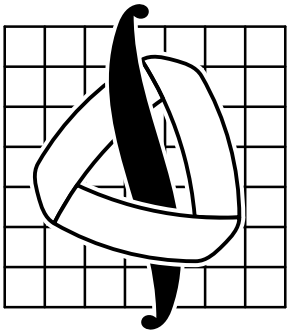
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА
Механико-математический факультет



Конспект спецкурса по математической логике

Лекторы — Лев Дмитриевич Беклемишев, Татьяна Леонидовна Яворская

III курс, 5 семестр, поток математиков

Москва, 2014 г.

Содержание

1. Теория множеств и философия оснований математики **5**
1.1. История вопроса . . . 5
1.2. Аксиоматика теории множеств ZFC . . . 6
1.2.1. Конечные аксиомы . . . 6
1.2.2. Натуральные числа . . . 7
1.3. Порядок и ординалы . . . 8
1.3.1. Линейные и полные порядки . . . 8
1.3.2. Ординалы . . . 10
1.4. Аксиома выбора . . . 13
1.4.1. Теорема Цермело и лемма Цорна . . . 13
1.4.2. Мощности и алефы . . . 15

2. Исчисление высказываний **19**
2.1. Аксиоматика Гильберта . . . 19
2.2. Интуиционистская логика высказываний . . . 22

Предисловие

Предлагаемый конспект охватывает материалы курса лекций по математической логике, прочитанного профессором кафедры математической логики и теории алгоритмов Львом Дмитриевичем Беклемишевым и доцентом кафедры Татьяной Леонидовной Яворской на механико-математическом факультете МГУ в 2014-2015 учебном году. Курс охватывает четыре основных раздела логики: теории множеств, моделей (теорема о полноте), доказательств (теорема о неполноте) и алгоритмов.

Данный текст ни в коем случае не претендует на истину в последней инстанции! Это не курс лекций, а лишь скромный конспект; вина за все опечатки и смысловые ошибки целиком и полностью возлагается на наборщика. Данный текст не ставит своей целью дать подробное объяснение и обоснование происходящего; за таковым рекомендуем обращаться к известным учебным пособиям, в частности, к «Введению в математическую логику» Э. Мендельсона и трёхтомник («Начала теории множеств», «Языки и исчисления», «Вычислимые функции») Верещагина и Шеня.

Эта сборка была скомпилирована 18 ноября 2014 г. Последняя версия документа всегда будет доступна на странице ВКонтакте `http://vk.com/id183071829`. Для пожеланий, критических замечаний и сообщений об опечатках можно использовать и электронный адрес `rudetection@gmail.com`.

Документ подготовлен Александром Запрягаевым, студентом группы 304, в издательской системе LaTeX. Особая благодарность Анастасии Оноприенко, Арсению Каданеру и Ираклию Глунчадзе за неоценимую помощь, без которой этот конспект не увидел бы свет.

Версия: `0.11`

Программа ВАК 01.01.06: математическая логика

1. Понятие алгоритма и его уточнения. Вычислимость по Тьюрингу, частично рекурсивные функции, рекурсивно перечислимые и рекурсивные множества. Тезис Чёрча.
2. Универсальные вычислимые функции. Существование перечислимого неразрешимого множества. Алгоритмические проблемы.
3. Построение полугруппы с неразрешимой проблемой распознавания равенства.
4. Классы P и NP. Полиномиальная сводимость и NP-полные задачи. Теорема об NP-полноте задачи ВЫПОЛНИМОСТЬ.
5. Логика высказываний. Представимость булевых функций формулами логики высказываний. Конъюнктивные и дизъюнктивные нормальные формы.
6. Исчисление высказываний. Полнота и непротиворечивость.
7. Логика предикатов. Приведение формул логики предикатов к предварённой нормальной форме.
8. Исчисление предикатов. Непротиворечивость. Теорема о дедукции. Полнота исчисления предикатов. Теорема Мальцева о компактности.
9. *Элементарные теории классов алгебраических систем. Категоричные в данной мощности теории. Теорема о полноте теории, не имеющей конечных моделей и категоричной в бесконечной мощности.
10. Разрешимые теории. Теория плотного линейного порядка.
11. Формальная арифметика. Теорема о представимости вычислимых функций в формальной арифметике (без доказательства).
12. *Теорема Гёделя о неполноте формальной арифметики. Теорема Тарского о невыразимости арифметической истинности в арифметике.
13. *Неразрешимость алгоритмической проблемы выводимости для арифметики и логики предикатов.
14. *Аксиоматическая теория множеств. Порядковые числа, принцип трансфинитной индукции. Аксиома выбора.

Начало лекции № 1 от 25 сентября 2014 г.

1. Теория множеств и философия оснований математики

> Я совершил ещё одно преступление, Хедли. Я снова разгадал правду.
>
> *Три гроба*
> Джон Диксон Карр

1.1. История вопроса

Осознанная история исследования аксиоматизации как отдельной научной проблемы восходит, пожалуй, к тем временам, когда Евклид в «Началах» изложил основы известной геометрии в наборе аккуратных аксиом. Сразу же возник вопрос об их избыточности и возможности вывода одних из них через другие. Под подозрение попал пятый постулат о параллельных[1], который на протяжении тысячелетий казался геометрам теоремой, выводимой из остальных утверждений. Однако многочисленные доказательства, даже если не содержали ошибок, где-нибудь всё равно использовали факт, в действительности эквивалентный пятому постулату[2]. Лобачевский произвёл революцию, предложив идею о возможности существования непротиворечивой геометрии с отрицанием пятого постулата, что означало бы, что его нельзя доказать или опровергнуть, возможно лишь принять за аксиому. Но что конкретно было доказано? Даже когда Бельтрами предложил псевдосферу, на поверхности которой двумерная плоскость Лобачевского реализуется в пространстве Евклида, не существовало сколько-нибудь полного осознания границ геометрии, полной аксиоматизации, которую можно было бы предъявить и сказать «мы работаем в ней».

Решающий вклад в проблему внёс Давид Гильберт в своей передовой работе Gründlagen der Geometrie (1899), излагающей некоторые аксиомы, вообще говоря, не являющиеся теорией первого порядка и изначально содержавшей одну лишнюю, выводимую из остальных, аксиому. Доработаны его идеи были Тарским (1959), который и доказал полноту такой теории.

Гильберт мечтал о том, что его последователи совершат аналогичную работу в аксиоматизации теперь уже теории чисел и анализа, изложив их в самых базовых из возможных понятий — на языке множеств. Но если первое до какой-то степени удалось, то со вторым возникли проблемы, связанные с несовершенством само́й наивной теории множеств. В известном парадоксе Рассела[3] предлагается рассмотреть множество вида $\{\, x \mid x \in x \,\}$, которое принадлежит самому себе тогда и только тогда, когда не принадлежит.

Таким образом, программа Гильберта диктовала аксиоматическое изложение уже самих знаний о множествах. Одними из первых были Рассел и Уайтхед с их «теорией типов», тщательно и формально собиравшей более сложные объекты из простых «кирпичиков». Но она крайне сложна для понимания и не обладает интуитивной наглядностью, естественностью изложения. Наиболее рациональную и общепринятую конструкцию предложил Э. Цермело (Zermelo) из школы Гильберта, к аксиомам которого А. Френкель (Fraenkel) добавил ещё две (регулярности и схему подстановки), в результате чего сложилась аксиоматика ZF теории множеств. Именно о ней[4] и пойдёт наш разговор. Насколько могут судить современные специалисты, эта система непротиворечива (по крайней мере, пока противоречия не найдено) и годится равно для всей математики.

[1] «И если прямая, падающая на две прямые, образует внутренние и по одну сторону углы, меньшие двух прямых, то продолженные неограниченно эти прямые встретятся с той стороны, где углы меньше двух прямых. . . »

[2] «Через точку, не лежащую на прямой можно провести прямую, параллельную данной, и притом только одну», «Сумма углов треугольника равна π», «Существуют подобные, но не равные треугольники» и т. д.

[3] Бертран Рассел сообщил его Фрегелю в ответ на статью последнего, где предлагалось описание теории чисел на языке предикатов, но при этом рассматривались слишком широкие классы множеств.

[4] Точнее, о ZFC, где добавлена аксиома выбора.

Эта теория страдает очевидным изъяном. Чтобы аксиомы имели смысл, нужно как-то доказать не только их непротиворечивость друг другу, но и реализуется в какой-то модели. А о какой модели может идти речь, когда мы сами этими аксиомами и строим те объекты, с которыми в дальнейшем работаем? Остаётся лишь поверить... Гильберт не до конца различал синтаксическое понятие непротиворечивости и семантическое — полноты. Поэтому после работ Гёделя настал серьёзный кризис. Как доказать, что ZFC непротиворечива? Вторая теорема о неполноте говорит, что этого нельзя сделать, оставаясь в рамках теории. А если бóльшей теории нет? И модель мы не предъявим — это будет сведéние к чему-то более сложному! Остаётся апеллировать к максимальной наглядности, свести утверждения о бесконечном к понятным конечным вещам, которые человеческая интуиция уже способна, по нашей вере, охватить. Итак, изнутри узнать, противоречива ли ZFC, невозможно, программа Гильберта провалилась — и всё же мы знаем больше, чем знали раньше.

Важно различать *теорию,* в которой мы работаем, формализуем её, подчиняем строгому своду правил, и *метатеорию* над ней, в качестве которой у нас всё время незримо будет выступать ZFC.

1.2. Аксиоматика теории множеств ZFC

> Consider the set of all sets that have never been considered. Hey! They're all gone!! Oh, well, never mind...
>
> Dr. David Batchelor

1.2.1. Конечные аксиомы

Пусть сигнатура состоит из двух символов бинарных отношений: $\sigma = \{\in, =\}$. Обозначение $x \in y$ будем читать как «x принадлежит y». Наличие обычных аксиом равенства (рефлексивность, транзитивность, симметричность, $x = x_1 \wedge y = y_1 \longrightarrow (x \in y \leftrightarrow x_1 \in y_1)$) подразумеваем без комментариев; иначе, считаем теорию *нормальной*. В некоторых вариациях аксиоматики предполагается ограничиться только отношением принадлежности, а равенство определять через него по следующей аксиоме-«определению»:

Аксиома 1.1 (Объёмности).

$$x = y \leftrightarrow \forall z(z \in x \leftrightarrow z \in y). \tag{1}$$

Начнём описывать, какие множества у нас будут допустимыми.

Аксиома 1.2 (Пары).

$$\forall x, y\, \exists z : \forall w(w \in z \leftrightarrow (w = x \vee w = y)). \tag{2}$$

Неформальный смысл: существует *неупорядоченная пара* x, y, состоящая из элементов x, y. Если взять один и тот же, то существует *синглетон* — множество x ровно из одного элемента. Возникает вопрос: а существует ли тройка, четвёрка и т. д.? Для их введения нам понадобится

Аксиома 1.3 (Объединения).

$$\forall x \exists y(y = \cup x). \tag{3}$$

Здесь под $\cup x$ мы подразумеваем множество, состоящее из объединения элементов всех его элементов:

$$y = \cup x \overset{\text{def}}{\iff} \forall z(z \in y \leftrightarrow \exists w \in x(z \in w)) \tag{4}$$

Отсюда мгновенно выводим стандартное понятие объединения двух множеств: $a \cup b \Leftrightarrow \cup\{a, b\}$. Теперь мы получаем и желанную тройку: $x, y, z \overset{\text{def}}{=} x, y \cup z$. Более того, имеем и неупорядоченные n-ки для любого n (хотя, оставаясь в рамках теории первого порядка, мы и не можем формально записать и доказать такое обобщение).

Следующая аксиома была предложена специально для ликвидации проблем в духе парадокса Рассела. Говоря неформально, мы хотим, чтобы для любого «свойства» φ (записанного формулой логики высказываний) и множества x существует его подмножество

$$\{\, y \in x \mid \varphi(y) \,\} \tag{5}$$

и не более. «Множества всех множеств» из теории исключаются. Записывая формально:

Аксиома 1.4 (Выделения (схема аксиом)).

$$\forall z (z \in y \leftrightarrow z \in x \wedge \varphi(z)). \tag{6}$$

Однако, такая запись недостаточно удовлетворительна. Смотрите: формул всего счётное число, значит, из любого по мощности множества можно выделить лишь счётное число различных подмножеств. Неужели мы имеем право описать лишь счётное число лучей вида

$$\varphi = \{\, \text{быть меньше } a \mid a \in \mathbb{R} \,\}? \tag{7}$$

Чтобы исправить проблему, оказывается, нужно заменить формулы на параметрические серии вида $\varphi = \varphi(t, \ldots)$. Тогда оказывается, что, например, предложенные лучи выделяются единственной формулой с зависимостью от a.

Внезапный вопрос на сообразительность: а почему по всем этим аксиомам вообще существует хотя бы одно множество? Ответ: мы не заостряли внимания, но, кроме аксиом равенства и смысловых математических аксиом, скрыто существуют и логические, утверждающие, среди прочего, что $\exists x\colon\ x = x$. Теперь, кстати, мы можем обосновать существование пустого множества: раз хоть какое-то множество w существует, выберем какое-нибудь свойство, которое заведомо ни для чего не выполняется ($x \neq x$), и выделим им пустое подмножество из w по аксиоме выделения. Аксиома объёмности, в свою очередь, гарантирует, что такое множество ровно одно; обозначим его привычным нам символом $\varnothing$.

В качестве упражнения теперь докажите:

Утверждение 1.1. $x \neq \varnothing \longrightarrow \exists y = \cap x$, *то есть* $\exists y\, (\forall z\, (z \in y \leftrightarrow \forall u \in x\, z \in u))$.

Аксиома 1.5 (Степени).

$$\forall x\, \exists y = P(x) \ - \textit{ множество всех подмножеств } x. \tag{8}$$

1.2.2. Натуральные числа

Впрочем, ни одна из имеющихся аксиом пока не гарантирует нам чего-то большего, нежели конечные множества. (Убедитесь, что совокупность всех конечных множеств является для уже описанных аксиом моделью!) Чтобы перейти к бесконечности, предъявим одно из них конструктивно и положим его существующим.

Определение. Множество X называется *индуктивным,* если

$$(\varnothing \in X) \wedge\ (\forall y \in X\, S(y) \stackrel{\text{def}}{=} (y \cup \{y\}) \in X). \tag{9}$$

Интуитивно: если мы обозначим $\varnothing$ за 0, $\varnothing \cup \{\varnothing\}$ за 1, $\varnothing \cup \{\varnothing \cup \{\varnothing\}\}$ за 2 и т. д., получим последовательность своего рода «натуральных чисел».

Теперь скажем, что такие последовательности существуют.

Аксиома 1.6 (Бесконечности).

$$\exists w\colon (\varnothing \in w \wedge (\forall y \in w\, S(y) \in w)) \tag{10}$$

Почему существует множество всех натуральных чисел $\mathbb{N}$[5]? Можно сказать, что мы фиксируем среди всех индуктивных множеств минимальное по включению; или же, мы просто берём $\bigcap_{I \text{ – индуктивно}} I$. Опять же, мы сказали неформально; для пущей строгости определим так.

[5] Логики пишут ω.

Определение. $\mathbb{N}$ — наименьшее из индуктивных множеств, то есть $\mathbb{N} \stackrel{\text{def}}{=} \bigcap\{J \subset I \mid J \text{ – индуктивно}\}$. Здесь I — какое-то индуктивное множество, минимальность подразумевается по включению.

Раз уж у нас появились числа, введём на них естественный порядок.

Определение. Пусть $n, m \in \mathbb{N}$. Тогда $n < m \stackrel{def}{\iff} n \in m$.

И операцию взятия следующего элемента.

Определение. $n + 1 \stackrel{\text{def}}{=} S(n) = n \cup \{n\}$.

Упражнение 1.1. *Докажите, что* $x < y + 1 \iff (x < y \vee x = y)$.

□

$$x < y + 1 \Leftrightarrow x \in y \cup \{y\} \Leftrightarrow x \in y \vee x = y \Leftrightarrow x < y \vee x = y. \tag{11}$$

■

Пора доказать на основании аксиом 1 – 6 фундаментальную теорему о свойстве натуральных чисел.

Теорема 1.2 (Принцип индукции). *Пусть* $0 \in A$, *и* $\forall n\,(n \in A \to n+1 \in A)$. *Тогда* $\forall n \in \mathbb{N}\, n \in A$, *то есть* $\mathbb{N} \subset A$.

□ $\mathbb{N} \cap A$ - индуктивно. Но $\mathbb{N}$ — минимальное по включению среди индуктивных $\Rightarrow$ $\mathbb{N} \cap A \equiv \mathbb{N}$, $\mathbb{N} \subseteq A$. ■

Это утверждение можно глубоко обобщить.

Теорема 1.3 (Порядковая индукция). *Если* $\forall n \in \mathbb{N}\,(\forall m < n\, m \in A \to n \in A)$, *то* $\mathbb{N} \subseteq A$.

□ Рассмотрим $A' \stackrel{\text{def}}{=} \{n \in \mathbb{N} \mid \forall m < n\, m \in A\}$. Докажем, что A' — индуктивно.

$0 \in A'$ — тривиально.

$n \in A' \to \forall (m < n)\, m \in A \xrightarrow{\text{предп. инд.}} n \in A \to n + 1 \in A \to \forall (m < n + 1)\, m \in A$. ■

Упражнение 1.2. *Всякое непустое подмножество натуральных чисел имеет наименьший элемент.*

Конец лекции № 1 от 25 сентября 2014 г. (к началу)

Начало лекции № 2 от 2 октября 2014 г.

1.3. Порядок и ординалы

> Дважды два равно четырём. И не здесь и сейчас, а всегда!
>
> Жак Фатрелл

1.3.1. Линейные и полные порядки

Определение. Пусть на множестве P задано бинарное отношение $<$. Будем говорить, что это *отношение частичного порядка,* если оно

1° иррефлексивно: $\forall x\, \neg(x < x)$;

2° транзитивно: $\forall x, y, z\,(x < y \wedge y < z) \to x < z$.

Само множество P называется при этом *частично упорядоченным множеством.*

Нас будут особо интересовать

Определение. *Линейные порядки* — это частичные порядки с дополнительным условием

3° $\forall x, y \in P\,(x = y \vee x < y \vee y < x)$ — любые два элемента сравнимы.

Очевидно, не все порядки линейны: рассмотрите отношение «быть делителем» на $\mathbb{N}$. Договоримся обозначать *нестрогий порядок* $x \leqslant y \Leftrightarrow x < y \vee x = y$. Введём понятия, характеризующие элементы в частично упорядоченном множестве:

Определение. *Максимальным (минимальным)* называется элемент X, такой, что $\neg\exists a\,(a > x)$ (соответственно, $(a < x)$).

Не путать со следующим определением!

Определение. *Наибольший (наименьший)* элемент x — это такой, что $\forall a\,(a \leqslant x)$ (соответственно, $a \geqslant x$).

Точно так же определяются эти элементы в подмножествах $A \subset X$.

Рассмотрим отношение делимости на $0, \dots, 10$. Там есть максимум, и даже не один (10, 9, 8, 7, 6 годятся), но не имеется наибольшего. Вообще, наибольший элемент, если он есть, является максимальным, но обратное, вообще говоря, неверно. Однако в линейном порядке эти понятия всё же эквивалентны.

Определение. Пусть $A \subset P; a \in P$ — *верхняя (нижняя) грань* A, если $\forall x \in A\, x \leqslant a$ (соответственно, $x \geqslant a$).

$a = \sup A$ *(точная верхняя грань), если* a *— наименьшая среди всех верхних граней. Аналогично определяется* $inf A$ *— наибольшая среди всех нижних граней.*

Пример 3.1. У множества $\{x \in \mathbb{Q} \mid x^2 \leqslant 2\}$ в $\mathbb{Q}$ много верхних граней, но точной нет.

Определение. Пусть $(P, <_P)$ и $(Q, <_Q)$ — частично упорядоченные множества. $f\colon P \to Q$ *возрастает (сохраняет порядок),* если

$$x < y \Rightarrow f(x) < f(y)\,\forall x, y \in P. \tag{12}$$

Определение. f — *изоморфизм (порядков),* если f сохраняет порядок и является биекцией между P и Q. Такие порядки $<_P$ и $<_Q$ называются *изоморфными.*

Пример 3.2. **1°** $\mathbb{N}$ и $\mathbb{Q}$ — не изоморфны (наименьший должен переходить в наименьший).

2° $\left(-\frac{\pi}{2}; \frac{\pi}{2}\right)$ и $\mathbb{R}$ — изоморфны (arctg).

3° $(0;1) \cup (2;3)$ и $\mathbb{R}$ - не изоморфны (изоморфизм монотонно возрастает в обычном числовом смысле, поэтому у него не более чем счётное число разрывов первого рода, но разрывов первого рода быть не может в силу существования обратного отображения).

4° $\mathbb{Q} \setminus \{a\}$ изоморфно $\mathbb{Q}$: «всё счётные плотные линейные порядки без первого и последнего элемента изоморфны» (а несчётные — совсем нет).

Решающим определением в этом разделе курса станет следующее.

Определение. Пусть $(P, <_P)$ — линейный порядок. P называется *вполне упорядоченным множеством,* если $\forall A \subset P$ A обладает наименьшим элементом.

Пример 3.3. $(\mathbb{N}, <)$.

Какова наша основная цель? Отношение порядкового изоморфизма разбивает все вполне упорядоченные множества на классы эквивалентности — так называемые «порядковые типы». Будем их изучать.

Утверждение 1.4 (О монотонности). *Пусть* $(W, <)$ *— вполне упорядочено;* $f\colon W \to W$ *возрастает. Тогда* $\forall x \in W\ f(x) \geqslant x$.

□ От противного. Пусть $A \stackrel{\text{def}}{=} \{x \mid f(x) < x\} \neq \varnothing$. $A \subseteq W \Rightarrow \exists a$ — наименьший элемент A. Что можно сказать про $f(a)$? $f(a) < a$, поскольку $a \in A$. Но f возрастает, поэтому применим к неравенству f ещё раз: $f(f(a)) < f(a)$. Обозначив $b = f(a)$, имеем $f(b) < b$. Но $b < a \Rightarrow b \neq a \Rightarrow f(b) \geqslant b$ в силу того, что a был в A наименьшим. Противоречие. ■

Следствие 1.1. *Пусть* $(W, <)$ *— вполне упорядочено;* $f\colon W \to W$ *— автоморфизм*[6]*. Тогда* $f(x) = x\,\forall x \in W$.

□ По доказанному, $f(x) \geqslant x\ \forall x$. Но существует f^{-1} — тоже автоморфизм, и $f^{-1}(x) \geqslant x$. Навешивая f, имеем $f(f^{-1}(x)) = x \leqslant f(x) \Rightarrow f(x) \equiv x$. ■

Следствие 1.2. *Если* $(W_1, <_1)$ *и* $(W_2, <_2)$ *- изоморфные вполне упорядоченные множества, то их изоморфизм — единственен.*

□ Пусть $f, g\colon W_1 \to W_2$ — два изоморфизма. Тогда $\mathrm{id}_{W_2} = f \circ g^{-1}\colon W_2 \to W_2$ — автоморфизм; $\mathrm{id}_{W_1} = g^{-1} \circ f\colon W_1 \to W_1$ — автоморфизм $\Rightarrow f = (g^{-1})^{-1} = g$. ■

[6] То есть изоморфизм в себя.

Определение. Пусть $(W, <)$ — вполне упорядоченное множество, $u \in W$. *Начальным отрезком* W назовём подмножество $W(u) \stackrel{\text{def}}{=} \{x \in W \mid X < u\}$. В силу того, что минимальные элементы в подмножествах сохраняются, начальный отрезок — тоже вполне упорядочен.

Утверждение 1.5 (О неизоморфности). *Пусть $(W, <)$ — вполне упорядочено. Тогда ни для какого $u \in W$ W и $W(u)$ не изоморфны.*

□ Если $f\colon (W, <) \leftrightharpoons (W(u), <)$ — изоморфизм, то $f(u) \in W(u) \Rightarrow f(u) < u$. Противоречие. ■

Теорема 1.6 (О порядке на полных порядках). *Пусть W_1, W_2 — два вполне упорядоченных множества. Тогда имеет место одна из трёх возможностей:*

1° *W_1 и W_2 изоморфны;*

2° *W_1 изоморфно $W_2(u)$ для некоторого u;*

3° *W_2 изоморфно $W_1(u)$ для некоторого u.*

Неформально: любые два вполне упорядоченных множества сравнимы.

□ Обозначим $f \subseteq W_1 \times W_2$, $f \stackrel{\text{def}}{=} \{\langle x, y\rangle \in W_1 \times W_2 \mid W_1(x) \text{ и } W_2(y) \text{ изоморфны}\}$. Тогда f функционально и инъективно (воспользуйтесь только что доказанным утверждением 1.5 (О неизоморфности)!). f сохраняет порядок: пусть $W_1(x_1)$ и $W_2(f(x_1))$ изоморфны, $W_1(x_1)$ и $W_2(f(x_1))$ — тоже, где $W_1(x_1) \subseteq W_1(x_2)$. Второй изоморфизм будет служить продолжением первого, откуда $W_2(f(x_1)) \subseteq W_2(f(x_2))$, что и влечёт $f(x_1) < f(x_2)$.

Обозначим:

$$\begin{aligned} \operatorname{dom} f &= \{x \mid \exists y \ \langle x, y\rangle \in f\} \\ \operatorname{ran} f &= \{y \mid \exists x \ \langle x, y\rangle \in f\} \end{aligned} \tag{13}$$

Возможны следующие варианты:

A° $\operatorname{dom} f = W_1$, $\operatorname{ran} f = W_2$ — это первый пункт.

B° $\operatorname{ran} f \neq W_2$, $W_2 \setminus \operatorname{ran} f \neq \varnothing$. Выберем наименьший элемент в $W_2 \setminus \operatorname{ran} f$, то есть $\operatorname{ran} f = W_2(y)$. Допустим, при этом оказалось, что $\operatorname{dom} f \neq W_1$. Тогда[7] $\operatorname{dom} f = W_1(x)$, $x \in W_1$. Но это влечёт $\langle x, y\rangle \in f \Leftrightarrow y \in \operatorname{ran} f$ — противоречие с выбором y. Итак, $\operatorname{dom} f = W_1$ — второй пункт.

C° $\operatorname{dom} f \neq W_1$ — аналогично. ■

1.3.2. Ординалы

> Дети прекрасно знают, что считать можно до бесконечности. Они стремятся превзойти друг друга, говоря «бесконечность», затем «бесконечность плюс один», и так далее.
>
> Саймон Сингх

Чтобы не рассуждать о «классах эквивалентности вполне упорядоченных множеств», введём соответствующую аксиоматику: предъявим по конкретному множеству каждого класса и будем изучать их.

Определение. Множество A называется *транзитивным,* если $\forall X \ (x \in A \to x \subseteq A)$.

Определение. A — *ординал,* если

1° A — транзитивно;

2° $(A, \in)$ вполне упорядочено (по отношению принадлежности).

Ординалы существуют: сразу понятно, что $\varnothing$ — ординал. $\{\varnothing\}$, $\{\varnothing, \{\varnothing\}\}$, $\{\varnothing, \{\varnothing, \{\varnothing, \{\varnothing\}\}\}\}$ — все тоже таковы, и так далее.

Возьмём Ord — *класс* всех ординалов. На нём установим порядок: $\forall \alpha, \beta \in \text{Ord}$, $\alpha < \beta \stackrel{\text{def}}{\iff} \alpha \in \beta$. Докажем ряд простых свойств, вытекающих из этих определений.

Конец лекции № 2 от 2 октября 2014 г. (к началу)

[7] Если $x_2 \in \operatorname{dom} f$ и $x_1 < x_2$, то $x_1 \in \operatorname{dom} f$.

Начало лекции № 3 от 9 октября 2014 г.

Лемма 1.7 (Свойства ординалов).

1° $0 = \varnothing \in \mathrm{Ord}$.

2° $\alpha \in \mathrm{Ord} \wedge \beta \in \alpha \Rightarrow \beta \in \mathrm{Ord}$.

3° $\alpha, \beta \in \mathrm{Ord} \wedge \alpha \subsetneq \beta \Rightarrow \alpha \in \beta$.

4° $\alpha, \beta \in \mathrm{Ord} \Rightarrow \alpha \subset \beta$ *или* $\beta \subset \alpha$.

□ **1°** Очевидно.

2° $\beta \in \alpha \Rightarrow \beta \subseteq \alpha$.

$(\alpha, \in)$ вполне упорядочено $\Rightarrow (\beta, \in)$ вполне упорядочено.

Покажем транзитивность: $y \in x \in \beta (\in \alpha) \Rightarrow$ (ибо $\beta \subseteq \alpha$ из транзитивности) $y \in x \in \alpha \overset{x \subseteq \alpha}{\Longrightarrow} \beta \in \alpha, x \in \alpha, y \in \alpha, y \in x \in \beta$. Но $\in$ на α — отношение порядка. Поэтому $y \in \beta$.

3° $\beta \setminus \alpha \neq \varnothing$. Возьмём какой-нибудь $\gamma \in (\beta \setminus \alpha)$. $\alpha = \beta(y) = \{x \in \beta \mid x < y\}$. В самом деле, пусть $x \in \alpha, x \geqslant \gamma$. Тогда либо $\gamma \in x \in \alpha$, либо $\gamma = x \in \alpha$, и в обоих случаях $\gamma \in \alpha$, вопреки выбору γ.

Итак, $\alpha = \{x \in \beta \mid x \in \gamma\} = y \in \beta \Rightarrow \alpha \in \beta$.

4° $\gamma = \alpha \cap \beta \in \mathrm{Ord}$ (проверьте пункты определения руками). Допустим, $\gamma \neq \alpha \wedge \gamma \neq \beta$. Из этого следует, что $\gamma \in \alpha \wedge \gamma \in \beta \Rightarrow \gamma \in (\alpha \cap \beta) = \gamma$. Но это противоречит определению ординала, требовавшего строгого порядка! Значит, или $\gamma = \alpha \Rightarrow \alpha \subset \beta$, или $\gamma = \beta \Rightarrow \beta \subset \alpha$. ■

Выведем ряд простых и важных следствий.

Следствие 1.3.

1° $<$ — *линейный порядок на Ord.*

2° $\forall \alpha \in \mathrm{Ord}\ \alpha = \{\beta \in \mathrm{Ord} \mid \beta < \alpha\}$.

3° $C \neq \varnothing, C \subseteq \mathrm{Ord} \Rightarrow \cap C \in \mathrm{Ord}, \cap C \in C, \cap C = \inf C$.

4° *Пусть* $X \neq \varnothing$, X — *множество ординалов. Тогда* $\cup X \in \mathrm{Ord}$, *и* $\cup X = \sup X$.

5° $\forall \alpha \in \mathrm{Ord}\ \alpha \cup \{\alpha\} \in \mathrm{Ord}, \alpha \cup \{\alpha\} = \inf\{\beta \in \mathrm{Ord} \mid \beta > \alpha\}$.

□ **1°** $\alpha \in \beta \in \gamma \Rightarrow \alpha \in \gamma$, так как γ — транзитивно.

$\alpha, \beta \in \mathrm{Ord} \Rightarrow \Rightarrow \alpha \subset \beta$ или $\beta \subset \alpha \Rightarrow \alpha = \beta \vee \alpha \in \beta \vee \beta \in \alpha$.

2° Очевидно; $\subseteq$ по п. 2 леммы 1.7 (Свойства ординалов).

3° $\cap C \in \mathrm{Ord}$ — очевидно.

$\alpha \in C, \cap C \subseteq \alpha \Rightarrow (\cap C) \in \alpha \in C$.

Если $\cap C \notin C$, то $\forall \alpha \in C\ \neg \alpha = \cap C \Rightarrow \forall \alpha \in C\ \cap C \in \alpha \Rightarrow \cap C \in \cap C$ — противоречие.

4° $Y \subseteq (\cup X)$.

$\{\alpha \in X \mid \alpha \cap Y \neq \varnothing\}$.

5° Простая проверка показывает, что свойство транзитивности наследуется на $\alpha \cup \{\alpha\}$. Упорядоченность тоже присутствует: мы просто объявили элемент α больше всех ранее имевшихся, ибо все прежние принадлежат α и потому меньше. Итак, $\alpha \cup \{\alpha\}$ — ординал. То, что он является какой-то верхней гранью, понятно из построения. Почему она точна? Если $\gamma > \alpha$, то $\alpha\gamma \Rightarrow \alpha \subseteq \gamma$. ■

Такой ординал $\alpha \cup \{\alpha\}$ называется *последовательным ординалом.* Бывают и *предельные,* не представимые в таком виде.

Теорема 1.8. *Пусть* $(W, <)$ — *вполне упорядочено. Тогда* $\exists!\, \alpha \in \mathrm{Ord}\colon \alpha \simeq (W, <)$.

□ Единственность сразу следует из того, что разные ординалы являются начальными отрезками друг друга и поэтому попарно неизоморфны. Докажем существование.

Аксиома 1.7 (Замены).

$$\forall x, y, z(\varphi(x, y, \vec{p}) \wedge \varphi(x, z, \vec{p}) \to y = z) \to \forall X \exists Y \forall y (y \in Y \leftrightarrow \exists x \in X\, \varphi(x, y, \vec{p})). \tag{14}$$

Пусть $x \in W$. Обозначим

$$W(x) \stackrel{\text{def}}{=} \{y \in W \mid y < x\}. \tag{15}$$

Определим бинарное отношение $x(\in W)\, F\, \alpha(\in \mathrm{Ord}) \stackrel{\text{def}}{=} \alpha =\!\simeq W(x)$, $F(x) = \alpha$.

$F(W) = \{F(x) \mid x \in W\}$ — множество.

Докажем, что F всюду определена на W. От противного: иначе существует наименьший элемент: $y \in \{x \in W \mid F(x) \text{ не определена}\} \subseteq W$. Но тогда $\forall z < y\, W(z)$ изоморфно $F(z)$.

$W(y)$ изоморфно $\bigcup\limits_{z<y} F(z)$. Противоречие с выбором y. (За $\varphi(x, \alpha)$ берём «α — ординал, и $W(x)$ изоморфно α»).

Итак, F всюду определено на W. Тогда существует наименьший ординал $\gamma \notin F(W) \subseteq \mathrm{Ord}$. (Почему в $\mathrm{Ord} \setminus F(W)$ есть элементы? Рассмотрим $\cup F(W) + 1 \notin F(W)$ заведомо.) Тогда $F(W) = \{F(x) \mid x \in W\} = \gamma$ (в силу минимальности γ, во все меньшие что-то обязано перейти!). Но тогда F - это изоморфизм между W и ординалом γ. ■

Если $\alpha = \beta{+}1$, то он последовательный. Иначе $\alpha = sup\{\beta \mid \beta < \alpha\} = \cup\alpha$ — предельный ординал. Наименьший предельный ординал (натуральные числа) называется ω.

Теорема 1.9. *Пусть $C \subset \mathrm{Ord}$, такое, что:*

1° $0 \in C$.

2° $\forall \alpha \in \mathrm{Ord}\, (\alpha \in C \Rightarrow \alpha + 1 \in C)$.

3° *Если $\alpha \neq 0$ и α — предельный, то $\forall \beta < \alpha\, (\beta \in C \Rightarrow \alpha \in C)$.*

Тогда $C = \mathrm{Ord}$.

Конец лекции № 3 от 9 октября 2014 г. (к началу)

Начало лекции № 4 от 16 октября 2014 г.

□ Если $C \neq \mathrm{Ord}$, то рассмотрим наименьший ординал, не принадлежащий C, и получаем противоречие. ■

Определение. Трансфинитная последовательность: $\langle \alpha_\xi \mid \xi < \alpha \rangle$ ($\alpha \in \mathrm{Ord}$ — *длина* этой последовательности).

Пусть G — функция, заданная на последовательностях.

Теорема 1.10 (Трансфинитная рекурсия). $\forall \Theta\ \exists!\ \langle a_\xi \mid \xi < \Theta \rangle$ *такое, что* $a_\alpha = G(\langle a_\beta \mid \beta < \alpha \rangle)\ \forall \alpha < \Theta$.

Теорема 1.11. *Пусть V — класс трансфинитных последовательностей, G — функция на V. Тогда $\exists!\ F$ — функция на* Ord*: $\forall \alpha \in \mathrm{Ord}\ F(\alpha) = G(F|\alpha)$. $F|\alpha = \langle F(\xi) \mid \xi < \alpha \rangle$ — множество.*

Пример 3.4. Рассмотрим примеры применения теоремы. Определим сложение ординалов так:

$$\begin{cases} \alpha + 0 = \alpha, \\ \alpha + (\beta + 1) = (\alpha + \beta) + 1, \\ \alpha + \beta = \lim\limits_{\xi \to \beta} (\alpha + \xi), & \beta \text{ — предельный.} \end{cases} \tag{16}$$

(Здесь $\lim\limits_{\xi \to \beta} (\alpha{+}\xi) = \sup\{\alpha{+}\xi \mid \xi < \beta\}$.) Тогда существует функция $+\colon \mathrm{Ord} \times \mathrm{Ord} \to \mathrm{Ord}$, обладающая свойствами 1—3. В самом деле: определим такую функцию G_α следующим образом: $G_\alpha(\Lambda) = \alpha$, $G_\alpha(\langle a_\xi \mid \xi < \gamma \rangle) =$

$$\begin{cases} a_\beta + 1, & \gamma = \beta + 1, \\ \sup\{a_\xi \mid \xi < \gamma\}, & \gamma \text{ — предельная.} \end{cases} \tag{17}$$

Теперь применим теорему.

Умножение:

$$\begin{cases} \alpha \times 0 = 0, \\ \alpha \times (\beta + 1) = \alpha \times \beta + \alpha, \\ \alpha + \lambda = \sup\limits_{\beta < \lambda} (\alpha \times \beta), & \lambda \text{ — предельный.} \end{cases} \tag{18}$$

Возведение в степень:

$$\begin{cases} \alpha^0 = 1, \\ \alpha^{\beta+1} = \alpha^\beta \times \alpha, \\ \alpha^\lambda = \sup\limits_{\beta<\lambda}(\alpha^\beta), \qquad \lambda \text{ — предельный.} \end{cases} \tag{19}$$

Посчитаем: $1 + \omega = \sup\limits_{n<\omega}(1+n) = \omega \neq \omega + 1$, $2 \times \omega = \omega$ и т. д.

□ Докажем единственность. Пусть F_1 и F_2 — функции на Ord, и $F_i(\alpha) = G(F_i\big|_\alpha)$, $i = 1, 2$. Предположим, что $\exists\,\alpha\colon\ F_1(\alpha) \neq F_2(\alpha)$. Класс всех таких α непуст. Пусть $\alpha_0 = \min\{\alpha \in \mathrm{Ord} \mid F_1(\alpha) \neq F_2(\alpha))\}$. Тогда $\forall\beta < \alpha_0\ F_1(\beta) = F_2(\beta)$, $F_1\big|_{\alpha_0} = F_2\big|_{\alpha_0}$. Но при этом $F_1(\alpha_0) = F_2(\alpha_0)$ — противоречие.

Докажем существование. Рассмотрим $\mathscr{F}$ — семейство всех функций f таких, что $\mathrm{dom}(f) \in \mathrm{Ord}$, и $\forall\alpha \in \mathrm{dom}(f)\ f(\alpha) = G(f\big|_\alpha)$. Это семейство непусто: например, $\varnothing \in \mathscr{F}$. Далее, пусть $\mathrm{dom}\, f = 1 = \{0\} = \{\varnothing\}$. Тогда, если $f(0) = G(f\big|_0) = G(0)$, то $f \in \mathscr{F}$.

Положим $F \stackrel{\text{def}}{=} \bigcup \mathscr{F}$. Что нужно проверить?

1° F — функция.

2° $\mathrm{dom}\, F = \mathrm{Ord}$.

3° $\forall\alpha \in \mathrm{Ord}\ F(\alpha) = G(F|\alpha)$.

Нам понадобится следующая

Лемма 1.12. *Если* $\mathrm{dom}(f_1) = \alpha < \beta = \mathrm{dom}(f_2)$ *$(f_1, f_2 \in F)$, то* $f_1 \subseteq f_2$.

□ Аналогично единственности. ■

Это сразу доказывает первый пункт. Обоснуем второй. Если бы $\mathrm{dom}(F) \neq \mathrm{Ord}$, то мы бы выбрали $\alpha_0 = \min(\mathrm{Ord} \setminus \mathrm{dom}\, F)$. Тогда $\forall\beta < \alpha_0\ \beta \in \mathrm{dom}\, F$. Значит, существует такая конкретная $f \in \mathscr{F}$, что определено $f(\beta)$. Но f определена на каком-то ординале. Проверим третье. $F\big|_{\alpha_0}$ у нас определено, положим $x \stackrel{\text{def}}{=} G(F\big|_{\alpha_0})$, $f_0 \stackrel{\text{def}}{=} (F\big|_{\alpha_0}) \cup \{\langle\alpha_0, x\rangle\}$, то есть продолжили $F\big|_{\alpha_0}$ до f_0, положив $f(\alpha_0) \stackrel{\text{def}}{=} x$. По построению, $f_0 \in \mathscr{F}$, $\mathrm{dom}(f_0) = \alpha_0 + 1$. Противоречие. ■

Ключевым моментом было использование аксиомы подстановки: нужно, чтобы $F\big|_\alpha$ было множеством, ведь только множества можно подставлять в G!

1.4. Аксиома выбора

1.4.1. Теорема Цермело и лемма Цорна

> The Axiom of Choice is obviously true, the well-ordering principle obviously false, and who can tell about Zorn's lemma?
>
> Jerry Bona

Аксиома 1.8 (Выбора, AC). *Пусть S — класс, состоящий из непустых множеств. Тогда $\exists\, f\colon S \to \cup S$ такая, что $\forall x \in S\ f(x) \in x$.*

Особенность этой аксиомы — невозможность явно предъявить эту функцию, можно лишь утверждать её существование. Следующие два неконструктивных утверждения не только следуют из аксиомы выбора, но и эквивалентны ей:

Теорема 1.13 (Цермело, принцип вполне упорядочения). *Пусть X — произвольное множество; тогда существует такое отношение $<$ на X, что $(X, <)$ — вполне упорядочено.*

Лемма 1.14 (Цорна). *Пусть $(X, <)$ — частично упорядоченное множество, и всякая цепь[8] в нём обладает верхней гранью. Тогда в X имеется максимальный элемент.*

[8] То есть линейно упорядоченное подмножество.

Пример 4.1. Существует *базис Гамеля* $\mathbb{R}$ *над* $\mathbb{Q}$, то есть такое подмножество векторов $B \subset \mathbb{R}$, что

$$\forall x \in \mathbb{R}\ \exists!\, r_1, \ldots, r_n \in B,\ \exists!\, q_1, \ldots, q_n \in \mathbb{Q}\colon\ x = q_1 r_1 + q_2 r_2 + \ldots + q_n r_n.$$

□ Используем лемму Цорна. Назовём множество B *линейно независимым над* $\mathbb{Q}$, если

$$\forall r_1, \ldots, r_n \in B\ \forall q_1, \ldots, q_n \in \mathbb{Q}\ \ q_1 r_1 + q_2 r_2 + \ldots + q_n r_n = 0 \Longleftrightarrow q_1 = \ldots = q_n = 0. \tag{20}$$

Положим $\mathscr{B} \stackrel{\text{def}}{=} \{B \subseteq \mathbb{R} \mid B$ — линейно независимо над $\mathbb{Q}\}$. Рассмотрим какую-нибудь цепь в $\mathscr{B}$: объединив все её вложенные друг в друга линейно независимые подмножества, получим тоже линейно независимое. В самом деле, любая линейная комбинация, по определению, конечна, и каждый вектор в ней пришёл из какого-то конкретного множества в объединении. Их только конечное число, поэтому можно найти среди них наибольший по включению. В нём лежат все наши векторы линейной комбинации, но он уже был линейно независимым, поэтому все коэффициенты в линейной комбинации равны нулю.

Применяя лемму Цорна, устанавливаем существование такого максимально линейно независимого подмножества $B_0 \subseteq \mathbb{R}$ (по включению), что к нему нельзя добавить больше ни одного нового вектора, не нарушив линейной независимости. Оно и будет искомым базисом. ■

Конец лекции № 4 от 16 октября 2014 г. (к началу)

Начало лекции № 5 от 23 октября 2014 г.

□ **1. Аксиома выбора ⇒ лемма Цорна.**

От противного: пусть $(A, <)$ — частично упорядоченное множество, в котором всякая цепь имеет верхнюю грань, но нет максимального элемента. Зафиксируем какую-нибудь цепь C : тогда $\exists a \forall x \in C\,(a > x)$ — так называемая «строгая верхняя грань» C. В самом деле: пусть b — какая-то верхняя грань C (существует по условию). b — не максимум, поэтому $\exists d > b \geqslant x \in C$, его и возьмём. Обозначим $\Psi(C) = \{a \mid a$ — строгая верхняя грань $C\}$. $\Psi \subseteq P(A) \times P(A)$, поэтому это множество. Пусть $S = \{\Psi(C) \mid C$ — цепь в $A\}$. Это тоже множество (подмножество $P(A)$). Применяем аксиому выбора: $\exists f \forall C\, f(\Psi(C)) \in \Psi(C)$. Положим $\varphi(C) \stackrel{\text{def}}{=} f(\Psi(C)) \in \Psi(C)$ и используем это отображение, чтобы построить слишком большую цепь, которая не поместится в A и приведёт к противоречию.

Назовём $B \subseteq A$ *корректным,* если:

1° $(B, <)$ — вполне упорядочено,

2° $\forall x \in B\ x = \varphi(B_x)$, $B_x \stackrel{\text{def}}{=} \{y \in B \mid y < x\}$.

Корректные множества бывают: например, $\varnothing$; $\{\varphi(\varnothing)\}$; $\{\varphi(\varnothing), \varphi(\{\varphi(\varnothing)\})\}$ и т. д.

Лемма 1.15.

1° *Если* B, D *корректны, то одно из них — начальный отрезок другого.*

2° *Если* $\mathcal{T}$ *— семейство корректных множеств, то и* $\cup\mathcal{T}$ *— корректно.*

□ **1°** Пусть множества даны как в формулировке. Скажем, что I_0 — *общее начало* B и D, если оно является начальным отрезком их обоих. Обозначим $I \stackrel{\text{def}}{=} \{I_0 \mid I_0$ — общее начало B и $D\}$. Тогда I само по себе оказывается их общим началом. В самом деле: пусть $x \in I$; тогда $\exists I_0\ (x \in I_0)$. Но тогда всякий $y \in B$, меньший x, тоже лежит в этом I_0, то есть $y \in I$.

Если $I = B \vee I = D$, то всё доказано: одно из множеств — начальный отрезок второго. Пусть, однако, $I \neq B$, $I \neq D$. Это даёт нам возможность (по вполне упорядоченности!) выбрать $b \stackrel{\text{def}}{=} \min_B(B \setminus I)$, $d \stackrel{\text{def}}{=} \min_D(D \setminus I)$. I — общее начало для B и D; поэтому (второй пункт определения корректности) $b = \varphi(B_b) = \varphi(D_d) = d$, ибо $B_b = D_d = I$. Но теперь у нас $I \cup \{b\}$ — общее начало для B и D, бóльшее, нежели объединение всех общих начал. Противоречие.

2° Пусть теперь $\mathcal{T}$ — семейство корректных множеств, $U = \cup\mathcal{T}$. Тогда выполняются следующие факты.

1. $(U, <)$ — линейный порядок (по пункту 1).

2. $\forall B \in \mathcal{T}\ B$ — начальный отрезок для U. Проверим: пусть $x \in B$, $y \in U$, $y < x$. Если существует $y \notin B \Leftrightarrow y \in U \setminus B$. $\exists D \in \mathcal{T}\ (y \in D) \Rightarrow y \in D \setminus B$. По пункту 1, имеем два корректных множества B и D, причём понятно, что именно B — начальный отрезок D (в D есть элемент, которого нет в B). Но тогда и $y \in B$. Противоречие.

3. $(U, <)$ — вполне упорядочено. В самом деле: пусть $Y \subseteq U$, $Y \neq \varnothing$. Поскольку $Y \subseteq \cup\mathcal{T}$, то $\exists B \in \mathcal{T}$ $(y \in B)$, $y \in Y \cap B \neq \varnothing$. Значит, $\exists m$ — наименьший элемент в Y. Тогда m — наименьший и в Y (рассмотрим элемент $x \in Y$, $x < y$).

4. Выполняется $\forall x \in U\ x = \varphi(U_x)$. Почему? Возьмём $x \in B \in \mathcal{T}$. Тогда $x = \varphi(B_x)$. Но B, в свою очередь, является начальным отрезком в U, откуда $B_x = U_x$, и $x = \varphi(U_x)$. ■

Теперь мы готовы доказать лемму Цорна. Положим Σ — семейство *всех* корректных подмножеств $B \subseteq A$. $U = \cup\Sigma$ — вполне упорядочено $\Rightarrow$ U — цепь, а $\varphi(U)$ — строгая верхняя грань для U. Тогда $U \cup \{\varphi(U)\}$ удовлетворяет определению корректного множества (полагаем новый элемент больше всех прежних, $B_x = U$). Но оно больше объединения всех корректных. Противоречие.

2. Лемма Цорна $\Rightarrow$ теорема Цермело.

Хотим для заданного множества X построить $<\subseteq X^2$, чтобы $(X, <)$ стало вполне упорядоченным. Для $S \subseteq X$ будем рассматривать $\{(S, <_s) \mid (S, <_s) \text{ — вполне упорядочено}\} \stackrel{\text{def}}{=} W(x)$. Введём порядок: $(S, <_s) \prec (T, <_t) \leftrightharpoons S \subsetneq T$ — начальный отрезок в $(T, <_T)$, и $<_S = <_T\big|_S$. Тогда оказывается, что $(W(x), \prec)$ удовлетворяет условиям леммы Цорна: пусть C — цепь в $(W(x), <)$; тогда, например, $\left(\bigcup\limits_{(S,<_S)\in C} S,\ \bigcup\limits_{(S,<_S)\in C} <_S\right) \in W(x)$ является верхней гранью C в $(W(x), \prec)$.

Итак, в $(W(x), \prec)$ есть максимальный элемент $(M, <_M)$. Если мы докажем, что $M = X$, то всё готово. От противного: пусть $M \subsetneq X$; $a \in X \setminus M$. Тогда $(M, <_M) < (M \cup \{a\}, <_M \cup \{(m, a) \mid m \in M\}) \in W(x)$. Противоречие с идеей о максимальности $(M, <_M)$ завершает доказательство.

Теорема 1.16 (Кантора, о сравнении мощностей). $\forall A, B\ (\exists f\colon A \to B) \vee (\exists f\colon A \to B)$ — *инъективное, то есть мощность одного не превосходит мощности другого, и они сравнимы.*

□ Вполне упорядочим оба множества и вспомним, что из двух вполне упорядоченных множеств одно является начальным отрезком другого. ■

3. Теорема Цермело $\Rightarrow$ аксиома выбора.

Здесь доказывать, собственно говоря, уже нечего: если $(A, <_A)$, $X \subseteq A$, то положим $f(x) \stackrel{\text{def}}{=} \min_{<_A} X \in X$, что будет искомой функцией выбора. ■

Следствие 1.4. $(\mathbb{R}, +)$ *и* $(\mathbb{C}, +)$ *изоморфны как группы.*

□ Установим изоморфизм по базисам Гамеля мощности континуум. ■

Конец лекции № 5 от 23 октября 2014 г. (к началу)

Начало лекции № 6 от 30 октября 2014 г.

1.4.2. Мощности и алефы

Q: What is the world's longest song?
A: «Aleph-nought Bottles of Beer on the Wall.»

Unknown

Определение. *A равномощно B* (обозначение: $A \sim B$), если $\exists f\colon A \to B$ — биекция.
A не превосходит B по мощности (обозначение: $A \lesssim B$), если $\exists f\colon A \to B$ — инъекция.

Считаем известным из анализа следующее утверждение.

Теорема 1.17 (Кантора-Бернштейна). *Если $A \lesssim B$ и $B \lesssim A$, то A равномощно B.*

В условиях аксиомы выбора также устанавливается:

Теорема 1.18 (О сравнимости). *Для любых A, B $A \lesssim B$ или $B \lesssim A$.*

С ней же устанавливается и такая теорема:

Теорема 1.19. *Всякое бесконечное множество содержит счётное подмножество.*

Напомним определения:

Определение. A счётно, если $A \sim \omega$. A конечно, если $\exists n \in \omega\ A \sim n$. A бесконечно, если не является конечным.

□ В чём тут суть аксиомы выбора? Пусть мы хотим выбрать из множества счётное число точек $a_1, a_2, \ldots$ Тогда мы хотим сопоставить $n \mapsto a_n$, $\omega \mapsto A$, построив последовательность $a_n = F(\{a_1, \ldots, a_n\})$. Получаем функцию $F\colon P(A) \setminus \{A\} \to A$. Но это почти что сама аксиома выбора: пусть φ — функция выбора на непустых подмножествах в A; тогда положим $F(B) = \varphi(A \setminus B)$. К счастью, механически выбирать по порядку не нужно: заметим, что если мы вполне упорядочили A, то, по теореме 1.18 (О сравнимости), $A \leqslant \omega$ или $\omega \leqslant A$. (Впрочем, по сути, мы свели к тому же.) ■

Продолжим выводить из AC следствия.

Теорема 1.20 (О сюръекции). *Если $\exists f\colon B \to A$ — сюрьекция, то $A \lesssim B$.*

□ Определим функцию $g : A \to B$ через функцию выбора на множестве $\{f^{-1}(a) \mid a \in A\}$. Она будет осуществлять инъекцию. ■

Теорема 1.21 (Объединение счётных множеств счётно). $\bigcup\limits_{i\in\omega} A_i$ *счётно, если все* $A_i \sim \omega$.

□ $\forall i\ \exists a^i\colon \omega \to A_i$, осуществляющее сюръекцию. Из них мы получаем суммарное отображение $a\colon \omega \times \omega \to \bigcup\limits_{i\in\omega} A_i$. Без всякой AC, по лемме Кантора, устанавливается равномощность $\omega \times \omega$ и ω. Осталось сослаться на теорему 1.20 (О сюръекции). ■

Дадим главное определение.

Определение. Множество α — *кардинал,* если $\alpha \in \mathrm{Ord}$, и $\forall \beta < \alpha\ \beta \nsim \alpha$.

Следствие 1.5. ω — *наименьший бесконечный кардинал.*

Следствие 1.6. $\forall \alpha \in \mathrm{Ord}\ \exists \beta$ — *кардинал:* $\alpha \sim \beta$.

□ В совокупности всех ординалов, равномощных α, выберем минимальный элемент. ■

Следствие 1.7. *Всякое множество X равномощно единственному кардиналу.*

□ Вполне упорядочим X и рассмотрим $\sup\{\alpha \in \mathrm{Ord} \mid \alpha$ изоморфно начальному отрезку $X\}$ (равный его объединению — по аксиоме подстановки, это множество). Тогда это ординал, изоморфный всему X. По предыдущему следствию, есть и изоморфный (единственный) кардинал. ■

Введём иерархию алефов.

Определение.

$$\omega_0 = \aleph_0 \stackrel{\text{def}}{=} \omega. \tag{21}$$

$$\aleph_{\alpha+1} \stackrel{\text{def}}{=} \min\{x \mid x \text{ — кардинал, и } \aleph_\alpha < x\}. \tag{22}$$

$$\aleph_\lambda \stackrel{\text{def}}{=} \sup\{\aleph_\alpha \mid \alpha < \lambda\}, \text{ если } \lambda \text{ — предельный.} \tag{23}$$

Утверждение 1.22. $\forall \alpha \in \mathrm{Ord}\ \aleph_\alpha$ — *кардинал.*

□ В первых двух случаях всё очевидно. В третьем, если $\aleph_\lambda$ — не кардинал, то существует $\beta < \aleph_\lambda$, равномощный $\aleph_\lambda \Leftrightarrow \exists \alpha < \lambda :\ \beta < \aleph_\lambda$. Тогда $\aleph_\alpha \sim \aleph_\lambda (\beta \subseteq \aleph_\alpha \subseteq \aleph_\lambda$, и применяем теорему Кантора-Бернштейна), но тогда $\aleph_\alpha \sim \aleph_{\alpha+1}$. Противоречие. ■

Определение. $\varkappa^+ = \min\{\beta \mid \beta$ — кардинал, и $\varkappa < \beta\}$. $\varkappa$ — предельный кардинал, если $\forall \beta < \varkappa \exists \mu$ — кардинал такой, что $\beta < \mu < \varkappa$.

Утверждение 1.23. *Для любого бесконечного кардинала $\varkappa$ существует и единственен $\alpha \in \mathrm{Ord} :\ \varkappa = \aleph_\alpha$. Таким образом, «функция» $\aleph$ не пропускает ни одного кардинала.*

□ От противного. Пусть $\varkappa$ — наименьший кардинал, не являющийся алефом. Он не может быть ω, поэтому (рассмотрим множество всех кардиналов, строго меньших $\varkappa$; там может либо достигается супремум, либо нет, в каком случае он просто равен $\varkappa$) либо $\varkappa = \mu^+$, где $\mu < \varkappa$, но тогда $\varkappa$ — непосредственно следующий алеф, либо он предельный, все меньшие его — уже алефы, и он оказывается их супремумом, то есть $\aleph_\lambda$ для них. ■

Теперь мы можем, наконец, спокойно вести определение.

Определение. *Мощность* A (обозначение: $|\mathrm{A}|$) — единственный кардинал, изоморфный A.

В предположении AC докажем важный факт.

Теорема 1.24 (Обобщённая лемма Кантора). *Пусть A бесконечно. Тогда $A \times A \sim A$.*

□ Следуя Гёделю, введём *каноническое*[9] *вполне упорядочение* на $\mathrm{Ord} \times \mathrm{Ord}$: скажем, что $(\alpha_1, \beta_1) < (\alpha_2, \beta_2)$, если выполняется одно из трёх:

1° $\max(\alpha_1, \beta_1) > \max(\alpha_2, \beta_2)$.

2° $\max(\alpha_1, \beta_1) = \max(\alpha_2, \beta_2)$ и $\alpha_1 < \alpha_2$.

3° $\max(\alpha_1, \beta_1) = \max(\alpha_2, \beta_2)$, $\alpha_1 = \alpha_2$ и $\beta_1 < \beta_2$.

Видим, что порядок линеен. Почему он полон? Чтобы найти минимальный элемент, нужно сперва отобрать те, где максимум минимален, затем минимизировать первый элемент и из оставшихся — второй, что даст глобальный минимум. Теперь запишем отображение $\pi\colon \mathrm{Ord} \times \mathrm{Ord} \to \mathrm{Ord}$ («маршрут обхода произведения»), действующее по схеме:

$$\pi(\alpha, \beta) = \text{ порядковый тип } \{(x, y) \mid (x, y) < (\alpha, \beta)\}. \tag{24}$$

Видим, что $\pi(\alpha, \alpha) \geqslant \alpha$; положим $\pi[\alpha \times \alpha]$ — начальный сегмент (образ углового квадрата), определяемый $\pi(\alpha, \alpha)$.

Конец лекции № 6 от 30 октября 2014 г. *(к началу)*

Начало лекции № 7 от 6 ноября 2014 г.

Выпишем два полезных наблюдения о начальных сегментах.

Утверждение 1.25 (Ординал есть сегмент). *Рассмотрим любой ординал α. Тогда $\alpha \times \alpha$ есть начальный сегмент в каноническом упорядочении, имеющий вид $\{(x, y) \mid (x, y) < (0, \alpha)\}$.*

□ Понятно при внимательном рассмотрении квадрата. ■

Утверждение 1.26. $\pi[\alpha \times \alpha] \geqslant \alpha$.

□ Обозначим $f(\alpha) \stackrel{\text{def}}{=} \pi[\alpha \times \alpha]$. Тогда f сохраняет порядок: $\alpha < \beta \Rightarrow f(\alpha) < f(\beta)$ (ибо $\alpha \times \alpha \subset \beta \times \beta$), откуда $f(\alpha) \geqslant \alpha$ по утверждению 1.4 (О монотонности). ■

Лемма 1.27. $\pi[\aleph_\alpha \times \aleph_\alpha] = \{\pi(\alpha_1, \beta_1) \mid \alpha_1, \beta_1 < \aleph_\alpha\}$[10] $= \aleph_\alpha$ *для всех* α.

□ От противного. Положим $\varkappa$ — наименьший бесконечный кардинал, при котором $\pi[\varkappa \times \varkappa] > \varkappa$. Тогда существуют $\alpha, \beta < \varkappa\colon\ \pi(\alpha, \beta) = \varkappa$. Возьмём $\delta \in \mathrm{Ord}\colon\ \alpha, \beta < \delta < \varkappa$. В силу того, что, $\varkappa \in \pi[\delta \times \delta]$, а этот $\pi[\delta \times \delta]$ является ординалом, получаем $\varkappa \subseteq \pi[\delta \times \delta]$, что, казалось бы, должно означать, что $|\pi\delta \times \delta| = |\delta \times \delta| \geqslant |\varkappa| = \varkappa$. Однако, с другой стороны, $|\delta \times \delta| = ||\delta| \times |\delta|| =$ [11] $|\delta| < \varkappa$. Противоречие. ■

■

Следствие 1.8. *Пусть A, B — бесконечны, $\varkappa_1, \varkappa_2$ — бесконечные кардиналы. Тогда для кардинальных операций над кардиналами (не путать с одноимёнными ординальными, которые можно провести над теми же объектами с совершенно другими результатами!)* $|A \times B| = |A| \times |B|$, $|A \sqcup B| = |A| + |B|$, $\varkappa_1 + \varkappa_2 = \varkappa_1 \times \varkappa_2 = \max(\varkappa_1, \varkappa_2)$.

Для операций на кардиналах верным будет $\varkappa_1 + \varkappa_2 = \varkappa_1 \times \varkappa_2 = \max(\varkappa_1, \varkappa_2)$.

Введём степени кардиналов и операцию возведения двойки в степень:

Определение. $\varkappa^\mu \stackrel{\text{def}}{=} |\{f\colon \mu \to \varkappa\}|$.

[9] Не лексикографическое!

[10] Это множество — начальный сегмент в Ord по утверждению 1.25 (Ординал есть сегмент) выше, то есть само является ординалом.

[11] $|\delta| \leqslant \delta < \varkappa$, и, по предположению индукции, $\pi[|\delta| \times |\delta|] = \delta$.

Континуум-гипотеза CH: $2^{\aleph_0} = \aleph_1$.

$$\beth_\alpha \stackrel{\text{def}}{=} \begin{cases} \beth_0 = \aleph_0, \\ \beth_{\alpha+1} = 2^{\beth_\alpha}, \\ \beth_\lambda = \sup\{\beth_\alpha \mid \alpha < \lambda\},\ \lambda \text{ — предельный.} \end{cases} \tag{25}$$

Принято обозначать $2^{\aleph_0} = \mathfrak{c}$ — «континуум». Не зависит от ZFC *обобщённая континуум-гипотеза:* $\beth_\alpha = \aleph_\alpha\ \forall\alpha$.

2. Исчисление высказываний

2.1. Аксиоматика Гильберта

Будем считать понятия формулы и интерпретации логики высказываний хорошо известными из общего курса. Вместо этого мы сконцентрируемся на выводимости и исчислениях, предложив две интерпретации: одну каноническую, другую — более удобную на практике.

Пусть $p_0, p_1, \ldots$ — счётный набор пропозициональных символов, $\wedge, \vee, \to, \neg$ — логические связки. Следуя Гильберту, введём схемы аксиом:

1° $\varphi \to (\psi \to \varphi)$.

2° $(\varphi \to (\psi \to \theta)) \to ((\varphi \to \psi) \to (\varphi \to \theta))$.

3° $\varphi \wedge \psi \to \varphi$, $\varphi \wedge \psi \to \psi$.

4° $\varphi \to (\psi \to (\varphi \wedge \psi))$.

5° $\varphi \to \varphi \vee \psi$, $\psi \to \varphi \vee \psi$.

6° $(\varphi \to \theta) \to ((\psi \to \theta) \to ((\varphi \vee \psi) \to \theta))$.

7° $(\varphi \to \psi) \to ((\varphi \to \neg\psi) \to \neg\varphi)$.

8° $\varphi \to (\neg\varphi \to \psi)$ (ex falso sequitur quodibet)

9° $\neg\neg\varphi \to \varphi$. (снятие двойного отрицания)

Правило вывода единственно: modus ponens (MP).

$$\frac{\varphi,\ \varphi \to \psi}{\psi}$$

Определение. *Вывод* — это последовательность формул $\varphi_1, \ldots, \varphi_n$, в которой каждая φ_i — или аксиома, или получена из каких-либо φ_k и φ_l по MP. Обозначают $\vdash \varphi$ и говорят «φ выводимо», если существует вывод, оканчивающийся на формулу φ.

Понятным образом объясняется и понятие *вывода из гипотез* Γ: пусть Γ — множество формул (называемых *гипотезами*); тогда в выводе из гипотез всякая формула либо аксиома, либо принадлежит Γ, либо получена модус поненсом из двух ранее выписанных. Обозначение: $\Gamma \vdash \varphi$.

Приведём конкретный пример вывода, который нам скоро пригодится.

Утверждение 2.1. $\vdash \varphi \to \varphi$ *для любой* φ.

□ Про аксиомы, начиная с третьей, забудем: говорим только об импликации. В аксиому 2 подставим $\varphi = \varphi$, $\theta = \varphi$, $\psi = (\varphi \to \varphi)$:

1° $\varphi \to (\varphi \to \varphi)$ (1)

2° $\varphi \to ((\varphi \to \varphi) \to \varphi)$ (1)

3° $(\varphi \to ((\varphi \to \varphi) \to \varphi)) \to ((\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi))$ (2)

4° $(\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi)$ (MP из 2, 3)

5° $\varphi \to \varphi$ (MP из 1, 4) ■

Теперь приведём пример вывода из гипотез.

Пример 1.1. $p \wedge q \vdash q \wedge p$.

□

1° $p \wedge q$

2° $p \wedge q \to p, p \wedge q \to q$

3° p, q

4° $q \to (p \to (q \wedge p))$

5° $q \wedge p$ по MP.

■

Логика без аксиомы 9 носит название *интуиционистской*. Почти все доказанные нами факты, кроме особо оговорённых, действительны не только в классической логике высказываний, но и в ней. При удалении аксиом 8 и 9 одновременно получается *минимальная логика,* на изучении которой мы останавливаться не будем.

Не требует доказательства ряд важных свойств выводимости из гипотез[12].

Лемма 2.2. **1°** $\Gamma \vdash \varphi$ *и* $\Gamma \subseteq \Delta \Rightarrow \Delta \vdash \varphi$ *(монотонность)*

2° $\Gamma \vdash \varphi$ *и* $\forall \psi \in \Gamma\ \Delta \vdash \psi \Rightarrow \Delta \vdash \varphi$ *(транзитивность)*

3° $\Gamma \vdash \varphi \Rightarrow$ *существует конечное* $\Delta \subseteq \Gamma:\ \Delta \vdash \varphi$ *(компактность)*

И в классической, и в интуиционистской логике верна

Теорема 2.3 (О дедукции). $\Gamma, \varphi \vdash \psi \Leftrightarrow \Gamma \vdash \varphi \to \psi$.

□

$\boxed{\Leftarrow}$ Очевидно.

$\boxed{\Rightarrow}$ Индукция по длине вывода $\Gamma, \varphi \vdash \psi$. Возможны четыре случая.

1° ψ есть аксиома. Тогда достроим вывод так: $\psi \to (\varphi \to \psi)$, $\varphi \to \psi$.

2° $\psi \in \Gamma$. То же самое: допишем ψ, $\psi \to (\varphi \to \psi)$, $\varphi \to \psi$.

3° $\psi = \varphi$. Тогда нужно написать вывод для $\varphi \to \varphi$, что мы научились делать.

4° ψ получена правилом MP из θ и $\theta \to \psi$. По предположению индукции, есть выводы: $\Gamma \vdash \varphi \to \theta$, $\Gamma \vdash \varphi \to (\theta \to \psi)$. Допишем их к нашему текущему выводу, затем дополним $(\varphi \to (\theta \to \psi)) \to ((\varphi \to \theta) \to (\varphi \to \psi))$, $(\varphi \to \theta) \to (\varphi \to \psi)$, $\varphi \to \psi$.

■

Пример 1.2. Закон контрапозиции: $\varphi \to \psi \vdash \neg\psi \to \neg\varphi$.

□ По теореме о дедукции, достаточно показать $\neg\psi, \varphi \to \psi \vdash \neg\varphi$. Проведём следующий вывод:

$(\varphi \to \psi) \to ((\varphi \to \neg\psi) \to \neg\varphi)$. (7)

ψ (гипотеза)

$\neg\psi \to (\varphi \to \neg\psi)$ (1)

... ■

Пример 1.3. Силлогизм: $\varphi \to \psi, \psi \to \theta \vdash \varphi \to \theta$.

□ $\varphi, \varphi \to \psi, \psi \to \theta \vdash \theta$. Два раза модус поненс. ■

Пример 1.4. Аксиома 8 следует из 9: $\varphi, \neg\varphi \vdash \psi$.

□ Докажем, что $\varphi, \neg\varphi \vdash \neg\neg\psi$. По теореме о дедукции, достаточно сделать $\neg\psi \to \varphi, \neg\psi \to \neg\varphi \vdash \neg\neg\varphi$ — по аксиомам 1 и 7. ■

Конец лекции № 7 от 6 ноября 2014 г. *(к началу)*

Начало лекции № 8 от 13 ноября 2014 г.

Пример 1.5. $\vdash A \to \neg\neg A$.

□ $(\neg A \to A) \to ((\neg A \to \neg A) \to \neg\neg A)$ (аксиома 7)

$A \to (\neg A \to A)$ (1)

A (гипотеза)

$\neg A \to A$ (MP 2,3)

$(\neg A \to \neg A) \to \neg\neg A$ (MP)

$\neg A \to \neg A$ (умеем)

$\neg\neg A$ (MP 5,6) ■

Пример 1.6. Обращение закона контрапозиции (только классическая логика!): $\neg B \to \neg A \vdash A \to B$.

□ $\neg B \to \neg A$

$\neg\neg A \to \neg\neg B$ ... ■

[12] Впрочем, существуют исчисления, в которых понятие вывода определяется иначе, и эти свойства перестают выполняться, что может оказаться полезным в приложениях. Так, немонотонным логикам посвящён целый раздел логики высказываний.

Пример 1.7. $A \wedge B \to C \vdash A \to (b \to C)$,
$A \to (B \to C) \vdash A \wedge B \to C$.

□

1° $A \wedge B \to C$ (гипотеза)
A (гипотеза)
B (гипотеза)
$A \to (B \to A \wedge B)$ (4)
$A \wedge B$ (MP дважды)
C (MP 1,5)
2° $A \to (B \to C)$ (гипотеза)
$A \wedge B$ (гипотеза)
$A \wedge B \to A$ (3)
$A \wedge B \to B$ (3)
A (MP 2,3)
B (MP 2,4)
C (MP 1,5,6 дважды) ■

Главным утверждением этой части курса служит:

Теорема 2.4 (О корректности и полноте). $\vdash A \Leftrightarrow A$ — *тавтология.*

□ $\boxed{\Rightarrow}$ Индукция по построению вывода. Все аксиомы являются тавтологиями (проверка таблиц истинности всех аксиом). Если применяется модус поненс, то по предположению индукции A и $A \to B$ истинны на всех наборах переменных. Тогда B истинно по определению импликации. $\boxed{\Leftarrow}$ Докажем, что всякая тавтология выводима.

Определение. Пусть Γ — множество формул; будем говорить, что Γ непротиворечиво, если $\forall A_1, \ldots, A_n \in \Gamma \nvdash \neg(A_1 \wedge A_2 \wedge ... \wedge A_n)$. Γ максимально непротиворечиво, если $\forall A \in \mathrm{Fm}\ (A \in \Gamma \vee \neg A \in \Gamma)$.

Лемма 2.5 (0). *Пусть* Γ *непротиворечиво,* $A \in \mathrm{Fm}$. *Тогда одно из множеств* $\Gamma \cup \{A\}$ *или* $\Gamma \cup \{\neg A\}$ *непротиворечиво.*

□ От противного: пусть оба множества $\Gamma \cup \{A\}$ и $\Gamma \cup \{\neg A\}$ противоречивы. Это означает, что существуют такие $A_1, \ldots, A_j \in \Gamma$, что $\vdash \neg(A \wedge \bigwedge\limits_{i=1}^{n} A_i)$ и $\vdash \neg(\neg A \wedge \bigwedge\limits_{j=1}^{n} A_j)$. По правилу контрапозиции, тогда выводятся $\vdash \neg(A \wedge \bigwedge\limits_{i=1}^{n} A_i \wedge \bigwedge\limits_{j=1}^{n} A'_j)$ и $\vdash \neg(\neg A \wedge \bigwedge\limits_{i=1}^{n} A_i \wedge \bigwedge\limits_{j=1}^{n} A'_j)$. Далее обозначим $\bigwedge\limits_{i=1}^{n} A_i \wedge \bigwedge\limits_{j=1}^{n} A'_j$ за B. Таким образом, имеем $\vdash \neg(A \wedge B)$ и $\vdash \neg(\neg A \wedge B)$, что по аксиоме 8 влечёт $\neg(A \wedge B) \to (A \wedge B \to C)$ (C любое). Далее:
$\neg(A \wedge B)$
$A \wedge B \to C$
$B \to (A \to C)$
$B \to (A \to \neg C)$
$B \to \neg A$ (аксиома 7)
и аналогичные посылки для $\neg A$. Наконец, аксиома 7 даёт нам из этого $\neg B$. ■

Лемма 2.6 (1). *Если* Γ *непротиворечиво, то существует максимально непротиворечивое* $\Gamma' \supseteq \Gamma$.

□ Если множество переменных счётно, то и формул счётное число; будем добавлять всякую формулу либо отрицание по порядку. Счётное объединение в пределе тоже непротиворечиво, ибо непротиворечивость устанавливается конечным числом формул (по определению) и поэтому должна проявиться на конечном шаге. Пусть оно несчётно. Рассмотрим класс всех непротиворечивых множеств, упорядоченный по включению. По только что сказанному, всякая цепь имеет верхнюю грань. Тогда существует максимальный элемент, в котором в силу леммы 0 лежит всякая либо формула, либо отрицание. Значит, он максимально непротиворечив. ■

Лемма 2.7 (2). *Пусть* Γ *максимально непротиворечиво. Тогда*

0° $\Gamma \vdash A \Leftrightarrow A \in \Gamma$.

1° $\Gamma \ni A \wedge B \Leftrightarrow \Gamma \ni A$ *и* $\Gamma \ni B$.

2° $\Gamma \ni A \vee B \Leftrightarrow \Gamma \ni A$ *или* $\Gamma \ni B$.

3° $\Gamma \ni \neg A \Leftrightarrow \Gamma \not\ni A$.

4° $\Gamma \ni A \to B \Leftrightarrow \Gamma \not\ni A$ *или* $\Gamma \ni B$. *TODO*

□

0° Пусть $\Gamma \vdash A$, но $A \notin \Gamma$. Тогда должно быть $\Gamma \ni \neg A$. В частности, существует вывод $\neg A$ из Γ; пусть $A_1, \ldots, A_n \in \Gamma$ — гипотезы, участвующие в этом выводе. Тогда $\vdash \neg(\neg A \wedge A_1 \wedge \ldots \wedge A_n)$ (ибо без отрицания она выводит $\neg A$ и A одновременно — аксиома 7!). Но Γ непротиворечиво. Противоречие.

Все последующие номера — тривиальное упражнение с заменой выводимости на принадлежность.

4° $\boxed{\Leftarrow}$ $\Gamma \not\ni A \Rightarrow \Gamma \ni \neg A$

$\neg A \to (A \to B)$ (аксиома)

$\Gamma \vdash A \to B$

$\Gamma \ni (A \to B)$

$\Gamma \ni B; \vdash B \to (A \to B)$

$\boxed{\Rightarrow}$ $\Gamma \ni A \to B$

$\Gamma \ni A$ и $\Gamma \not\ni B$ TODOTODO

$\Gamma \vdash B$

$\Gamma \ni B$ ■

Пусть A — невыводимая тавтология. Тогда $\Gamma_0 = \{\neg A\}$ непротиворечиво. Расширим его до максимально непротиворечивого Γ. Зададим оценку такую, что $v(p) = true \Leftrightarrow p \in \Gamma$.

Лемма 2.8 (Основная). $\forall F \in \mathrm{Fm}\, v(F) = true \Leftrightarrow F \in \Gamma$.

□ Индукция по построению F.

1° F — терм: по определению v.

2° $F = F_1 \wedge F_2$. Тогда $v(F) = true \Leftrightarrow v(F_1) = v(F_2) = true \Leftrightarrow F_1 \in \Gamma$ и $F_2 \in \Gamma \Leftrightarrow (\textit{лемма} 2) F_1 \wedge F_2 \ldots$

3°

4°... ■

... ■

2.2. Интуиционистская логика высказываний

В обычной логике адекватное понятие истинности — «быть тавтологией». Но в интуиционистской выводится меньше тавтологий; поговорим о семантике Крипке.

Определение. $K = (W, R, v)$, где W — множество всех возможных миров, $R \subseteq W^2$ — рефлексивно и транзитивно, оценка $v(p) \subseteq W$ удовлетворяет свойству наследования истинности в видимых мирах: если $x \in v(p)$ и xRy, то и $y \in v(p)$.

Пусть $x \in W$, $F \in \mathrm{Fm}$. Определим истинность в конкретном мире так: $K, x \models p \overset{\text{def}}{\Longleftrightarrow}$

1° $K, x \models p \Leftrightarrow x \in v(p)$.

2° $\vee, \wedge$ — по таблицам истинности.

3° $K, x \models \neg F \Leftrightarrow \forall y (xRy \Leftrightarrow \not\models F)$.

4° $K, x \models (F \to G) \Leftrightarrow \forall y (xRy \Leftrightarrow y \not\models F \vee y \models G)$.

Утверждение 2.9. $\models$ *монотонно, то есть* $\forall x, y \in W\ \forall F \in \mathrm{Fm}$, *если* $x \models F$ *и* xRy, *то* $y \models F$.

□ Индукция по построению формы. ■

Конец лекции № 8 от 13 ноября 2014 г. *(к началу)*

Последняя компиляция: 18 ноября 2014 г.
Обновления документа — на странице http://vk.com/id183071829.
Об опечатках и неточностях пишите на rudetection@gmail.com.