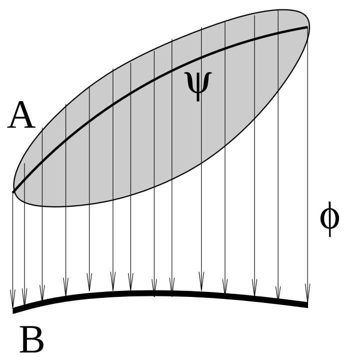
0. Топология, лекция 0: Аксиома выбора и ее приложения

0.1. Сечение отображения

Пусть $\varphi: A \longrightarrow B$ сюрьективное отображение множеств. **Сечением** отображения φ называется отображение $\psi: B \longrightarrow A$, такое, что $\psi\circ\varphi = \mathsf{Id}$.



Сечение сюрьективного отображения

Аксиома выбора утверждает, что каждое сюрьективное отображение имеет сечение.

0.2. Аксиоматическая теория множеств

Один из подходов к обоснованию математики называется **формализмом**, и принадлежит он Давиду Гильберту. В начале XX-го века математика оказалась в кризисе, сотрясаемая парадоксами, которые следовали из "наивной теории множеств", придуманной Георгом Кантором. Стало ясно, что обращение с произвольно взятыми бесконечными множествами опасно и приводит к противоречиям. В надежде избежать парадоксов, математики (Фреге, Гильберт, Цермело, Рассел-Уайтхед) стали строить аксиоматическое обоснование для теории множеств, надеясь, что аккуратное следование логическим построениям поможет избежать парадоксов.

Система аксиом, предложенная Фреге, оказалось противоречивой, основания математики по версии Рассела-Уайтхеда – слишком сложными, и к настоящему времени канонической стала система аксиом, предложенная в 1908-м году Эрнстом Цермело, и улучшенная в 1922 Адольфом Френкелем и (независимо от него) Торальфом Сколемом (Adolf Fraenkel, Thoralf Skolem). В учебниках встречается немало версий системы Цермело-Френкеля, но все они эквивалентны.

Ernst Friedrich Ferdinand Zermelo
(1871 - 1953)

Цермело провел 3 года (1905-1908), пытаясь доказать, что его система аксиом непротиворечива (не приводит к противоречию). Вплоть до 1930-х годов, Гильберт с коллегами были уверены, что в скором времени удастся доказать непротиворечивость системы аксиом Цермело-Френкеля, и аксиоматическая теория множеств станет фундаментом для всей математики.

В 1931-м году, Курт Гёдель доказал, что непротиворечивость Цермело-Френкеля недоказуема. Если точно, Гедель доказал, что невозможно доказать непротиворечивость любой системы аксиом в математическом языке, достаточно сильном, чтобы сформулировать на нем утверждения арифметики, если из этой системы аксиом следуют аксиомы Пеано (существование натуральных чисел и принцип индукции). Еще точнее – Гедель доказал невозможность доказательства средствами, допускающими формализацию в рамках того же самого математического языка.

Отмечу, что *опровергнуть* непротиворечивость такой системы аксиом как раз весьма просто – надо вывести из аксиом противоречие. Таким образом, к примеру, была опровергнута система аксиом Готлоба Фреге.

Многие математики убеждены в непротиворечивости системы аксиом Цермело-Френкеля; другие считают, что в случае противоречий будет изобретена новая система аксиом, и осмысленную часть математических утверждений с легкостью переведут на новый язык (и так до бесконечности, по мере обнаружения противоречий). Именно этой точке зрения следовала группа Бурбаки.

Есть немало математиков, считающих, что аксиоматический метод порочен сам по себе. Эта точка зрения была выдвинута голландским математиком Брауэром (Luitzen Egbertus Jan Brouwer), знаменитым топологом, в 1908-м году, в статье, провокативно озаглавленной "De onbetrouwbaarheid der logische principes" – "О сомнительности основ логики". Брауэр считал, что классическая (аристотелева) логика не может быть применима к бесконечным множествам, и все математические исследования, которые основаны на таких применениях – неправильны. Особенно Брауэру не нравился принцип исключенного третьего, на котором основаны популярные доказательства "от противного". На протяжении 1920-х годов Брауэр был редактором журнала Mathematische Annalen, и он принципиально возвращал авторам все статьи, где использовались доказательство от противного.

Брауэр называл свою философию "интуиционизмом". В середине XX-го века русские математики, близкие к Маркову и Колмогорову, развили свою версию философии интуиционизма, под названием "конструктивизм"; как и интуиционисты, конструктивные математики отрицают классическую математику, точнее – все неявные доказательства существования.

С точки зрения конструктивиста, любой математический объект должен быть задан явно. Например, действительное число в конструктивной математике это алгоритм его вычисления с любой точностью, плюс оценка скорости сходимости этого алгоритма.

Исследования конструктивистов оказались очень полезны в компьютерных науках, теории алгоритмов и лингвистике.

0.3. Аксиома выбора и ее конкуренты

Большой части математиков (даже не следующих экзотическим философиям) свойственно недоверие к неявным построениям. Действительно, явный пример числа (в виде ряда, к примеру) гораздо удобнее иметь, чем теорему вида "существует такое число, что...".

Тем не менее, аргументами "от противного" и неявными построениями по необходимости пользуются почти все математики, потому что если от них отказаться, придется отказываться от большого числа полезных утверждений, не имеющих явного доказательства.

Самым патологическим примером "неявной конструкции" является аксиома выбора, которая утверждает существование объектов, которые заведомо не могут быть построены никакой явной конструкцией.

Ближе к концу 1920-х годов, оказалось, что аксиома выбора позволяет доказывать (наряду с верными и полезными) утверждения чрезвычайно сомнительные и противоречащие физической интуиции. Так, в 1924-м году Банах и Тарский обнаружили парадоксальное разложение шара в $\mathbb{R}^3$ в счетное количество частей, из которых можно сложить два таких же шара. Сейчас известно, что шар можно разложить в 5 частей, и сложить из них два таких шара, изометрически передвигая эти части в $\mathbb{R}^3$.

Это утверждение сродни мечте алхимиков получить из небольшого куска золота очень большой, и вызывает столько же сомнений.

Впрочем, исключение аксиомы выбора не избавит математику от противоречий: непротиворечивость системы Цермело-Френкеля с аксиомой выбора[1] равносильна непротиворечивости Цермело-Френкеля без нее.

Тем не менее, хорошим тоном считается не пользоваться аксиомой выбора по возможности, или пользоваться ею, всякий раз обозначая факт неявности выбора.

В математике (кроме очень экзотических областей) без аксиомы выбора довольно часто удается обойтись. Основные утверждения, для которых нужна аксиома выбора, такие.

1. Теорема о существовании максимальных идеалов (см. лекцию 9).

2. Теорема о существовании базиса в любом бесконечномерном векторном пространстве ("базиса Коши-Гамеля").

3. Теорема Хана-Банаха о существовании замкнутой гиперплоскости, разделяющей два выпуклых, непересекающихся, замкнутых под-

[1]Эту систему аксиом часто обозначают ZF+AC.

множества в топологическом векторном пространстве.

4. Теорема Тихонова о компактности произведения бесконечного количества компактов.

Аксиома выбора влечет много утверждений, которые не нужны для доказательства полезных теорем, и противоречат интуиции – наподобие парадокса Банаха-Тарского. Основная проблема, которая следует из принятия аксиомы выбора – существование **неизмеримых множеств**, множеств, для которых не определена мера Лебега (**мерой Лебега** в математике называется понятие "объема подмножества" в $\mathbb{R}^n$; неизмеримые подмножетва – подмножества, для которых не определен объем). Множества, которые фигурируют в парадоксе Банаха-Тарского, очевидно неизмеримы: иначе суммарный объем пяти частей, на которых разбит шар, не мог бы равняться удвоенному объему шара.

Существуют аксиомы теории множеств, которые противоречат аксиоме выбора; самая известная из них – аксиома детерминированности (axiom of determinacy), из которой, среди прочего, следует, что любое подмножество $\mathbb{R}^n$ измеримо.

Неизвестно, следует ли из непротиворечивости ZF+AC непротиворечивость системы Цермело-Френкеля с аксиомой детерминированности (ZF+AD). Другими словами, ZF+AD может оказаться противоречива, даже если ZF+AC непротиворечива. Поэтому ZF+AD не нашла широкого употребления.

Другая причина, по которой аксиомы, отрицающие аксиому выбора, не нашли употребления, такая. Пусть X и Y – два множества. Из аксиомы выбора следует, что X равномощно подмножеству Y, либо Y равномощно подмножеству X. Оказывается, что это утверждение *равносильно* аксиоме выбора. Поэтому из любой аксиомы, отрицающей аксиому выбора, следует существование таких множеств X и Y, что X не равномощно подмножеству Y, а Y не равномощно подмножеству X. Вместо изящной иерархии кардинальных чисел,[2] построенной Кантором, мы получаем огромное количество множеств, которые никак не соизмеримы по мощности.

Вместо использования аксиомы выбора можно пользоваться ее слабой формой, которая называется **аксиома зависимого выбора** (de-

[2]**Кардиналом**, или **кардинальным числом**, называется класс равномощных множеств. Согласно теореме Кантора-Бернштейна, если одно множество равномощно подмножеству другого, а другое – подмножеству первого, эти множества равномощны. Поэтому из двух неравномощных множества, одно равномощно подмножеству другого, но не наоборот. Это задает отношение порядка на кардинальных числах, которое и называется **иерархия кардиналов**.

pendent choice). Аксиома зависимого выбора утверждает следующее. Пусть дано множество X, и в нем подмножество $V \subset X \times X$ такое, что $\pi_1(V) = X$, где π_1 – проекция на первый сомножитель. Тогда есть бесконечная последовательность $\{x_i\}$ такая, что $(x_i, x_{i+1}) \in V$, для любого i.

Система аксиом Цермело-Френкеля без аксиомы выбора, но с зависимым выбором (ZF+DC) достаточна для почти всех задач, где необходим выбор, но недостаточна для утверждений 1-4, перечисленных выше. Также она следует из аксиомы детерминированности.

Любопытно, что непротиворечивость Цермело-Френкеля равносильна непротиворечивости системы аксиом, состоящей из ZF+DC плюс аксиомы "каждое подмножество $\mathbb{R}^n$ измеримо". Кроме того, DC следует из аксиомы детерминированности.

0.4. Вполне упорядоченные множества

Определение 0.1. Пусть X – множество, а $R \subset X \times X$ – бинарное отношение на множестве X, обозначенное $x_1 \prec x_2$. Это отношение называется **отношением частичного порядка** (partial order), если верны следующие утверждения

транзитивность: из $x \prec y$ и $y \prec z$ следует $x \prec z$.

асимметричность: если $x \prec y$, то невозможно $y \prec x$.

Множество $(X, \prec)$ с отношением частичного порядка называется **частично упорядоченное множество**.

Определение 0.2. Пусть $(X, \prec)$ – частично упорядоченное множество. Если для каких-то $x, y \in X$ имеет место $x \prec y$ либо $y \prec x$, мы говорим, что x и y **сравнимы**. Отношение $\prec$ называется **отношением линейного порядка** (total order), если любые два элемента сравнимы. Множество $(X, \prec)$ с отношением линейного порядка называется **линейно упорядоченное множество**.

Линейно упорядоченные множества также называются **монотонно упорядоченными**, или просто **упорядоченными**.

Если $x = y$ или $x \prec y$, мы пишем $x \preccurlyeq y$.

Определение 0.3. Пусть $(X, \prec)$ – линейно упорядоченное множество, а $Y \subset X$ – его подмножество. Элемент $y_0 \in Y$ называется **минимальным**, если для любого $y \in Y$, имеем $y_0 \preccurlyeq y$. Линейно упорядоченное множество называется **вполне упорядоченным** (well-ordered set), если любое его подмножество имеет минимальный элемент. Отношение порядка на таком множестве называется **отношение полного порядка**.

Определение 0.4. Начальным элементом вполне упорядоченного множества называется его минимальный элемент. **Отрезком** линейно упорядоченного множества $(X, \prec)$ называется подмножество $Y \subset X$ такое, что для любых $x, z \in Y$, и любого $y \in X$ такого, что $x \prec y \prec z$, имеем $y \in Y$. **Начальным отрезком** вполне упорядоченного множества называется отрезок, содержащий минимальный элемент.

Замечание 0.5. Пусть $X_0 \subset X$ – начальный отрезок вполне упорядоченного множества, x_0 его начальный элемент, а x – минимальный элемент в $X \backslash X_0$ (мы предполагаем, что это множество непусто). Легко видеть, что X_0 – множество всех y таких, что $x_0 \preccurlyeq y \prec x$ (докажите это). Мы обозначаем такой отрезок $[x_0, x[$.

Вполне упорядоченные множества изобрел Георг Кантор, создатель теории множеств. Кантор базировал свою теорию множеств на понятии вполне упорядоченного множества и понятии ординала.

Georg Ferdinand Ludwig Philipp Cantor
(1845 - 1918)

Определение 0.6. Два вполне упорядоченных множества называются **изоморфными**, если между ними есть биекция, сохраняющая порядок. Классы изоморфизма вполне упорядоченных множеств называются **ординалами**, или же **ординальными числами**.

Замечание 0.7. Ординалы можно складывать (для этого надо взять объединение $X \coprod Y$ двух непересекающихся вполне упорядоченных множеств, и положить $X \prec Y$). Это сложение некоммутативно, но ассоциативно. Кроме того, ординалы можно умножать. Полный порядок на произведении $X \times Y$ задается так:

$$(x, y) \prec (x', y') \text{ если } x \prec x', \text{ либо } x = x', y \prec y'.$$

Задача 0.8. Докажите, что эти определения задают вполне упорядоченные множества. Докажите ассоциативность и умножения и сложения и дистрибутивность слева сложения относительно умножения. Приведите примеры, когда сложение и умножение ординалов не коммутативно и не дистрибутивно справа.[1]

Теорема 0.9: Пусть X, Y – вполне упорядоченные множества. Тогда X изоморфно начальному отрезку Y, либо Y изоморфно начальному отрезку X. Более того, такой изоморфизм определен однозначно.

Доказательство: Пусть Z – множество пар (X_1, Y_1) изоморфных начальных отрезков X и Y.

Шаг 1. Изоморфизм начальных отрезков (X_1, Y_1) определяется однозначно множеством X_1. В самом деле, пусть существует два различных вложения $\varphi: X_1 \longrightarrow Y$ и $\varphi': X_1 \longrightarrow Y$, задающие изоморфизм X_1 и начального отрезка Y. Обозначим за x минимальный элемент X_1, такой, что $\varphi(x) \neq \varphi'(x)$. Тогда $\varphi\Big|_{[x_0, x[} = \varphi'\Big|_{[x_0, x[}$. Поскольку φ и φ' – изоморфизм, из этого следует, что $\varphi(x) = \varphi'(x)$.

Шаг 2. Мы получили, что Z упорядочено по включению и это задает на Z полный порядок (докажите). Пусть x – минимальный элемент X, не принадлежащий X_1 для какого-то $(X_1, Y_1) \in Z$. Если такого нет, это значит, что X изоморфен начальному отрезку Y. Если $Y_1 = Y$, мы все

[1]Дистрибутивность слева: $x \cdot (y + z) = x \cdot y + x \cdot z$. Дистрибутивность справа: $(y + z) \cdot x = y \cdot x + z \cdot x$.

доказали. В противном случае, начальный отрезок $[x_0, x[$ изоморфен начальному отрезку $[y_0, y[$, следовательно, отрезок $[x_0, x]$ изоморфен $[y_0, y]$. Мы пришли к противоречию. Это доказывает Теорему 0.9. ■

Теоремой Цермело называется следующее утверждение, доказанное Эрнстом Цермело в 1904-м году.

Теорема 0.10: (Теорема Цермело, "well-ordering theorem") Любое множество может быть вполне упорядочено.

Теорема Цермело равносильна аксиоме выбора; мы докажем это немного погодя.

0.5. Лемма Цорна и теорема Цермело

Другое утверждение, также равносильное аксиоме выбора - лемма Цорна.

Пусть $(S, \prec)$ – частично упорядоченное множество. Элемент $x \in S$ называется **максимальным**, если не существует $y \in S$ с $x \prec y$. Для подмножества $S_1 \subset S$ и $x \in S$, мы пишем $S_1 \preccurlyeq x$, если для каждого $\xi \in S_1$ имеем $\xi \preccurlyeq x$.

Теорема 0.11: (лемма Цорна) Пусть $(S, \prec)$ – частично упорядоченное множество, причем для любого вполне упорядоченного подмножества $S_1 \subset S$ найдется элемент $\xi \in S$ такой, что $S_1 \preccurlyeq \xi$. Тогда в S найдется максимальный элемент.

Теорема 0.12: Следующие утверждения равносильны:

ZL Лемма Цорна.

WOT Теорема Цермело.

AC Аксиома выбора.

Доказательство: Отметим, что полностью аккуратное доказательство Теоремы 0.12 требует развития аксиоматической теории множеств.

ZL $\Rightarrow$ WOT: Пусть X – любое множество, а S – множество всех пар $(X_1, \prec)$, где $X_1 \subset X$ – подмножество, а $\prec$ – отношение полного порядка на X_1.

Рассмотрим отношение частичного порядка на S: $(X_1, \prec) < (X_2, \prec)$, если $(X_1, \prec)$ это начальный отрезок $(X_2, \prec)$. Легко видеть, что условие леммы Цорна выполнено для $(S, <)$: если $S_1 \subset S$ вполне (и даже линейно) упорядочено, объединение $\Xi \subset X$ всех элементов S_1 с естественным отношением порядка – вполне упорядочено и удовлетворяет $S_1 \leqslant \Xi$. Поэтому в S есть максимальный элемент $(\Xi, \prec)$. Если $\Xi \neq X$, возьмем $\xi \in X \backslash \Xi$, и определим отношение порядка на $\Xi_1 := \Xi \cup \{\xi\}$, положив $\Xi \prec \xi$. Мы получим, что Ξ_1 – вполне упорядоченное множество, начальным отрезком которого является Ξ, а значит Ξ не максимально. Мы пришли к противоречию; следовательно $\Xi = X$. Поэтому X вполне упорядочено.

WOT $\Rightarrow$ AC: Пусть $X \xrightarrow{\varphi} Y$ – сюрьекция, а X вполне упорядочено. Определим отображение $Y \xrightarrow{\psi} X$, взяв за $\psi(y)$ минимальный (в смысле полного порядка) элемент $\varphi^{-1}(y)$. Легко видеть, что это сечение.

AC $\Rightarrow$ ZL.

Шаг 1: Пусть $(S, \prec)$ – частично упорядоченное множество, удовлетворяющее условиям леммы Цорна, и не содержащее максимального элемента. Тогда для каждого вполне упорядоченного подмножества $S_1 \subset S$, найдется $\xi \succcurlyeq S_1$. Поскольку ξ не максимален, найдется $\xi_1 \in S$ такой, что $\xi_1 \succ \xi$, а значит, $\xi \succ S_1$.

Шаг 2: Пусть $\mathfrak{S}$ – множество вполне упорядоченных подмножеств S, а $\gamma: \mathfrak{S} \longrightarrow S$ – отображение, переводящее $S_1 \subset S$ в элемент $\xi \in S$, удовлетворяющий $\xi \succ S_1$. Такое отображение существует в силу аксиомы выбора. Для доказательства этого, рассмотрим множество всех пар

$$\mathfrak{R} := \{(S_1 \in \mathfrak{S}, \xi \in S) \mid \xi \succ S_1\}$$

Естественная проекция $\mathfrak{R} \longrightarrow \mathfrak{S}$ сюрьективна, что доказано на шаге 1. Сечение $\mathfrak{R} \longrightarrow \mathfrak{S}$ в композиции с проекцией $\mathfrak{R} \longrightarrow S$ задаст искомое отображение γ.

Шаг 3: Пусть Θ – множество вполне упорядоченных подмножеств $P \subset S$ таких, что для каждого $p \in P$, начальный отрезок $[p_0, p[$ удовлетворяет $p = \gamma([p_0, p[)$. Когда $p = p_0$, это значит, что $p_0 = \gamma(\emptyset)$.

Множество Θ вполне упорядочено по вложению. В самом деле, возьмем $P, Q \in \Theta$, и пусть p – минимальный элемент P такой, что отрезок

$[p_0, p[$ лежит в Q, а $[p_0, p]$ уже не лежит в Q. Поскольку $p = \gamma([p_0, p[)$, а $[p_0, p[$ лежит в Q, из $p \notin Q$ следует, что $Q = [p_0, p[$.

Шаг 4: Мы получили, что объединение $P_\infty := \bigcup_{P \in \Theta} P$ лежит в Θ. Это невозможно, потому что объединение $P_\infty \cup \gamma(P_\infty)$ строго больше P_∞, и тоже лежит в Θ. Мы пришли к противоречию. Лемма Цорна доказана. ■