просто сюръекцией $[0, a_0)$ на $[0, a_0) \times [0, a_0)$, а биекцией между $[0, a_0)$ и $[0, a_0) \times [0, a_0)$. (Это свойство не нужно для доказательства теоремы; однако примечательно, что в процессе доказательства нам удалось явно описать взаимно однозначное соответствие между $[0, a_0)$ на $[0, a_0) \times [0, a_0)$.)

Более короткое доказательство данной теоремы, использующее Лемму Цорна, можно найти в [1, Теорема 34].

9 Лемма Цорна

Студенты специальности ПМФ могут пропустить эту главу.

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 5 (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 6 *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 граню 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 6 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 7 *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 7. *Указание:* Воспользуйтесь трансфинитной индукцией. В предположении индукции должны содержаться все три утверждения (а), (б) и (в) (для всех s', меньших s).

Из Леммы 7 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.

10 Базис Гамеля и его применения

Определение. Базисом Гамеля векторного пространства L над полем F называется такое множество векторов $B \subset L$, что

1. никакая нетривиальная линейная комбинация конечного набора векторов из B не равна нулевому вектору, и

2. всякий вектор из L можно представить в виде линейной комбинации конечного набора векторов из B.

Покажите, что всякий ненулевой вектор из L *единственным* образом представляется в виде конечной линейной комбинации векторов из B с ненулевыми коэффициентами.

Теорема 9 *В любом векторном пространстве есть базис Гамеля.*

Доказательство. Ниже мы докажем теорему о существовании базиса Гамеля с помощью леммы Цорна, как мы это делали на лекции для студентов специальности ПМИ.

Будем называть *предбазисом* такое множество $B \subset L$, что никакая нетривиальная линейная комбинация конечного набора векторов из B не равна нулевому вектору (в частности, пустое множество является предбазисом).

Рассмотрим множество всех предбазисов для данного векторного пространства L и введем на них частичный порядок: будем говорить, что предбазис B_1 не превосходит предбазиса B_2, если $B_1 \subseteq B_2$. Заметим, что для всякой цепи предбазисов имеется верхняя грань. В самом деле, если $\mathcal{B}$ есть множество попарно сравнимых предбазисов, то можно рассмотреть объединение всех предбазисов данного семейства. Назовем это объединение B. Для всякого конечного набора векторов $\{v_1, \ldots, v_k\} \subset B$ найдется такой предбазис из $\mathcal{B}$, который содержал в себе все эти векторы. (Объясните, почему!) Следовательно, никакая нетривиальная линейная комбинация $\{v_1, \ldots, v_k\}$ не может быть нулевой. Это и означает, что множество B само является предбазисом.

Теперь мы можем применить к множеству всех предбазисов с отношением включения лемму Цорна и заключить, что среди всех предбазисов существует (хотя бы один) максимальный.

Пусть $B_{\max}$ является максимальным (по включению) предбазисом. Тогда всякий вектор $v \in L$ можно представить в виде линейной комбинации векторов из B (в противном случае вектор v можно было бы добавить к B; расширенное множество $B \cup \{v\}$ оставалось бы предбазисом, что противоречит максимальности B). Таким образом, *максимальный* предбазис является базисом Гамеля, и теорема доказана.

Теорему о существовании базиса Гамеля можно доказать без использования леммы Цорна, непосредственно применяя трансфинитную рекурсию. Такое доказательство мы обсуждали на лекции для студентов специальности ПМФ. Похожее доказательство излагается в [1, Теорема 26].

Рассмотрим множество вещественных чисел $\mathbb{R}$ с обычной операцией сложения как векторное пространство над полем рациональных чисел (вещественные числа можно складывать и умножать на рациональные числа, все аксиомы векторного пространства выполняются). В этом пространстве есть базис Гамеля. Докажем, что этот базис должен быть бесконечным (и даже несчетным).

Утверждение 4 *Рассмотрим $\mathbb{R}$ как векторное пространство над $\mathbb{Q}$. Каждый базис Гамеля в этом пространстве имеет мощность континуума.*

Доказательство: Всякий вектор вектор из пространства $\mathbb{R}$ представляется (единственным образом) в виде линейной комбинации векторов базиса B. Подсчитаем, сколько всего существует линейных комбинаций векторов базиса.

Множество нетривиальных линейные комбинаций из k базисных векторов равномощно множеству

$$B^k \times (\mathbb{Q} \setminus \{0\})^k$$

(мы выбираем k вектор из базиса и выбираем для каждого из них рациональный коэффициент, не равный нулю). Таким образом, множество всех векторов пространства равномощно

$$B \times (\mathbb{Q} \setminus \{0\}) \cup B^2 \times (\mathbb{Q} \setminus \{0\})^2 \cup \ldots \cup B^3 \times (\mathbb{Q} \setminus \{0\})^3 \cup \ldots$$

Если бы базис B был конечен, что множество всех таких линейных комбинаций было бы счетно. Если же B бесконечно, то множество всех линейных комбинаций равномощно B (декартова степень B равномощна B, умножение B на счетное множество не увеличивает мощности, и объединение счетного семейства множеств равномощных B также равномощно B, см. Теорему 7). Чтобы в итоге получилось множество всех векторов, имеющее мощность континуума, сам базис B должен иметь мощность континуума. Утверждение доказано.

Следствие 2 *Аддитивные группы $(\mathbb{R}, +)$ и $(\mathbb{R}^2, +)$ изоморфны.*

Доказательство: Обе группы можно рассмотреть как векторные пространства над полем $\mathbb{Q}$. В обоих пространствах найдутся базисы Гамеля, и оба этих базиса имеют мощность континуум. Установим взаимно однозначное соответствие между базисами в $(\mathbb{R}, +)$ и $(\mathbb{R}^2, +)$. Соответствие между базисами естественным образом продолжается до соответствия между рациональными линейными комбинациями базисных векторов в первом и втором пространстве. Это соответствие и является изоморфизмом между аддитивными группами $(\mathbb{R}, +)$ и $(\mathbb{R}^2, +)$. (Объясните, почему!)

Следствие 3 *Существует отображение $f : \mathbb{R} \to \mathbb{R}$ такое, что для любых $a, b \in \mathbb{R}$*

$$f(a + b) = f(a) + f(b),$$

но $f(x)$ не является умножением на константу.

Доказательство: Снова рассмотрим $\mathbb{R}$ как векторное пространство над $\mathbb{Q}$. Пусть B некоторый базис Гамеля в этом пространстве, и пусть $v_0 \in B$ один из базисных векторов.

По определению базиса, каждый вектор x (в нашем случае вектор – это просто вещественное число) представляется в виде конечной линейной комбинации векторов из B с рациональными коэффициентами,

$$x = \lambda_0 v_0 + \ldots + \lambda_k v_k.$$

Сопоставим каждому числу x коэффициент λ_0 при векторе v_0 в данном разложении (если вектор v_0 не входит в линейную комбинацию для x, то считаем $\lambda_0 = 0$).

В качестве отображения f можно взять соответствие $f : x \mapsto \lambda_0$. Нетрудно проверить, что для данного отображения $f(a+b) = f(a) + f(b)$ для любых a, b. Но данное отображение не является умножением на константу, поскольку все его значения рациональны.

11 Заключительные комментарии.

Комментарий о трансфинитной рекрусии. В нескольких доказательствах мы использовали тип рассуждения, которое называется *трансфинитной рекурсией*. В каждом случае мы строили некоторое отображение f, областью определения которого является вполне упорядоченное множество. Отображение задавалось рекурсивным правилом – значение f в каждой точке области определения вычислялось через значения этого же отображения в *меньших* точках. Далее мы в каждом случае проверяли, что определение корректно, и задаваемая им функция f обладает нужными нам свойствами. Все эти рассуждения были похожи друг на друга.

Все наши рассуждения с трансфинитной рекурсией являются частными случаями некоторого универсального правила. Общее утверждение о корректности определений, основанных на трансфинитной рекурсии, можно найти в [1, теоремы 18 и 19].

Комментарий об аксиомах. В первой части курса мы избегали излишней формализации и не обсуждали аксиоматическое построение теории множеств. Лишь *аксиому выбора* нам пришлось сформулировать явным образом. В конце семестра мы кратко обсудим аксиматику Цермело–Френкеля теории множеств. Пока же заинтересованные читатели могут познакомиться с аксиоматическим построением теории множеств в [3, 4].

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.