Обязательный спецкурс кафедры математической логики и теории алгоритмов

Л.Д. Беклемишев, С.Л. Кузнецов, Т.Л. Яворская

21 мая 2016 г.

Список лекций

- Введение. Аксиомы ZFC.
- Порядки. Вполне упорядоченность.
- Ординалы и их свойства.
- Трансфинитная рекурсия. Аксиома выбора.
- Доказательство эквивалентности различных формулировок аксиомы выбора.
- Мощности и алефы.
- Континуум-гипотеза. Гильбертова аксиоматика логики высказываний. Теорема о дедукции.
- Примеры выводов. Теорема о корректности и полноте. Семантика Крипке.
- Теорема о корректности и полноте в интуиционистской логике. Свойство дизъюнктивности.
- Разрешимость Int. Теорема Гливенко, неконечнозначность интуиционистской логики.
- Исчисление предикатов. Теорема о корректности.
- Теорема о дедукции. Теорема о полноте.
- Теорема о полноте (продолжение). Следствия.
- Теории с равенством. Теоремы Лёвенгейма-Скулема.

- Элиминация кванторов. Теорема Тарского-Зайденберга.
- Упорядоченные поля.
- Упорядоченные поля (продолжение). Категоричные теории.
- Примитивно рекурсивные функции. Примеры.
- Свойства примитивной рекурсивности.
- Рекурсивные функции (в широком смысле).
- Кодирование синтаксиса языка.
- Бета-функция Гёделя.
- Теорема Гёделя о неполноте.

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

1 Теория множеств и философия оснований математики

1.1 История вопроса

Осознанная история исследования аксиоматизации как отдельной научной проблемы восходит, пожалуй, к тем временам, когда Евклид в «Началах» изложил основы геометрии в виде набора аксиом. Сразу же возник вопрос о его избыточности, т.е. 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».

[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.

Решающий вклад в проблему внёс Давид Гильберт в своей передовой работе Grundlagen der Geometrie (1899), где была впервые изложена полная система аксиом элементарной геометрии. Аксиоматическая теория Гильберта, вообще говоря, не является теорией первого порядка. В дальнейшем Тарский (1959) предложил упрощённую систему аксиом для геометрии и доказал полноту и разрешимость построенной им теории.

Гильберт верил в то, что аналогичная полная аксиоматизация возможна и для теории чисел и анализа. Георг Кантор в качестве базового ввел понятие множества. Описание множеств было неаксиоматическим, наивным. Современные Кантору математики восприняли это понятие по-разному. После работ Кантора строгое изложение математического анализа базировалось на понятии множества. Но если полную аксиоматизацию элементарной геометрии всё же удалось построить, то с теорией множеств возникли проблемы. Однако в начале XX века возникли парадоксы, такие как известный парадокс Рассела, в котором предлагается рассмотреть множество вида $\{ x \mid x \notin x \}$,, которое принадлежит самому себе тогда и только тогда, когда не принадлежит. После этого Гильберт сформулировал задачу аксиоматического описания понятия множества. 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 ученик Гильберта Э. Цермело (Zermelo), к аксиомам которого А. Френкель (Fraenkel) добавил ещё две (регулярности и схему подстановки), в результате чего сложилась аксиоматическая теория ZF. Мы будем описывать ее саму, а также ее расширение аксиомой выбора ZFC.

Эта теория страдает очевидным изъяном. Чтобы аксиомы имели смысл, нужно как-то доказать не только их непротиворечивость друг другу, но и их реализацию 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... До теорем Гёделя о полноте многие логики не до конца различали синтаксическое и семантическое понятия следования. 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

Мы будем описывать аксиоматически понятие множества. Подразумесается, что все объекты — множества. Пусть сигнатура состоит из двух символов бинарных отношений: $\sigma = \{\in, =\}$. Обозначение $x \in y$ будем читать как "x принадлежит y". Помимо математических аксиом, которые мы сейчас будем описывать, подразумевается наличие логических аксиом и обычных аксиом равенства (рефлексивность, транзитивность, симметричность, $x = x_1 \wedge y = y_1 \to (x \in y \leftrightarrow x_1 \in y_1)$).

1.2.1 Конечные аксиомы

Аксиома 1.1 (Объёмности или экстенсиональности)

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

Замечание 1 В аксиоме объемности импликация $\to$ следует из аксиом равенства, собственно содержательным является обратное утверждение.

В некоторых вариантах теории множеств предполагается ограничить сигнатуру отношением принадлежности, а равенство определять через него в соответствии с аксиомой объемности.

Определение 1 Пустое множество: $\emptyset = \{x \mid x \neq x\}$. Подмножество: $B \subseteq A = \forall x\ (x \in B \Rightarrow x \in A)$.

Заметим, что пустое множество единственно (в силу аксиомы объемности). Следующие аксиомы описывают, какие множества допустимы. Аксиома пары позволяет построить непустое множество.

Аксиома 1.2 (Пары)

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

Заметим, что множество z, существование которого утверждает аксиома пары, единственно (в силу принципа объемности), следовательно, для пары элементов x и y можно ввести спецмиальное обозначение $\{x, y\}$. Неформальный смысл: существует *неупорядоченная пара* $\{x, y\}$, состоящая из элементов x, y. Если взять $y = x$, то из аксиомы пары следует, что существует *синглетон* — множество $\{x\}$ ровно из одного элемента.

Следующая аксиома была предложена специально для ликвидации проблем в духе парадокса Рассела. Говоря неформально, мы хотим, чтобы из любого множества

x любое "свойство" φ (записанное формулой логики предикатов в сигнатуре теории множеств) выделяло подмножество элементов, обладающих свойством φ:

$$z = \{\, y \in x \mid \varphi(y) \,\} \tag{3}$$

Формально это означает следующее:

Аксиома 1.3 (Выделения (схема аксиом))

$$\forall x \exists z\, \forall y (y \in z \leftrightarrow y \in x \wedge \varphi(y)). \tag{4}$$

Заметим, что множество z, существование которого утверждает аксиома выделения, единственное в силу аксиомы объемности. Поэтому мы можем использовать обозначение

$$\{y \in x \mid \varphi(y)\}.$$

Замечание 2 Уточним: формул всего счётное число, и кажется, что из любого по мощности множества можно выделить лишь счётное число различных подмножеств (по числу выделяющих их формул). Получается, что на действительной прямой мы не можем описать все лучи $(a, +\infty)$. Эта проблема решается, если допустить параметры (свободные переменные) в формуле φ. Тогда, например, все лучи выделяются единственной формулой $\varphi(x, a) = (x < a)$ при разных значениях парамента a

Замечание 3 Почему эти аксиомы обеспечивают существование хотя бы одного множества?

Ответ: мы не заостряли на этом внимание, 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 $\varnothing$.

Аксиома выделения позволяет определить некоторые теоретико-множественные операции. Например

$$\begin{aligned} x \cap y &\rightleftharpoons \{z \in x \mid z \in y\} \\ x \setminus y &\rightleftharpoons \{z \in x \mid z \notin y\} \end{aligned}$$

Однако она не позволяет определить объединение множеств и построить множества из трех, четырех элементов и т. д. Для этого понадобится

Аксиома 1.4 (Объединения)

$$\forall x \exists y (y = \cup x). \tag{5}$$

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

$$y = \cup x \overset{\text{def}}{\leftrightharpoons} \forall z(z \in y \leftrightarrow \exists w \in x(z \in w)) \tag{6}$$

т.е. $\cup x = \{z \mid \exists u \in x(z \in u)\}$. Стандартное объединение двух множеств также существует в силу аксиомы объединения:

$$x \cup y \Leftrightarrow \cup\{x, y\}.$$

Определим тройку: $\{x, y, z\} \overset{def}{\leftrightharpoons} \{x, y\} \cup \{z\}$. Более того, можем определить и неупорядоченные n-ки для любого n (хотя, оставаясь в рамках теории первого порядка, мы и не можем формально записать и доказать такое обобщение).

Упражнение 1 Утверждение 1 $x \neq \varnothing \to \exists y = \cap x$, то есть $\exists u\,(u \in x) \to \exists y\,(\forall z\,(z \in y \leftrightarrow \forall u \in x\, z \in u))$.

Аксиома 1.5 (Степени)

$$\forall x\, \exists y\, (\forall z\, (z \in y \leftrightarrow z \subseteq x)). \tag{7}$$

Замечание 4 Такое множество y единственное в силу аксиомы объемности; обозначим его через $\mathcal{P}(x)$.

Опишем теберь схематично, как в теории множеств строятся стандартные математические объекты, а именно, бинарные отношения между множествами, функции и т.д.

Определение 2 Пусть X и Y — множества. *Упорядоченная пара* $\langle x, y\rangle$, где $x \in X,\ y \in Y$ — это объект, обладающий следующим характеристическим свойством:

$$\langle x, y\rangle = \langle x_1, y_1\rangle \Longleftrightarrow x = x_1 \text{ и } y = y_1.$$

Декартово произведение множеств X и Y — это множество всех упорядоченных пар $\langle x, y\rangle$, где $x \in X,\ y \in Y$. *Бинарное отношение* R между множествами X и Y — это подмножество их декартова произведения, $R \subseteq X \times Y$.

Функция f из множества X в множество Y — это бинарное отношение $f \subseteq X \times Y$, удовлетворяющее следующим двум свойствам:

- *функциональность*, т.е. $\forall x, y, z\ (\langle x, y\rangle \in f \& \langle x, z\rangle) \in f \to y = z$
- *тотальность*: т.е. $\forall x \exists y\ \langle x, y\rangle \in f$

Вместо $\langle x, y\rangle \in R$ мы будем писать xRy.

Опишем эти понятия в языке ZF.

Определение 3 Упорядоченная пара (по Куратовскому): $\langle x, y\rangle \rightleftharpoons \{\{x\}, \{x, y\}\}$.

Утверждение 2 Для упорядоченной пары по Куратовскому выполняется основное свойство упорядоченных пар:

$$\langle x, y\rangle = \langle x_1, y_1\rangle \Longleftrightarrow x = x_1 \text{ и } y = y_1.$$

Доказательство. Заметим, что $\bigcap\langle x, y\rangle = \{x\}$, поэтому

$$\langle x, y\rangle = \langle x_1, y_1\rangle \;\Rightarrow\; \bigcap\langle x, y\rangle = \bigcap\langle x_1, y_1\rangle \;\Rightarrow\; \{x\} = \{x_1\}.$$

Далее, $\bigcup\langle x, y\rangle = \{x, y\}$, поэтому

$$\langle x, y\rangle = \langle x_1, y_1\rangle \;\Rightarrow \bigcup\langle x, y\rangle = \bigcup\langle x_1, y_1\rangle \;\Rightarrow\; \{x, y\} = \{x_1, y_1\} \;\Rightarrow\; \{x, y\} = \{x, y_1\} \;\Rightarrow\; y = y_1.$$

Определение 4 Декартово произведение множеств X и Y определяется следующим образом:

$$X \times Y = \{\langle x, y\rangle \in \mathcal{P}(\mathcal{P}(\mathcal{X} \cup \mathcal{Y})) \mid \S \in \mathcal{X},\ \dagger \in \mathcal{Y}\}.$$

Дальше из декартова произведения можно выделять бинарные отношения, среди них различать функции и т.д.

1.2.2 Натуральные числа и аксиома бесконечности

Имеющиеся аксиомы не гарантирует нам существования бесконечного множества. Моделью этих аксиом является семейство наследственно конечных множеств. Они определяются следующим образом:

$$\begin{array}{lcl} V_0 & = & \emptyset \\ V_1 & = & \{\emptyset\} \\ V_2 & = & \mathcal{P}(V_0) = \{\emptyset, \{\emptyset\}\} \\ \ldots & = & \ldots \\ V_{n+1} & = & \mathcal{P}(V_n) \end{array}$$

Далее, на метауровне мы можем определить множество $V_\omega = \bigcup_{n\in\mathbb{N}} V_n$, однако формально, в рамках теории множеств, построить множество V_ω мы не можем. Для этого требуется аксиома бесконечности. Неформально говоря, она утверждает существование бесконечного множества. Поскольку понятие бесконечного множества сложно формализовать, мы заменяем его более узким понятием индуктивного множества.

Определение 5 Множество X называется *индуктивным,* если

$$(\varnothing \in X) \wedge \forall y \in X\ (y \cup \{y\} \in X). \tag{8}$$

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

Теперь скажем, что такие последовательности существуют.

Аксиома 1.6 (Бесконечности) *Существует индуктивное множество:*

$$\exists w(\varnothing \in w \wedge \forall y \in w\,(y \cup \{y\} \in w)). \tag{9}$$

Определим множество натуральных чисел $\mathbb{N}$, или, как чаще мы будем его обозначать, ω. Зафиксируем произвольное индуктивное множество I.

Определение 6 ω — наименьшее из индуктивных множеств по включению, то есть

$$\omega \overset{def}{\leftrightharpoons} \bigcap\{J \in \mathcal{P}(I) \mid J \text{ индуктивно}\}.$$

Введём на числах естественный порядок: пусть $n, m \in \omega$, тогда $n < m \overset{def}{\leftrightharpoons} n \in m$.
Определим операцию взятия следующего элемента: $n + 1 \overset{def}{\leftrightharpoons} n \cup \{n\}$.

Заметим, что пересечение произвольного семейства индуктивных множеств индуктивно, следовательно ω индуктивно, и кроме того, ω включено в любое индуктивное множество.

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

Решение.

$$x < y + 1 \Leftrightarrow x \in y \cup \{y\} \Leftrightarrow x \in y \vee x = y \Leftrightarrow x < y \vee x = y. \tag{10}$$

Выпишем несколько первых элементов множества ω:

$$\begin{aligned} \varnothing &\in \omega \\ \{\varnothing\} &\in \omega \\ \{\varnothing, \{\varnothing\}\} &\in \omega \\ \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\} &\in \omega \\ \} &\in \omega \end{aligned}$$

Заметим, что элементы ω — это конечные множества мощности 0, 1, 2 и т.д., так что естественным представляется отождествить с ними натуральные числа.

На основании аксиом 1–6 докажем следующее фундаментальное свойство натуральных чисел.

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

Доказательство. A индуктивно по условию, следовательно $\mathbb{N} \cap A$ - индуктивное подмножество $\mathbb{N}$. Но $\mathbb{N}$ — минимальное по включению среди индуктивных, следовательно, $\mathbb{N} \cap A \equiv \mathbb{N}$ и $\mathbb{N} \subseteq A$.

Это утверждение можно несколько обобщить.

Теорема 2 [Порядковая индукция] Если $\forall n \in \mathbb{N}\,((\forall m < n\, m \in A) \to n \in A)$, то $\mathbb{N} \subseteq A$.

Доказательство. Рассмотрим $A' \overset{def}{\leftrightharpoons} \{n \in \mathbb{N} \mid \forall m < n\ m \in A\}$. Докажем, что множество A' индуктивно.

Очевидно, $0 \in A'$.

Далее, если $n \in A'$, то $\forall m < n\, m \in A$ по определению A'. Тогда по условию $n \in A$, следовательно, $\forall m < n + 1\ m \in A$, и значит $n + 1 \in A'$. В соответствии с принципом индукции имеем $\omega \subseteq A'$, а также по определению $A' \subseteq A$.

Следствие 1 Всякое непустое подмножество натуральных чисел имеет минимальный элемент:

$$\forall A \subseteq \mathbb{N}\,(\exists x\,(x \in A) \to \exists x\,(x \in A \wedge \forall y < x\ y \notin A)).$$

Доказательство. Предположим что найдется множество $A \subseteq \omega$, не содержащее минимального элемента. ч

Конец лекции № 1

Начало лекции № 2

1.3 Порядок и ординалы

1.3.1 Линейные и полные порядки

Определение 7 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: $\forall x, y, z\,(x < y \wedge y < z) \to x < z$[3].

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

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 P:

[3]Поскольку мы определяем *строгий* порядок, привычное требование антисимметричности порядка выводится из уже имеющихся: если $x < y \wedge y < x$, то по второй аксиоме получаем $x < x$, что противоречит аксиоме 1.

Определение 8 *Максимальным (минимальным)* называется элемент $x \in P$, такой, что $\neg\exists a \in P\,(a > x)$ (соответственно, $(a < x)$).

Наибольший (наименьший) элемент множества P — это такой $x \in P$, что $\forall a \in P\,(a \leq x)$ (соответственно, $a \geq x$).

Аналогично определяются максимальный (минимальный) и наибольший (наименьший) элементы для подмножества $A \subset P$.

Замечание 5 Рассмотрим отношение делимости на множестве $\{0, 1, 2, \ldots, 10\}$. Там есть максимум, и даже не один (10, 9, 8, 7, ...), но не имеется наибольшего элемента. Наибольший элемент, если он есть, является максимальным, но обратное, вообще говоря, неверно. Для линейных порядков эти понятия эквивалентны.

Упражнение 2 1) Доказать, что всякий наибольший элемент является максимальным, а наименьший — минимальным.

2) Доказать, что если порядок линеен, то обратное утверждение тоже верно.

3) Пусть максимальный элемент существует и единственный. Верно ли, что он наибольший?

Определение 9 Элемент $a \in P$ называется *верхней (нижней) гранью* подмножества $A \subseteq P$, если $\forall x \in A\,(x \leq a)$ (соответственно, $x \geq a$).

Элемент $a \in P$ называется *точной верхней гранью* подмножества $A \subseteq P$ и обозначается $a = \sup A$, если a — наименьшая среди всех верхних граней A. Аналогично определяется $\inf A$ — наибольшая среди всех нижних граней A.

Пример 1 Множество $\{x \in \mathbb{Q} \mid x^2 \leq 2\}$ в $\mathbb{Q}$ имеет много верхних граней, но не имеет точной верхней грани.

Определение 10 Пусть $(P, <_P)$ и $(Q, <_Q)$ — частично упорядоченные множества. Отображение $f\colon P \to Q$ *возрастает (сохраняет порядок),* если

$$\forall x, y \in P\,(x < y \Rightarrow f(x) < f(y)).$$

Отображение f называется *изоморфизмом порядков,* если f сохраняет порядок и является биекцией между P и Q. В этом случае порядки $<_P$ и $<_Q$ называются *изоморфными.* Обозначение: $(P, <_P) \simeq (Q, <_Q)$.

Пример 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 (изоморфизмом является функция $y = \operatorname{arctg} x$.

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 $\mathbb{Q}$, поскольку всё счётные плотные линейные порядки без первого и последнего элемента изоморфны между собой.

5) Приведите пример неизоморфных континуальных плотных линейных порядков без минимального и максимального элемента. Сколько таких порядков существует?

Определение 11 Пусть $(P, <_P)$ — линейный порядок. P называется *вполне упорядоченным множеством,* если любое непустое подмножество P имеет наименьший элемент.

Пример 3 $(\mathbb{N}, <)$ — вполне упорядоченно. (Это можно доказать индукцией)

Замечание 6 Ближайшая цель. Отношение порядкового изоморфизма разбивает все вполне упорядоченные множества на классы эквивалентности — так называемые "порядковые типы". Будем их изучать.

Утверждение 3 [О монотонности] Пусть $(W, <)$ — вполне упорядочено; $f\colon W \to W$ возрастает. Тогда $\forall x \in W\ f(x) \geq x$.

Доказательство. От противного. Пусть $A \overset{def}{\leftrightharpoons} \{x \in W \mid \mid f(x) < x\} \neq \emptyset$. Поскольку W вполне упорядоченно, найдется a — наименьший элемент A. Поскольку $a \in A$, $f(a) < a$. Но f возрастает, поэтому применим к неравенству f ещё раз: $f(f(a)) < f(a)$. Обозначим $b = f(a)$, имеем $f(b) < b$. Тогда $b \in A$ (по определению A) и $b < a$. Противоречие с тем, что a выбран в A наименьшим.

Следствие 2 Пусть $(W, <)$ — вполне упорядочено; $f\colon W \to W$ — автоморфизм (то есть изоморфизм упорядоченного множества на себя). Тогда $\forall x \in W\ (f(x) = x)$.

Доказательство. По доказанному, $\forall x\ (f(x) \geq x)$. Но обратное отображение f^{-1} — тоже автоморфизм, и $f^{-1}(x) \geq x$. Применяя f к обеим частям последнего неравенства, имеем $f(f^{-1}(x)) = x \geq f(x)$, следовательно $f(x) = x$.

Следствие 3 Если $(W_1, <_1)$ и $(W_2, <_2)$ - изоморфные вполне упорядоченные множества, то их изоморфизм — единственен.

Доказательство. 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. Следовательно $f = (g^{-1})^{-1} = g$.

Определение 12 Пусть $(W, <)$ — вполне упорядоченное множество, $u \in W$. *Начальным отрезком* W назовём подмножество $W(u) \overset{def}{\leftrightharpoons} \{x \in W \mid x < u\}$, упорядоченное ограничением отношения $<$.

В силу того, что минимальные элементы в подмножествах сохраняются, начальный отрезок — тоже вполне упорядочен.

Утверждение 4 [О неизоморфности] Пусть $(W, <)$ — вполне упорядочено. Тогда ни для какого $u \in W$ упорядоченные множества W и $W(u)$ не изоморфны.

Доказательство. Если $f\colon (W, <) \to (W(u), <)$ — изоморфизм, то $f(u) \in W(u)$, следовательно $f(u) < u$. Противоречие.

Неформально следующая теорема утверждает, что любые два вполне упорядоченных множества сравнимы.

Теорема 3 [О сравнении вполне упорядоченных множеств] Пусть W_1, W_2 — два вполне упорядоченных множества. Тогда имеет место одна из трёх возможностей:

1) W_1 и W_2 изоморфны;

2) изоморфно $W_2(u)$ для некоторого u;

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

Доказательство. Обозначим

$$f \subseteq W_1 \times W_2,\ f \stackrel{def}{=\!=} \{\langle x, y, \in\rangle W_1 \times W_2 \mid W_1(x) \text{ и } W_2(y) \text{ изоморфны}\}$$

Тогда f функционально и инъективно (воспользуйтесь только что доказанным утверждением 4).

Покажем, что f сохраняет порядок. Пусть $x_1, x_2 \in W_1$ и $x_1 < x_2$. Если $W_1(x_1)$ изоморфен $W_2(f(x_1))$ и $W_1(x_1)$ изоморфен $W_2(f(x_2))$, то поскольку $W_1(x_1) \subseteq W_1(x_2)$ и изоморфизм порядков единственен, второй изоморфизм будет служить продолжением первого. Следовательно $W_2(f(x_1)) \subseteq W_2(f(x_2))$, что и влечёт $f(x_1) < f(x_2)$.

Обозначим:

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

Возможны следующие варианты:

Вариант 1. $\mathrm{dom} f = W_1$, $\mathrm{ran}\, f = W_2$ — тогда имеет место первая из трех возможностей.

Вариант 2. $\mathrm{ran}\, f \neq W_2,\ W_2 \setminus \mathrm{ran}\, f \neq \emptyset$. Выберем наименьший элемент в $W_2 \setminus \mathrm{ran}\, f$, тогда $\mathrm{ran}\, f = W_2(y)$.

Допустим, при этом оказалось, что $\mathrm{dom} f \neq W_1$. Заметим, что если $x_2 \in \mathrm{dom} f$ и $x_1 < x_2$, то $x_1 \in \mathrm{dom} f$. Возьмем наименьший $x \in W_1$, такой что $x \notin \mathrm{dom}(f)$, тогде $\mathrm{dom} f = W_1(x)$. Между $W_1(x)$ и $W_2(y)$ отношение f является изоморфизмом. Это влечёт $< x, y >\in f$, следовательно, $y \in \mathrm{ran}\, f$, противоречие с выбором y. Итак, $\mathrm{dom} f = W_1$ — тогда имеет место вторая из трех возможностей.

Вариант 3 $\mathrm{dom} f \neq W_1$ — аналогично варианту 2.

Ординалы

Ординалы — это порядковые типы вполне упорядоченных множеств. Чтобы не рассуждать о "классах эквивалентности вполне упорядоченных множеств", предъявим по конкретному множеству каждого класса и будем изучать их.

Определение 13 Множество A называется *транзитивным,* если $\forall x(x \in A \to x \subseteq A)$. A называется *ординалом,* если

1. A — транзитивно;
2. $(A, \in)$ вполне упорядочено (по отношению принадлежности).

Замечание 7 По определению, если A — ординал, то отношение принадлежности $\in$ на A является линыйным порядком (в частности, любые два элемента сравнимы), и всякое непустое подмножество A содержит наименьший элемент по отношению $\in$.

Пример 4 Ординалы существуют: сразу понятно, что $\emptyset$ — ординал. $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ — все тоже таковы, и так далее.

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

Конец лекции № 2

Начало лекции № 3

Утверждение 5 [Свойства ординалов]

1) $0 \in \text{Ord}$ (здесь $0 = \emptyset$)

2) $\alpha \in \text{Ord} \wedge \beta \in \alpha \Rightarrow \beta \in \text{Ord}$.

3) $\alpha, \beta \in \text{Ord} \wedge \alpha \subsetneq \beta \Rightarrow \alpha \in \beta$.

4) $\alpha, \beta \in \text{Ord} \Rightarrow \alpha \subset \beta$ или $\beta \subset \alpha$.

Доказательство. 1) Очевидно.

2) Если $\beta \in \alpha$, то $\beta \subseteq \alpha$, поскольку α ординал, и значит транзитивно. Следовательно, поскольку $(\alpha, \in)$ вполне упорядочено, $(\beta, \in)$ тоже вполне упорядочено.

Покажем транзитивность β: возьмем $x \in \beta$ и докажем, что $x \subseteq \beta$. Пусть $y \in x \in \beta$. Тогда (т.к. $\beta \subseteq \alpha$) $y \in x \in \alpha$. Следовательно, поскольку $x \subseteq \alpha$ из-за транзитивности α, получим $y \in \alpha$.

Имеем: $y \in x \in \beta$, где $\beta \in \alpha$ (по условию), $x \in \alpha,\ y \in \alpha$ (доказано). Но $\in$ на α — отношение порядка. Поэтому $y \in \beta$.

3) Пусть $\beta \setminus \alpha \neq \emptyset$. Рассмотрим минимальный y, принадлежащий дополнению $\beta \setminus \alpha$. Покажем, что $\alpha = \beta(y) = \{x \in \beta \mid x < y\}$. Включение $\beta(y) \subseteq \alpha$ очевидно, докажем что $\alpha \subseteq \beta(y)$. От противного. Пусть $x \in \alpha,\ x \geq y$. Тогда либо $y \in x \in \alpha$, либо $y = x \in \alpha$, и в обоих случаях $y \in \alpha$, вопреки выбору y.

Итак, $\alpha = \{x \in \beta \mid x \in y\} = y \in \beta$. Поскольку $y \in \beta$, получим $\alpha \in \beta$.

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 4 1) $<$ — линейный порядок на Ord.

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

3) Пусть $C \neq \emptyset,\ C \subseteq \mathrm{Ord}$. Тогда $\cap C \in \mathrm{Ord}$, $\cap C \in C$, $\cap C = \inf C$.

4) Пусть $X \neq \emptyset,\ X \subseteq \mathrm{Ord}$. Тогда $\cup X \in \mathrm{Ord}$, $\cup X = \sup X$.

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

Доказательство. 1) $\alpha \in \beta \in \gamma \Rightarrow \alpha \in \gamma$, так как γ — транзитивно.

Далее, если $\alpha, \beta \in \mathrm{Ord}$, то по лемме 5, пункт 4, $\alpha \subset \beta$ или $\beta \subset \alpha$. Тогда по той же лемме, пункт 3, $\alpha = \beta \vee \alpha \in \beta \vee \beta \in \alpha$.

2) $\supseteq$ очевидно; $\subseteq$ по п. 2 леммы 5.

3) $\cap C \in \mathrm{Ord}$ — проверяется непосредственно по определению ординала.

Пусть $\alpha \in C$, тогда $\cap C \subseteq \alpha$. Если $\cap C \notin C$, то $\forall \alpha \in C\, \alpha \neq \cap C$. С учетом того что $\cap C \subseteq \alpha$ по лемме 5 пункт 3 получим $\forall \alpha \in C \cap C \in \alpha$. Следовательно $\cap C \in \cap C$ — противоречие.

4) Докажем, что $\cup X$ вполне упорядоченно. Пусть $Y \subseteq (\cup X)$. Для любого $\alpha \in X$ такого, что $\alpha \cap Y \neq \emptyset$, это пересечение содержит наименьший элемент. Поскольку α является начальным отрезком X, этот же элемент оказывается наименьшим и для Y. Итак, вполне упорядоченность установлена. Для доказательства транзитивности $\cup X$ возьмем произвольный $a \in \cup X$ и $b \in a$. Тогда для некоторого $\alpha \in X$ имеем $a \in \alpha$. Поскольку α — ординал, оно транзитивно, и следовательно $b \in \alpha$, откуда следует что $b \in \cup X$.

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 $\alpha \in \gamma \Rightarrow \alpha \subseteq \gamma$.

Для дальнейшего нам понадобится следующая схема аксиом *подстановки* или *замены.*

Аксиома 1.7 (Замены)

$$\forall x, y, z(\varphi(x, y, \vec{p}) \wedge \varphi(x, z, \vec{p}) \to y = z) \ \to\ \forall X \exists Y \forall y(y \in Y \leftrightarrow \exists x \in X\, \varphi(x, y, \vec{p})). \quad (11)$$

При заданных значениях параметров $\vec{p}$, формула $\varphi(x, y)$ задаёт бинарное отношение на классе всех множеств, которое также является, вообще говоря, классом. Посылка аксиомы говорит, что это отношение функционально (является частичной функцией). Заключение аксиомы говорит, что образ любого множества X при этой функции является множеством. Менее формально, если F — функция-класс, то для любого множества X совокупность $\{F(x) \mid x \in X\}$ также является множеством.

Теорема 4 Всякое вполне упорядоченное множество изоморфно некоторому ординалу, причем единственному. А именно, пусть $(W, <)$ — вполне упорядочено. Тогда найдется единственный $\alpha \in \mathrm{Ord}$, такой что $\alpha \simeq (W, <)$.

Доказательство. Единственность сразу следует из того, что из двух разных ординалов один является начальным отрезком другого, поэтому разные ординалы неизоморфны. Докажем существование. Пусть $x \in W$. Обозначим

$$W(x) \stackrel{def}{=} \{y \in W \mid y < x\}. \tag{12}$$

Рассмотрим формулу $\varphi(x, \alpha)$, выражающую предикат: "α — ординал, и $W(x)$ изоморфно α." Формула φ задаёт функциональное бинарное отношение-класс, поскольку изоморфные как упорядоченные множества ординалы равны (см. лемму 5). Обозначим соответствующую частичную функцию через $F(x)$.

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 $\forall z < y\, W(z) \simeq F(z)$. По аксиоме 1.7, $\{F(z) \mid z < y\}$ есть множество ординалов. Рассмотрим $\alpha = \cup\{F(z) \mid z < y\}$. Докажем, что α изоморфно $W(y)$. Действительно, в случае, если α изоморфно начальному отрезку $W(y)$, то этот отрезок изоморфен некоторому отрезку самого себя. И наоборот, если $W(y)$ изоморфен некоторому отрезку α, то этот отрезок изоморфен своему собственному начальному отрезку. Таким образом, $F(y) = \alpha$, что противоречит выбору y.

Итак, F всюду определена на W. По аксиоме 1.7, $F(W) = \{F(x) \mid x \in W\}$ — множество. Тогда существует наименьший ординал $\gamma \notin F(W)$ (Такой ординал γ существует. Действительно, возьмем любой ординал $y \notin F(W)$, например $y = \cup F(W) + 1$. Тогда $y \setminus F(W) \neq \emptyset$, следовательно в качестве γ можно взять наименьший элемент в $y \setminus F(W)$.) 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.

Ординал вида $\alpha \cup \{\alpha\}$ называется *последователем.* Ординалы $\alpha \neq 0$, не являющиеся последователями, называются *предельными.* Если α предельный, то $\alpha = \sup\{\beta \mid \beta < \alpha\} = \cup\alpha$. Наименьший предельный ординал обозначается ω и совпадает с множеством натуральных чисел $\mathbb{N}$.

Следующая теорема выражает принцип *трансфинитной индукции,* обобщающий индукцию с множества натуральных чисел на класс всех ординалов.

Теорема 5 [Трансфинитная индукция] Пусть $C \subseteq \mathrm{Ord}$ — такой класс, 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

Начало лекции № 4

Доказательство. Если $C \neq \mathrm{Ord}$, то рассмотрим наименьший ординал, не принадлежащий C. Такой ординал всегда существует — это наименьший элемент множества $\alpha \setminus C$, где $\alpha \notin C$. и получаем противоречие.

Определение 14 *Трансфинитной последовательностью* элементов некоторого множества A называется множество $\{a_\xi \mid \xi < \alpha\}$, занумерованное ординалами (для каждого $\xi < \alpha$ предполагается $a_\xi \in A$); $\alpha \in \mathrm{Ord}$ — *длина* этой последовательности.

Пусть теперь G — функция, заданная на трансфинитных последовательностях элементов A (каждой трансфинитной последовательности функция G сопоставляет некоторый элемент A).

Теорема 6 [Трансфинитная рекурсия] Для каждого $\Theta \in \mathrm{Ord}$ найдется единственная трансфинитная последовательность $\{a_\xi \mid \xi < \Theta\}$ такая, что для каждого $\alpha < \Theta$ выполняется $a_\alpha = G(\{a_\beta \mid \beta < \alpha\})$. Иными словами: пусть S — класс трансфинитных последовательностей элементов A, G — функция из S в A. Тогда найдется единственная функция F из Ord в A, такая что для всех $\alpha \in \mathrm{Ord}$ выполняется $F(\alpha) = G(F|_\alpha)$[4].

Пример 5 Прежде чем доказывать общий факт, рассмотрим некоторые примеры применения теоремы. Определим сложение ординалов так:

$$\begin{aligned} \alpha + 0 &= \alpha, \\ \alpha + (\beta + 1) &= (\alpha + \beta) + 1, \\ \alpha + \beta &= \lim_{\xi \to \beta}(\alpha + \xi),\ \beta \text{ — предельный.} \end{aligned}$$

(Здесь $\lim\limits_{\xi \to \beta}(\alpha + \xi) = \sup\{\alpha + \xi \mid \xi < \beta\}$.) Тогда существует функция $+\colon \mathrm{Ord} \times \mathrm{Ord} \mapsto \mathrm{Ord}$, обладающая этими свойствами. В самом деле: определим такую функцию G_α следующим образом:

$$\begin{aligned} G_\alpha(\Lambda) &= \alpha \\ G_\alpha(\{a_\xi \mid \xi < \gamma\}) &= \begin{cases} a_\beta + 1, & \text{если } \gamma = \beta + 1, \\ \sup\{a_\xi \mid \xi < \gamma\}, & \text{если } \gamma \text{ — предельный.} \end{cases} \end{aligned}$$

[4]Здесь незримо использована аксиома подстановки: нужно, чтобы $F|_\alpha \overset{def}{=} \{F(\xi) \mid \xi < \alpha\}$ было множеством, ведь только множества можно подставлять в качестве параметра в функцию G!

Теперь применим теорему.

Умножение:

$$\begin{aligned} \alpha \times 0 &= 0 \\ \alpha \times (\beta + 1) &= \alpha \times \beta + \alpha, \\ \alpha \times \lambda &= \sup_{\beta<\lambda}(\alpha \times \beta), \quad \lambda \text{ — предельный.} \end{aligned}$$

Возведение в степень:

$$\begin{aligned} \alpha^0 &= 1, \\ \alpha^{\beta+1} &= \alpha^\beta \times \alpha, \\ \alpha^\lambda &= \sup_{\beta<\lambda}(\alpha^\beta), \quad \lambda \text{ — предельный.} \end{aligned}$$

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

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

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

Положим $F \overset{def}{\leftrightharpoons} \bigcup\mathcal{F}$. Докажем, что

1) F — функция.

2) $\text{dom}F = \text{Ord}$.

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

Нам понадобится следующая

Утверждение 6 Если $f_1, f_2 \in \mathcal{F}$ и $\text{dom}(f_1) = \alpha < \beta = \text{dom}(f_2)$, то $f_1 \subseteq f_2$.

Доказательство. Аналогично единственности.

Пункт 1) непосредственно следует из леммы. Докажем 2). Предположим что $\text{dom}(F) \neq \text{Ord}$, выберем $\alpha_0 = \min(\text{Ord} \setminus \text{dom}F)$. Тогда $\forall\beta < \alpha_0\ \beta \in \text{dom}F$. Тогда $F|_{\alpha_0}$ определено, положим $x \overset{def}{\leftrightharpoons} G(F|_{\alpha_0})$, $f_0 \overset{def}{\leftrightharpoons} (F|_{\alpha_0}) \cup \{\langle\alpha_0, x\rangle\}$, то есть продолжим $F|_{\alpha_0}$ до f_0, положив $f(\alpha_0) \overset{def}{\leftrightharpoons} x$. По построению, $f_0 \in \mathcal{F}$, $\text{dom}(f_0) = \alpha_0 + 1$. Противоречие.

Для доказательства 3) заметим, что $F(\alpha) = f(\alpha)$ для некоторого $f \in \mathcal{F}$. Поскольку $f(\alpha) = G(f|_\alpha) = G(F|_\alpha)$, получим $F(\alpha)G(F|_\alpha)$.

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

Аксиома выбора

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 7 [Цермело, принцип вполне упорядочения] Пусть X — произвольное множество; тогда существует такое отношение $<$ на X, что $(X, <)$ — вполне упорядочено.

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

Ниже приведем пример использования Леммы Цорна.

Определение 15 *базис Гамеля $\mathbb{R}$ над $\mathbb{Q}$,* —это такое подмножество $B \subset \mathbb{R}$, что

$$\forall x \in \mathbb{R}\ \exists r_1 \dots r_n \in B, \exists q_1 \dots q_n \in \mathbb{Q}(x = q_1 r_1 + q_2 r_2 + \dots + q_n r_n)$$
$$\forall r_1 \dots r_n \in B\ \forall q_1 \dots q_n \in \mathbb{Q}\ \ (q_1 r_1 + \dots + q_n r_n = 0 \Longleftrightarrow q_1 = \dots = q_n = 0).$$

Теорема 9 Существует

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

$$\forall r_1 \dots r_n \in B\ \forall q_1 \dots q_n \in \mathbb{Q}\ \ (q_1 r_1 + \dots + q_n r_n = 0 \Longleftrightarrow q_1 = \dots = q_n = 0).$$

Положим $\mathcal{B} \overset{def}{\rightleftharpoons} \{B \subseteq \mathbb{R} \mid B$ — линейно независимо над $\mathbb{Q}\}$ с отношением $\subseteq$ на нем. Рассмотрим цепь $C \subseteq \mathcal{B}$. Множество $\bigcup C$ тоже линейно независимое. В самом деле, любая линейная комбинация $q_1 r_1 + \dots + q_n r_n$ элементов r_i множества $\bigcup C$, по определению, конечна, и каждое для каждого i имеем $r_i \in C_i \in C$. Среди C_i выберем наибольший

по включению, пусть это для определенности C_0. Тогда $\forall i\ (r_i \in C_0)$. Поскольку C_i линейно независимое множество векторов, получим $q_1 = \ldots = q_n = 0$.

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

Конец лекции № 4

Начало лекции № 5

Доказательство.

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 является максимальным элементом, поэтому $\exists d > b \geqslant x \in C$, и d является строгой верхней гранью. Обозначим $\Psi(C) = \{a \mid a$ — строгая верхняя грань $C\}$. (По аксиоме выделения $\Psi(C)$ — множество.) Применяем аксиому выбора: $\exists f\, \forall C\ f(\Psi(C)) \in \Psi(C)$. Положим $\varphi(C) \overset{def}{\rightleftharpoons} f(\Psi(C)) \in \Psi(C)$.

Используя φ, построим "слишком большую цепь", которая не поместится в A, что и приведёт к противоречию.

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

1) $(B, <)$ — вполне упорядочено,

2) $\forall x \in B\ x = \varphi(B_x)$, где $B_x \overset{def}{\rightleftharpoons} \{y \in B \mid y < x\}$.

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

Утверждение 7 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.

Доказательство. 1) Пусть множества B и D корректны. Скажем, что I_0 — *общее начало* B и D, если оно является начальным отрезком их обоих. Обозначим $I \overset{def}{\rightleftharpoons} \bigcup\{I_0 \mid I_0$ — 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 если $y \in B$ и $y < x$, то $y \in I_0$, следовательно $y \in I$.

Если $I = B$ или $I = D$, то всё доказано: одно из множеств — начальный отрезок второго. Пусть, однако, $I \neq B$, $I \neq D$. Это даёт нам возможность (поскольку B вполне упорядоченно) выбрать $b \overset{def}{\rightleftharpoons} \min_B(B \setminus I)$, $d \overset{def}{\rightleftharpoons} \min_D(D \setminus I)$. I — общее начало для B и D; поэтому (второй пункт определения корректности) $b = \varphi(B_b) = \varphi(D_d) = d$, ибо

$B_b = D_d = I$. Тогда $I \cup \{b\}$ — общее начало для B и D, следовательно $I \cup \{b\} \subseteq I$, а значит $b \in I$. 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 $Y \subseteq U$ и $Y \neq \emptyset$. Возьмем некоторый элемент $y \in Y$. Поскольку $Y \subseteq \cup\mathcal{T}$, то $\exists B \in \mathcal{T}\ (y \in B)$. Следовательно, $y \in Y \cap B$ и $Y \cap B \neq \emptyset$. Значит, найдется m — наименьший элемент в $Y \cap B$ (т.к. B вполне упорядоченно). Тогда m — наименьший и в Y. (Действительно, иначе рассмотрим элемент $x \in Y$, такой что $x < y$. Тогда $x \in B$, поскольку B — начальный отрезок в $\cup\mathcal{T}$. Следовательно $x \in Y \cap B$ и $x < y$ — противоречие.)

4. Выполняется $\forall x \in U\ x = \varphi(U_x)$. Действительно, возьмём $x \in B \in \mathcal{T}$. Тогда $x = \varphi(B_x)$ из-за корректности B. 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. Следовательно, U — цепь, а $\varphi(U)$ — строгая верхняя грань для U. Тогда $U \cup \{\varphi(U)\}$ удовлетворяет определению корректного множества (по определению φимеем $\varphi(U) > x$ для всех $x \in U$ и $B_\varphi(U) = U$). Но тогда $\varphi(U) \in U$ (т.к. U содержит все элементы всех корректных множеств). 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 $W \overset{def}{\leftrightharpoons} \{(S, <_s) \mid (S, <_s)$ — вполне упорядочено$\}$ Введём порядок на W: $(S, <_s) \prec (T, <_t) \leftrightharpoons S \subsetneq T$ — начальный отрезок в $(T, <_T)$, и $<_S = <_T|_S$. Тогда оказывается, что $(W, \prec)$ удовлетворяет условиям леммы Цорна: пусть C — цепь в $(W, <)$; тогда, например, $\langle \bigcup\limits_{(S,<_S)\in C} S, \bigcup\limits_{(S,<_S)\in C} <_S, \in\rangle W$ является верхней гранью C в $(W, \prec)$.

Итак, в $(W, \prec)$ есть максимальный элемент $(M, <_M)$. Осталось доказать, что $M = X$. 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 10 [Кантора, о сравнении мощностей] Для любых двух множеств A и B существует инъекция из A в B или инъекция из B в A, то есть мощность одного не

превосходит мощности другого, и они сравнимы.

Доказательство. Вполне упорядочим оба множества и вспомним, что из двух вполне упорядоченных множеств одно изоморфно начальному отрезку другого.

3. Теорема Цермело $\Rightarrow$ аксиома выбора.

Фактически, эта часть уже доказана: если $(A, <_A)$, $X \subseteq A$, то положим $f(x) \overset{def}{\leftrightharpoons} \min_{<_A} X \in X$, что будет искомой функцией выбора.

Следствие 5 $(\mathbb{R}, +)$ и $(\mathbb{C}, +)$ изоморфны как группы.

Доказательство. Установим изоморфизм по базисам Гамеля мощности континуум.

Конец лекции № 5

Начало лекции № 6

1.3.2 Мощности и алефы

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

Определение 16 *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 11 [Кантора-Бернштейна] Если $A \lesssim B$ и $B \lesssim A$, то A равномощно B.

В условиях аксиомы выбора также устанавливается:

Теорема 12 [О сравнимости] Для любых A, B $A \lesssim B$ или $B \lesssim A$.

С ней же устанавливается и такая теорема:

Теорема 13 Всякое бесконечное множество содержит счётное подмножество.

Напомним определения:

Определение 17 A счётно, если $A \sim \omega$. A конечно, если $\exists n \in \omega\, A \sim n$. A бесконечно, если не является конечным.

Доказательство. В чём тут суть аксиомы выбора? Пусть мы хотим выбрать из множества счётное число точек $a_1, a_2 \dots$ Тогда мы хотим сопоставить $n \mapsto a_n$, $\omega \mapsto A$, построив последовательность $a_n = F(\{a_1, \dots, a_{n-1}\})$. 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 $F(B) = \varphi(A \setminus B)$. Можно вместо выбора по порядку и просто сослаться на полный порядок: если мы вполне упорядочили A, то, по теореме 12, $A \leq \omega$ или $\omega \leq A$.

Продолжим выводить из AC следствия.

Теорема 14 [О сюръекции] Если $\exists f\colon B \to A$ — сюръекция, то $A \lesssim B$.

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

Теорема 15 [Объединение счётных множеств счётно] $\bigcup\limits_{i\in\omega} A_i$ счётно, если все $A_i \sim \omega$.

Доказательство. $\forall i\ \exists a^i\colon \omega \to A_i$, 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 14.

Дадим главное определение.

Определение 18 Множество α — *кардинал,* если $\alpha \in \mathrm{Ord}$, и $\forall \beta < \alpha\ \beta \nsim \alpha$.

Следствие 6 ω — наименьший бесконечный кардинал.

Следствие 7 $\forall \alpha \in \mathrm{Ord}\ \exists \beta$ — кардинал: $\alpha \sim \beta$.

Доказательство. В совокупности всех ординалов, равномощных α, выберем минимальный элемент.

Следствие 8 Всякое множество X равномощно единственному кардиналу.

Доказательство. Вполне упорядочим X и рассмотрим $\sup\{\alpha \in \mathrm{Ord} \mid \alpha$ изоморфно начальному (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 19

$$\omega_0 = \aleph_0 \overset{def}{\rightleftharpoons} \omega. \tag{13}$$

$$\aleph_{\alpha+1} \overset{def}{\rightleftharpoons} \min\{x \mid x \text{ — кардинал, и } \aleph_\alpha < x\}. \tag{14}$$

$$\aleph_\lambda \overset{def}{\rightleftharpoons} \sup\{\aleph_\alpha \mid \alpha < \lambda\}, \text{ если } \lambda \text{ — предельный.} \tag{15}$$

Утверждение 8 $\forall \alpha \in \mathrm{Ord}\ \aleph_\alpha$ — кардинал.

Доказательство. В первых двух случаях всё очевидно. В третьем, если $\aleph_\lambda$ — не кардинал, то существует $\beta < \aleph_\lambda$, равномощный $\aleph_\lambda$, и следовательно $\exists \alpha < \lambda :\ \beta < \aleph_\alpha$. 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 20 $\varkappa^+ = \min\{\beta \mid \beta$ — кардинал, и $\varkappa < \beta\}$. $\varkappa$ — предельный кардинал, если $\forall \beta < \varkappa\ \exists \mu$ — кардинал такой, что $\beta < \mu < \varkappa$.

Утверждение 9 Для любого бесконечного кардинала $\varkappa$ существует и единственен $\alpha \in \mathrm{Ord} :\ \varkappa = \aleph_\alpha$. Таким образом, "функция" $\aleph$ не пропускает ни одного кардинала.

Доказательство. 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 21 *Мощность* A (обозначение: $|\mathrm{A}|$) — единственный кардинал, изоморфный A.

В предположении AC докажем важный факт.

Теорема 16 [Обобщённая лемма Кантора] Пусть A бесконечно. Тогда $A \times A \sim A$.

Доказательство. Следуя Гёделю, введём *каноническое*[5] *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 $\pi :\ \mathrm{Ord} \times \mathrm{Ord} \to \mathrm{Ord}$ («маршрут обхода произведения»), действующее по схеме:

$$\pi(\alpha, \beta) = \text{ порядковый тип } \{(x, y) \mid (x, y) < (\alpha, \beta)\}. \tag{16}$$

[5]Не лексикографическое!

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

Конец лекции № 6

Начало лекции № 7

Выпишем два полезных наблюдения о начальных сегментах.

Утверждение 10 Рассмотрим любой ординал α. Тогда $\alpha \times \alpha$ есть начальный сегмент в каноническом упорядочении, имеющий вид $\{(x,y) \mid (x,y) < (0,\alpha)\}$.

Доказательство. Понятно при внимательном рассмотрении квадрата.

Утверждение 11 $\pi[\alpha \times \alpha] \geq \alpha$.

Доказательство. Обозначим $f(\alpha) \overset{def}{\leftrightharpoons} \pi[\alpha \times \alpha]$. Тогда f сохраняет порядок: $\alpha < \beta \Rightarrow f(\alpha) < f(\beta)$ (ибо $\alpha \times \alpha \subset \beta \times \beta$), откуда $f(\alpha) \geq \alpha$ по утверждению 3.

Утверждение 12 $\pi[\aleph_\alpha \times \aleph_\alpha] = \{\pi(\alpha_1,\beta_1) \mid \alpha_1,\beta_1 < \aleph_\alpha\}$[6] $= \aleph_\alpha$ для всех α.

Доказательство. От противного. Положим $\varkappa$ — наименьший бесконечный кардинал, при котором $\pi[\varkappa \times \varkappa] > \varkappa$. Тогда существуют $\alpha,\beta < \varkappa : \ \pi(\alpha,\beta) = \varkappa$. Возьмём $\delta \in \mathrm{Ord} : \ \alpha,\beta < \delta < \varkappa$. 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 $|\pi[\delta \times \delta]| = |\delta \times \delta| \geq |\varkappa| = \varkappa$. Однако, с другой стороны, $|\delta \times \delta| = ||\delta| \times |\delta|| =$[7]$|\delta| < \varkappa$. Противоречие.

Следствие 9 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 22 $\varkappa^\mu \overset{def}{\leftrightharpoons} |\{f \colon \mu \to \varkappa\}|$.

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

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

Принято обозначать $2^{\aleph_0} = \mathfrak{c}$ — "континуум". Как оказалось, не зависит от ZFC ни обычная, ни *обобщённая континуум-гипотеза:* $\beth_\alpha = \aleph_\alpha \ \forall \alpha$.

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

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

Исчисление высказываний

Аксиоматика Гильберта. Классическая логика

Пусть $p_0, p_1 \ldots$ — счётный набор пропозициональных символов, $\wedge, \vee, \to, \neg$ — логические связки.

Определение 23 Формулы пропозициональной логики определяются индуктивно:

- всякая пропозициональная переменная — формула;
- если A и B — формулы, то $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ и $(\neg A)$ — формулы.

Мы принимаем соглашение о приоритете операций, которое позволяет опускать часть скобок: по убывания приоритета, операции расположены следующим образом

$$\neg,\ \wedge,\ \vee,\ \to\ .$$

Введём следующие схемы аксиом (здесь φ, ψ, θ — произвольные формулы):

A1 $\varphi \to (\psi \to \varphi)$.

A2 $(\varphi \to (\psi \to \theta)) \to ((\varphi \to \psi) \to (\varphi \to \theta))$.

A3 $\varphi \wedge \psi \to \varphi$, $\varphi \wedge \psi \to \psi$.

A4 $\varphi \to (\psi \to (\varphi \wedge \psi))$.

A5 $\varphi \to \varphi \vee \psi$, $\psi \to \varphi \vee \psi$.

A6 $(\varphi \to \theta) \to ((\psi \to \theta) \to ((\varphi \vee \psi) \to \theta))$.

A7 $(\varphi \to \psi) \to ((\varphi \to \neg\psi) \to \neg\varphi)$.

A8 $\varphi \to (\neg\varphi \to \psi)$ (ex falso sequitur quodibet)

A9 $\neg\neg\varphi \to \varphi$. (снятие двойного отрицания)

Правило вывода: modus ponens (MP).

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

Определение 24 *Вывод* — это последовательность формул $\varphi_1 \dots \varphi_n$, 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 формулой φ.

Пусть Γ — множество формул (называемых *гипотезами*); *выводом из гипотез* Γ называется последовательность формул, в которой всякая формула либо аксиома, либо принадлежит Γ, либо получена модус поненсом из двух ранее выписанных. Обозначение: $\Gamma \vdash \varphi$.

Приведём конкретный пример вывода.

Утверждение 13 $\vdash \varphi \to \varphi$ для любой φ.

Доказательство. Используются только первые две аксиомы, описывающие поведение импликации. В аксиому 2 подставим $\varphi = \varphi$, $\theta = \varphi$, $\psi = (\varphi \to \varphi)$:

1. $\varphi \to (\varphi \to \varphi)$ (A1)
2. $\varphi \to ((\varphi \to \varphi) \to \varphi)$ (A1)
3. $(\varphi \to ((\varphi \to \varphi) \to \varphi)) \to ((\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi))$ (A2)
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.

Упражнение 3 $p \wedge q \vdash q \wedge p$.

Доказательство.

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 факты, которые будут выведены, кроме особо оговорённых, можно вывести не только в классической логике высказываний, но и в интуиционистской. При удалении аксиом 8 и 9 одновременно получается *минимальная логика,* на изучении которой мы останавливаться не будем.

Несложно доказать следующие важные свойства выводимости из гипотез.

Утверждение 14 1. если $\Gamma \vdash \varphi$ и $\Gamma \subseteq \Delta$, то $\Delta \vdash \varphi$ (монотонность)

2. если $\Gamma \vdash \varphi$ и $\forall \psi \in \Gamma\ \Delta \vdash \psi$, то $\Delta \vdash \varphi$ (транзитивность)
3. если $\Gamma \vdash \varphi$, то существует конечное $\Delta \subseteq \Gamma$, такое что $\Delta \vdash \varphi$ (компактность)

И в классической, и в интуиционистской логике верна

Теорема 17 [О дедукции] $\Gamma, \varphi \vdash \psi \Leftrightarrow \Gamma \vdash \varphi \to \psi$.

Доказательство.

$\Rightarrow$ Очевидно.

$\Leftarrow$ Индукция по длине вывода $\Gamma, \varphi \vdash \psi$. Возможны четыре случая.

- ψ есть аксиома. Тогда достроим вывод так: $\psi \to (\varphi \to \psi)$, $\varphi \to \psi$.
- $\psi \in \Gamma$. То же самое: допишем ψ, $\psi \to (\varphi \to \psi)$, $\varphi \to \psi$.
- $\psi = \varphi$. Тогда нужно написать вывод для $\varphi \to \varphi$, что мы научились делать.
- ψ получена правилом MP из θ и $\theta \to \psi$. По предположению индукции, $\Gamma \vdash \varphi \to \theta$ и $\Gamma \vdash \varphi \to (\theta \to \psi)$. Возьмем соответствующие выводы и допишем их к нашему текущему выводу $\Gamma, \varphi \vdash \psi$. Затем дополним полученную последовательность формулами $(\varphi \to (\theta \to \psi)) \to ((\varphi \to \theta) \to (\varphi \to \psi))$, $(\varphi \to \theta) \to (\varphi \to \psi)$, $\varphi \to \psi$. Получим вывод формулы $\varphi \to \psi$ из гипотез Γ.

Упражнение 4 Закон контрапозиции: $\varphi \to \psi \vdash \neg\psi \to \neg\varphi$.

Доказательство. По теореме о дедукции, достаточно показать $\neg\psi, \varphi \to \psi \vdash \neg\varphi$. Приводим вывод:

$(\varphi \to \psi) \to ((\varphi \to \neg\psi) \to \neg\varphi)$. (7)
ψ (гипотеза)
$\neg\psi \to (\varphi \to \neg\psi)$ (1)
$\varphi \to \neg\psi$ (по MP)
$\neg\varphi$ (по MP)

Упражнение 5 Правило силлогизма: $\varphi \to \psi, \psi \to \theta \vdash \varphi \to \theta$.

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

Упражнение 6 Аксиома 8 следует из 9: $\varphi, \neg\varphi \vdash \psi$.

Доказательство. 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

Начало лекции № 8

Упражнение 7 $\vdash A \to \neg\neg A$.

Доказательство.

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

Упражнение 8 Обращение закона контрапозиции (только классическая логика!): $\neg B \to \neg A \vdash A \to B$.

Доказательство. $\neg B \to \neg A$

$\neg\neg A \to \neg\neg B$

$\neg\neg B \to B$

$\neg\neg A \to B$

$A \to \neg\neg A$

$A \to B$.

Упражнение 9 $A \wedge B \to C \vdash A \to (B \to C)$,

$A \to (B \to C) \vdash A \wedge B \to C$.

Доказательство.

- $A \wedge B \to C$ (гипотеза)

  A (гипотеза)

  B (гипотеза)

  $A \to (B \to A \wedge B)$ (4)

  $A \wedge B$ (MP дважды)

  C (MP 1,5)

- $A \to (B \to C)$ (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)

Докажем главное утверждение в этой части курса.

Теорема 18 [О корректности и полноте] $\vdash A \Leftrightarrow A$ — тавтология.

Доказательство. ($\Rightarrow$) 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.

($\Leftarrow$) Докажем, что всякая тавтология выводима. Приведём вариант рассуждения, который впоследствии будет удобно обобщить на интуиционистское исчисление высказываний и исчисление предикатов. Утверждение теоремы будет следовать из ряда лемм.

Определение 25 Пусть Γ — множество формул; будем говорить, что Γ *непротиворечивое*, если $\forall A_1 \dots A_n \in \Gamma \not\vdash \neg(A_1 \wedge A_2 \wedge ... \wedge A_n)$.

Γ *максимальное непротиворечивое*, если $\forall A \in \mathrm{Fm}\,(A \in \Gamma \vee \neg A \in \Gamma)$.

Утверждение 15 [0] Пусть Γ непротиворечиво, $A \in \mathrm{Fm}$. Тогда одно из множеств $\Gamma \cup \{A\}$ или $\Gamma \cup \{\neg A\}$ непротиворечиво.

Доказательство. От противного: пусть Γ непротиворечиво, но оба множества $\Gamma \cup \{A\}$ и $\Gamma \cup \{\neg A\}$ оказываются противоречивыми. Это означает, что существуют такие $A_1 \dots A_n, A'_1, \dots, A'_k \in \Gamma$, что $\vdash \neg(A \wedge \bigwedge\limits_{i=1}^{n} A_i)$ и $\vdash \neg(\neg A \wedge \bigwedge\limits_{j=1}^{k} A'_j)$. Применяя правило контрапозиции и аксиому А3, получим, что тогда

$$\vdash \neg(A \wedge \bigwedge_{i=1}^{n} A_i \wedge \bigwedge_{j=1}^{k} A'_j) \text{ и } \vdash \neg(\neg A \wedge \bigwedge_{i=1}^{n} A_i \wedge \bigwedge_{j=1}^{k} A'_j).$$

Далее обозначим $B \rightleftharpoons \bigwedge\limits_{i=1}^{n} A_i \wedge \bigwedge\limits_{j=1}^{k} A'_j$. Мы имеем $\vdash \neg(A \wedge B)$ и $\vdash \neg(\neg A \wedge B)$. Следовательно, используя аксиому А8, получим

$$\vdash A \wedge B \to C \text{ и } \vdash \neg A \wedge B \to C \ (C \text{ любое}).$$

Следовательно

$$B \vdash A \to C \text{ и } B \vdash \neg A \to C \ (C \text{ любое}).$$

и поскольку C – любое, по аксиоме А7

$$B \vdash \neg A \text{ и } B \vdash \neg\neg A.$$

По аксиоме А7, получим $\vdash \neg B$. Согласно определению непротиворечивости, это означает, что множество Γ противоречиво. Утверждение доказано.

Утверждение 16 [1] Если Γ непротиворечиво, то существует максимальное непротиворечивое $\Gamma' \supseteq \Gamma$.

Доказательство. Если множество переменных счётно, то и формул счётное число; для всякой формулы по порядку будем добавлять ее саму либо ее отрицание с сохранением непротиворечивости. Счётное объединение в пределе тоже непротиворечиво, т.к. противоречивость устанавливается конечным числом формул (по определению) и поэтому должна проявиться на конечном шаге.

Пусть множество переменных 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.

Утверждение 17 [2] Пусть Γ — максимальное непротиворечивое множество формул. Тогда

0. если $\Gamma \vdash A$, то $A \in \Gamma$;
1. если $\Gamma \ni A \wedge B$, то $\Gamma \ni A$ и $\Gamma \ni B$;
2. если $\Gamma \ni A \vee B$, то $\Gamma \ni A$ или $\Gamma \ni B$;
3. если $\Gamma \ni \neg A$, то $\Gamma \not\ni A$;
4. если $\Gamma \ni A \to B$, то $\Gamma \not\ni A$ или $\Gamma \ni B$.

Доказательство.

0. Пусть $\Gamma \vdash A$, но $A \notin \Gamma$. Тогда должно быть $\Gamma \ni \neg A$. Пусть $A_1 \dots A_n \in \Gamma$ — гипотезы, участвующие в выводе A из Γ. Тогда $\neg A \wedge A_1 \wedge \dots \wedge A_n \vdash A, \neg A$, и следовательно согласно аксиоме 7 $\vdash \neg(\neg A \wedge A_1 \wedge \dots \wedge A_n)$. Но Γ непротиворечиво. Противоречие.

Все последующие номера — упражнения с заменой выводимости на принадлежность, состоящие в честном переборе всех возможных по таблицам случаев и ссылкой на предположение индукции.

Пусть A — невыводимая тавтология. Тогда множество $\Gamma_0 = \{\neg A\}$ непротиворечиво. Используя лемму 0, расширим его до максимального непротиворечивого Γ. Зададим оценку такую, что

$$v(p) = 1 \rightleftharpoons p \in \Gamma.$$

Утверждение 18 [Основная] Для всякой формулы F имеем $v(F) = 1 \Leftrightarrow F \in \Gamma$.

Доказательство. Индукциея по построению формулы F, с использованием леммы 1.

По основной лемме, $v(A) = 0$, поскольку $\neg A \in \Gamma$. Теорема о полноте доказана.

Интуиционистская логика высказываний

В обычной логике адекватное понятие истинности — "быть тавтологией". Но в интуиционистской логике, хотя выводятся по-прежнему лишь тавтологии, совокупность всех выводимых формул меньше, нежели в классической. Традиционный пример невыводимой формулы — закон исключенного третьего, $p \vee \neg p$.. Для того чтобы доказать невыводимость этой формулы, нужна семантика для интуиционистской логики, отличная от таблиц истинности. Опишем *семантику Крипке.*

Определение 26 Модель Крипке $K = (W, R, v)$ — это тройка, в которой

- пара (W, R) называется *шкалой,*
  - W — непустое множество всех возможных миров,
  - $R \subseteq W^2$ — рефлексивное и транзитивное отношение достижимости на W,
- v — оценка истинности переменных, которая каждой переменной p сопоставляет некоторое подмножество W, $v(p) \subseteq W$; оценка v удовлетворяет свойству наследования истинности в достижимых мирах:

$$\text{если } x \in v(p),\ xRy,\ \text{то и } y \in v(p).$$

Пусть $x \in W$, $F \in \mathrm{Fm}$. Определим истинность формулы F в мире x $(K, x \models F)$ индукцией по построению формулы F:

1. $K, x \models p \Leftrightarrow x \in v(p)$.
2. $\vee, \wedge$ — по таблицам истинности.
3. $K, x \models \neg F \ \rightleftharpoons\ \forall y(xRy \Rightarrow \not\models F)$.
4. $K, x \models (F \to G) \ \rightleftharpoons\ \forall y(xRy \ \Rightarrow\ y \not\models F \text{ или } y \models G)$.

Утверждение 19 $\models$ монотонно, то есть $\forall x, y \in W\ \forall F \in \mathrm{Fm}$, если $x \models F$ и xRy, то $y \models F$.

Доказательство. Индукция по построению формулы, база индукции следует из определения модели Крипке.

Конец лекции № 8

Начало лекции № 9

Определение 27 Определим истинность формулы A в модели K. $K \models A$, если A истинно во всех мирах модели K.

Упражнение 10 $\neg A \vee B \to (A \to B)$ истинна во всех моделях Крипке (можно проверить). Напротив, $(A \to B) \to (\neg A \vee B)$ не является тавтологией семантики Крипке. Рассмотрим следующую модель: x, y — два мира, причем xRy, и в y выполняются A и B. Тогда $v(A) = v(B) = y$, но $x \models A \to B$, $x \not\models B$, $x \not\models \neg A$, следовательно, $x \not\models \neg A \vee B$.

Еще один пример тавтологии, которую можно опровергнуть в модели Крипке — формула $((p \to q) \to p) \to p$. Рассмотрим модель, состоящую из двух миров x, y, где xRy. Пусть p истинно только в y. Тогда $x, y \not\models p \to q$, следовательно $x \models (p \to q) \to p$, но $x \not\models p$.

Теорема 19 [О корректности и полноте в семантике Крипке] Если $\mathrm{Int} \vdash A$, то $K \models A$ для каждой модели K (корректность).

Если $\mathrm{Int} \nvdash A$, то существует конечная модель $K = (W, R, v)$ и мир $x \in W$, такие что $K, x \not\models A$. (полнота)

Доказательство.

Докажем корректность. Пусть $\mathrm{Int} \vdash A$. Индукцией по выводу проверим, что все формулы в выводе истинны во всех моделях Крипке. Истинность аксиом проверяется непосредственно. Шаг индукции — это применение правила вывода. Истинность B при условии истинности A и $A \to B$ следует из определения истинности импликации в мирах моделей Крипке.

Докажем полноту. Не имея закона исключённого третьего, мы не можем говорить, что либо формула, либо её отрицание содержится в максимальном непротиворечивом множестве. Поэтому будем рассматривать пары, состоящие из двух множеств формул: множество истинных и множество ложных формул. Чтобы обеспечить конечность модели, эти множества будем составлять из подформул нашей формулы A.

Через $Sub(A)$ обозначим множество подформул A.

Определение 28 Пара конечных множеств формул (Γ, Δ) *непротиворечива,* если $\mathrm{Int} \nvdash (\bigwedge \Gamma) \to (\bigvee \Delta)$. Пара *максимальная непротиворечивая,* если дополнительно к этому $\Gamma \cup \Delta = Sub(A)$.

Утверждение 20 [1] Если (Γ, Δ) — непротиворечивая пара, то существует максимальная непротиворечивая пара (Γ', Δ'), такая что $\Gamma \subseteq \Gamma',\ \Delta \subseteq \Delta'$.

Доказательство. Пусть $B_1, \ldots, B_n$ — все подформулы A и пара (Γ, Δ) непротиворечива. Тогда одна из пар $(\Gamma \cup \{B_i\}, \Delta)$ или $(\Gamma, \Delta \cup \{B_i\})$ также непротиворечива. В самом деле: пусть обе они противоречивы. Тогда $\mathrm{Int} \vdash (\bigwedge \Gamma) \wedge B_i \to (\bigvee \Delta)$ и $\mathrm{Int} \vdash (\bigwedge \Gamma) \to (\bigvee \Delta) \vee B_i$. Обозначим для краткости $G = \bigwedge \Gamma;\ D = \bigvee \Delta$. Покажем, что тогда пара (Γ, Δ) противоречива: последовательно выведем следующие формулы

1. $G \wedge B_i \to D$ (т.к. $(\Gamma \cup \{B_i\}, \Delta)$ противоречива);

2. $G \to B_i \vee D$ (т.к. $(\Gamma, \Delta \cup \{B_i\})$ противоречива);

3. G (гипотеза)

4. $B_i \vee D$ (MP 2,3)

5. $G \to (B_i \to D)$ (следует из формулы 1)

6. $B_i \to D$ (MP 3,5)

7. $D \to D$ (уже умеем)

8. $(B_i \to D) \to ((D \to D) \to (B_i \vee D \to D))$ (аксиома)

9. D (MP трижды)

По теореме дедукции, $\vdash G \to D$, следовательно пара (Γ, Δ) противоречива.

Утверждение 21 [2] Пусть (Γ, Δ) — максимальная непротиворечивая. Тогда:

1. если $B \wedge C \in \Gamma$, то $B, C \in \Gamma$; если $B \wedge C \in \Delta$, то $B \in \Delta$ или $C \in \Delta$;

2. если $B \vee C \in \Gamma$, то $B \in \Gamma$ или $C \in \Gamma$; если $B \vee C \in \Delta$, то $B, C \in \Delta$;

3. если $B \to C \in \Gamma$, то $C \in \Gamma$ или $B \in \Delta$;

4. если $\neg B \in \Gamma$, то $B \in \Delta$.

Доказательство.

1. От противного: пусть $B \wedge C \in \Gamma$, но $B \notin \Gamma$. Тогда $B \in \Delta$. Тогда имеем следующую цепочку выводимых следований: $\bigwedge \Gamma \to B \wedge C$, $B \wedge C \to B$, $B \to \bigvee \Delta$, и значит $\bigwedge \Gamma \to B$, $B \to \bigvee \Delta$ и (Γ, Δ) — противоречивое.

Пусть $B \wedge C \in \Delta$, но $B, C \notin \Delta$; следовательно, $B, C \in \Gamma$. Тогда $\bigwedge \Gamma \to B \wedge C$, $B \wedge C \to \bigvee \Delta$. Далее рассуждаем аналогично.

2. Случай дизъюнкции разбираем аналогично.

3. Пусть $B \to C \in \Gamma$, $C \notin \Gamma$ и $B \notin \Delta$. Тогда $C \in \Delta$, $B \in \Gamma$. Тогда $\bigwedge \Gamma \to (B \to C) \wedge B$, $(B \to C) \wedge B \to C$, $C \to \bigvee \Delta$. Следовательно, $\bigwedge \Gamma \to \bigvee \Delta$, и (Γ, Δ) противоречива.

Теперь мы готовы определить опровергающую модель. Положим $K = (W, R, v)$, где:

W — множество всех максимально непротиворечивых пар;

$(\Gamma, \Delta) R (\Gamma', \Delta')$, если $\Gamma \in \Gamma'$;

$v(p) = \{(\Gamma, \Delta) \mid p \in \Gamma\}$.

Утверждение 22 [3] W непусто и конечно, R рефлексивно и транзитивно, v монотонно относительно R.

Доказательство. W непусто: если $\mathrm{Int} \nvdash A$, то $(\emptyset, \{A\})$ непротиворечиво, следовательно эту пару можно пополнить до максимальной непротиворечивой пары $(\Gamma, \Delta) \in W$.

W конечно: Γ и Δ — подмножества конечного множества $Sub(A)$.

Рефлексивность и транзитивность R следует из рефлексивности и транзитивности $\subseteq$.

Монотонность v прямо следует из определений R и v.

Утверждение 23 [4, основная семантическая лемма] Пусть $(\Gamma, \Delta) \in W, B \in Sub(a)$. Тогда

если $B \in \Gamma$, то $(\Gamma, \Delta) \models B$;

если $B \in \Delta$, то $(\Gamma, \Delta) \not\models B$.

Доказательство. Индукция по построению формулы B. База следует из определения оценки v.

Конъюнкция: если $B_1 \wedge B_2 \in \Gamma$, то по лемме 2 $B_1, B_2 \in \Gamma$. По индукции, $(\Gamma, \Delta) \models B_1, B_2$ и следовательно $(\Gamma, \Delta) \models B_1 \wedge B_2$. Наоборот, если $B_1 \wedge B_2 \in \Delta$, то по лемме 2 $B_1 \in \Delta$ или $B_2 \in \Delta$. По индукции, $(\Gamma, \Delta) \not\models B_1$ или $(\Gamma, \Delta) \not\models B_2$, и следовательно $(\Gamma, \Delta) \not\models B_1 \wedge B_2$. Дизъюнкция разбирается аналогично.

Импликация: пусть $B_1 \to B_2 \in \Gamma$. Тогда если $(\Gamma, \Delta) R (\Gamma', \Delta')$, то по определению R $\Gamma \subseteq \Gamma'$ и следовательно $B_1 \to B_2 \in \Gamma'$. Тогда по лемме 2 $B_1 \in \Delta'$ или $B_2 \in \Gamma'$, откуда по индукции получаем $(\Gamma', \Delta') \not\models B_1$ или $(\Gamma', \Delta') \models B_2$. Следовательно, $(\Gamma, \Delta) \models B_1 \to B_2$.

Пусть теперь $B_1 \to B_2 \in \Delta$. Рассмотрим пару $(\Gamma \cup \{B_1\}, \{B_2\})$. Эта пара непротиворечива: в самом деле, в противном случае, если бы формула $(\bigwedge \Gamma) \wedge B_1 \to B_2$ была выводимой, то, по теореме о дедукции, выводилось бы и $(\bigwedge \Gamma) \to (B_1 \to B_2)$. Но, поскольку $(B_1 \to B_2) \in \Delta$, это означало бы, что и исходная пара (Γ, Δ) противоречива. Пользуясь леммой 1 расширяем $(\Gamma \cup \{B_1\}, \{B_2\})$ до максимальной непротиворечивой пары (Γ', Δ'). Поскольку $\Gamma \subseteq (\Gamma \cup \{B_1\}) \subseteq \Gamma'$, выполнено соотношение $(\Gamma, \Delta) R (\Gamma', \Delta')$; кроме того, $(\Gamma', \Delta') \models B_1$; $(\Gamma', \Delta') \not\models B_2$ (предположение индукции). Следовательно, $(\Gamma, \Delta) \not\models B_1 \to B_2$.

Пусть теперь Int $\not\vdash A$. Тогда пара $(\emptyset, \{A\})$ непротиворечива. Расширим до максимальной непротиворечивой пары $(\Gamma, \Delta) \in W$, где $A \in \Delta$. Тогда $(\Gamma, \Delta) \not\models A$ (так как $A \in \Delta$). Теорема доказана.

На самом деле, верно и более сильное утверждение.

Теорема 20 Если Int $\not\vdash A$, то существует конечное дерево D, в корне которого опровергается A.

Доказательство. Пусть Int $\not\vdash A$, тогда найдется конечная модель K и точка a этой модели, такие что $K, a \not\models A$. Сузим рассмотрение до $W' \stackrel{def}{=\!=} \{x \mid aRx\}$. R на W' остаётся рефлексивным и транзитивным. Рассмотрим $K' = (W', R, v)$, по-прежнему, $K', a \not\models A$. Перейдём теперь к новой структуре $D = (U, \tilde{R}, \tilde{v})$, вершинами которой объявляются все пути в графе (W', R) с началом в a. Таким образом, каждая вершина

x модели K' расщепляется на несколько по числу незацикливающихся путей, ведущих в неё. Если $b, c \in U$ — два пути, мы будем говорить, что $b\tilde{R}c$, если b — начало пути c. Наконец, переменная p истинна в точке $b = (a, \ldots, x) \in U$, если $x \in v(p)$, т.е. $\tilde{v}(p)$ состоит из тех путей, которые оканчиваются в вершинах, ринадлежащих $v(p)$.

Индукцией по построению формулы F несложно доказать, что

$$D, (a, \ldots, x) \models F \Leftrightarrow K', x \models F.$$

Следовательно, D конечное дерево, и $D, (a) \not\models A$.

Следствие 10 Свойство дизъюнктивности: если $\mathrm{Int} \vdash A \vee B$, то $\mathrm{Int} \vdash A$ или $\mathrm{Int} \vdash B$.

Доказательство. Пусть $\mathrm{Int} \nvdash A$ и $\mathrm{Int} \nvdash B$. Построим деревья $K_1 = (W_1, R_1, v_1)$ и $K_2 = (W_2, R_2, v_2)$, в нижних точках которых, a_1 и a_2, опровергаются A и B соответственно. Объединим эти деревья и добавим новый корень a_0, т.е. положим $K = (W, R, v)$, где

$$\begin{aligned} W &= W_1 \cup W_2 \cup \{a_0\} \\ R &= R_1 \cup R_2 \cup \{(a_0, x) \mid x \in R_1 \cup R_2\} \\ v &= v_1 \cup v_2 \end{aligned}$$

Тогда для каждого $x \in W_i$ и каждой формулы F имеем $K, x \models F \Leftrightarrow K_i, x \models F$, и следовательно $K, a_1 \not\models A$, $K, a_2 \not\models B$. Следовательно по монотонности истинности формул $K, a_0 \not\models A,\ B$ и $K, a_0 \not\models A \vee B$. Противоречие с выводимостью $A \vee B$.

Конец лекции № 9

Начало лекции № 10

Следствие 11 Интуиционистская логика разрешима (то есть разрешимо множество всех теорем Int).

Доказательство. Множество теорем интуиционистской логики перечислимо: перечисляем всевозможные выводы в Int и выписываем заключительные формулы в них. Дополнение множества всех формул до Int также перечислимо: если формула не является теоремой, то существует конечная модель Крипке, опровергающая её. Перечисляем все конечные модели и в каждой проверяем истинность данной формулы; как только найдется опровергающая модель, выдадим 1 и останавливаем процесс. Этот алгоритм вычисляет полухарактеристическую функцию для множества $\mathrm{Fm} \setminus \mathrm{Int}$, равную 1 на этом множестве и не определённая на его дополнении. По теореме Поста, перечислимое множество с перечислимым дополнением разрешимо (на данной формуле запустим оба алгоритма, описанных выше, одновременно; вернем 1, если формула появится в результате алгоритма, перечисляющего Int, и 0, если завершил работу алгоритм для полухарактеристической функции). Рано или поздно мы получим ответ о том, является ли формула теоремой Int .

Теорема 21 [Гливенко] $\mathrm{CL} \vdash \varphi \Longleftrightarrow \mathrm{Int} \vdash (\neg\neg\varphi)$.

Доказательство. ($\Leftarrow$) Очевидно: выведем в Int формулу $\neg\neg\varphi$, затем снимем двойное отрицание.

($\Rightarrow$) От противного: пусть $\mathrm{Int} \nvdash \neg\neg\varphi$. Построим опровергающее дерево для $\neg\neg\varphi$. Поскольку в корне $a \not\models \neg(\neg\varphi)$, то есть вершина x, в которой $x \models \neg\varphi$. Отсюда для каждого y, такого что xRy, получим $y \not\models \varphi$. Возьмем в качестве y любой лист, достижимый из x, тогда $y \not\models \varphi$. Но в листах дерева и отрицание, и импликация устроены по классическому образцу, то есть в них истинны все классические тавтологии. Следовательно φ не является тавтологией, и $\mathrm{CL} \nvdash \varphi$.

Теорема 22 [Гёдель] Интуиционистская логика не конечнозначна: это значит, что нельзя предложить n значений истинности с выделенной единицей и интерпретировать дизъюнкцию, конъюнкцию, импликацию и отрицание обычными функциями двух (одной) дискретных переменных, чтобы воспроизвести интуиционистскую логику как множество формул, всегда принимающих значение единица. (Так, CL двузначна.)

Доказательство. От противного: пусть логика Int n-значна ($n \geq 2$). Рассмотрим формулу $I_n \overset{def}{=\!=} \bigvee\limits_{0 \leq i < j \leq n} (p_i \Leftrightarrow p_j)$. Очевидно, что она не выводима в интуиционистской логике: построим дерево из корня и $n+1$ листьев $a_1 \dots a_{n+1}$, положим $v(p_i) = a_i$ для каждого i. Тогда в корне ложна всякая из представленных эквивалентностей, а значит, и дизъюнкция в целом. Однако в любой n-значной логике функция, соответствующая такой формуле, содержала бы не более n различных значений на $(n+1)$ переменную, по принципу Дирихле одна из эквивалентностей обращалась бы в единицу и обращала бы в единицу и всю формулу I_n. Противоречие.

Назовём правилом вывода любую фигуру следующего вида: (здесь $\varphi_i, \varphi \in \mathrm{Fm}$)

$$\frac{\varphi_0 \ \dots \ \varphi_n}{\varphi}$$

Скажем, что правило *допустимо в логике* L, если для всякой подстановки σ из того что $L \vdash \varphi_{i\sigma}$ для всех i следует $L \vdash \varphi_\sigma$. Правило *выводимо в* L, если $\varphi_0 \dots \varphi_n \vdash_L \varphi$. Выводимые правила допустимы; в классической логике верно и обратное, а в интуиционизме — нет.

Правило Скотта:

$$\frac{(\neg\neg p \to p) \to p \vee \neg p}{\neg p \vee \neg\neg p}$$

Утверждение 24 Правило Скотта допустимо, но не выводимо в Int.

Доказательство. В самом деле, по теореме о дедукции для второго достаточно доказать, что $\mathrm{Int} \nvdash ((\neg\neg p \to p) \to p \vee \neg p) \to \neg p \vee \neg\neg p$. Построим модель 1->2, 1->3,

2->4, где в 4 истинно p. Тогда в a ложны и $\neg p$, (по 4) и $\neg\neg p$ (по 3, где $\neg p$). Тогда в 1 истинна посылка: в 4 $p \vee \neg p$, потому что p, а в 3 — потому что $\neg p$; в 2 $\not\models \neg\neg p \to p$: во всех точках есть посылка либо нет заключения, и вся формула в 1 ложна. Для допустимости заметим, что единственная разрешённая подстановка σ — это заменить p на какую-то формулу φ. Допустим, что $\mathrm{Int} \not\vdash \neg\varphi \vee \neg\neg\varphi$. Построим модель, в корне которой она ложна. Тогда $\mathrm{Int} \not\vdash \neg\varphi$ и $\mathrm{Int} \not\vdash \neg\neg\varphi$. Используя теорему Гливенко и снятие *тройного* отрицания в интуиционизме, получаем $\mathrm{CL} \not\vdash \neg\varphi$ и $\mathrm{CL} \not\vdash \varphi$. Построим два дерева, в корнях которых $\not\models \neg\varphi$ и $\not\models \varphi$ соответственно, добавим к ним новый корень, в нём будет $\not\models \neg\neg\varphi$, верхняя формула верна, а нижняя — нет.

Конец лекции № 10

Начало лекции № 11

Исчисление предикатов. Теория моделей

Структура и основные теоремы логики предикатов

Язык L_Σ исчисления предикатов содержит:

- *сигнатуру* $\Sigma = \mathrm{Func}_\Sigma \cup \mathrm{Pred}_\Sigma$ — множества имён предикатов и функций с указанием их валентности;
- стандартные символы: переменные $v_0, v_1, ...$;
- логические связки и кванторы $\vee, \wedge, \to, \neg, \forall, \exists$;
- вспомогательные символы: ( ) ,

Определение 29 *Термы* (множество термов сигнатуры σ обозначается через Term_Σ) — это слова, построенные по следующим правилам:

1. v_i и константы — термы;

2. если $f \in \mathrm{Func}_\Sigma$ — функциональный символ валентности n (часто будем писать f^n или $val(f) = n$), $t_1, \ldots, t_n$ — термы, то и выражение $f(t_1, \ldots, t_n)$ — терм.

Определение 30 *Формулы* (Fm_Σ) определяются по следующим индуктивным правилам:

1. если $P \in \mathrm{Pred}_\Sigma$, $val(P) = n$, $t_1 \ldots t_n \in \mathrm{Term}_\Sigma$, то $P(t_1 \ldots t_n)$ — (атомарная) формула;

2. если A, B — формулы, то $(A \wedge B), (\neg A), (A \vee B), (A \to B)$ — формулы;

3. если A — формула, то $(\forall x A), (\exists x A)$ — формулы. В этих формулах A называется областью действия квантора.

Вхождения переменной при кванторах и в области действия квантора по этой переменной называются *связанными*, остальные — *свободными*.

Терм, не содержащий переменных (т.е. построенный только из констант) называется *замкнутым*. Формула, не содержащая свободных вхождений переменных, называется *замкнутой*.

Определение 31 *Модель, или алгебраическая структура* сигнатуры Σ — это некоторое множество M и отображение, сопоставляющее (n-местному) предикатному каждому символу $P \in \mathrm{Pred}_\Sigma$ (n-местный) предикат P_M на M (то есть отображение $P\colon M^n \to \{0, 1\}$), а функциональному символу $f \in \mathrm{Func}_\Sigma$ — функцию f_M, то есть отображение $f\colon M^n \to M$.

Индукцией по построению формулы определим свободное и связанное вхождения переменной в формулу.

Определение 32 *Вхождением* будем называть любой экземпляр переменной в записи формулы.

1. В атомарной формуле A все вхождения всех переменных — свободные.
2. При образовании формулы из A и B связками логики высказываний сохраняются свободные и связанные вхождения переменных.
3. В формулах $\forall v_i A$, $\exists v_i A$ все вхождения v_i связаные, свободные и связанные вхождения остальных переменных сохраняются.

Определение 33 $A[v_i/t]$ — результат замены всех свободных вхождений v_i в A на терм t. *Замкнутая формула* — формула без свободных переменных.

Для любой модели естественным образом определяются *значения* замкнутых формул и термов. А именно:

Определение 34 Расширим модель (M, Σ), до так называемого *языка диаграммы,* обогатив язык константами для всех элементов M: $(M; \Sigma, \{a' : a \in M\})$, где a' — константа. Пусть t — замкнутый терм (то есть не содержащий переменных) языка диаграммы M; значение терма t, обозначаемое t_M, определим индуктивно.

1. если c — константа из Σ, то c_M — соответствующий элемент в M, который сопоставлен этой константе интерпретирующим отображением;
2. если $c = a'$, то $c_M = a$;
3. если $t = f(t_1, \ldots, t_n)$, то $t_M = f_M((t_1)_M, \ldots, (t_n)_M)$.

Определение 35 Пусть $M_\sigma = (M, \Sigma)$; будем говорить, что замкнутая формула A истинна в M_σ ($M_\sigma \models A$), если:

1. пусть $A = P(t_1, \ldots, t_n)$; тогда $M_\sigma \models A \Leftrightarrow P_M((t_1)_M, \ldots, (t_n)_M) = 1$;
2. $M_\sigma \models (A \wedge B) \;\Leftrightarrow\; M_\sigma \models A$ и $M_\sigma \models B$,
   $M_\sigma \models (A \vee B) \;\Leftrightarrow\; M_\sigma \models A$ или $M_\sigma \models B$,
   $M_\sigma \models (A \to B) \;\Leftrightarrow\; M_\sigma \not\models A$ или $M_\sigma \models B$,
   $M_\sigma \models (\neg A) \;\Leftrightarrow\; M_\sigma \not\models A$;
3. $M_\sigma \models (\forall x A)$, если для всех $a \in M$ $M_\sigma \models A[x/a]$;
   $M_\sigma \models (\exists x A)$, если существует $a \in M$ такой, что $M_\sigma \models A[x/a]$.

Скажем, что формулы *эквивалентны*, $(A \equiv B)$, если $M_\sigma \models A \Leftrightarrow M_\sigma \models B$. Для незамкнутых формул договоримся, чтобы $\forall \vec{a} \in M\ (M_\sigma \models A[x/a] \Leftrightarrow M_\sigma \models B[x/a])$, где $\vec{x}$ содержит все свободные переменные A и B.

Теперь сформулируем аксиомы и правила исчисления предикатов (сигнатуры Σ).

A1 Схемы аксиом логики высказываний, например, $A \to (B \to A)$, где $A, B \in \mathrm{Fm}_\Sigma$.

A2 $(\forall x A) \to A[x/t]$, если терм t подстановочен вместо x в A, то есть никакое вхождение ни одной из переменных, присутствующих в терме t, не превратится в связанное в результате его подстановок в формулу $A[x/t]$;

A3 $A[x/t] \to (\exists x A)$ при тех же условиях[8].

R Правило Modus Ponens и правила Бернайса:

$$\frac{A,\ A \to B}{B}, \qquad \frac{A \to B}{A \to (\forall x B)}, \qquad \frac{B \to A}{(\exists x B) \to A}$$

(если x не входит свободно в A);

Теорема 23 [О корректности] Если $\mathrm{PC}_\Sigma \vdash A$, то для любой модели M_σ сигнатуры Σ для всех $a \in M\ M_\sigma \models A[a]$.

Доказательство. Индукция по выводу A.

Конец лекции № 11

Начало лекции № 12

Теорема 24 [О дедукции] Если Γ, A состоит из замкнутых формул, то

$$\Gamma, A \vdash B \Leftrightarrow \Gamma \vdash A \to B.$$

Замечание 8 Если разрешить незамкнутые посылки, то теорема неверна. В самом деле: из гипотезы $A(x)$ выводится формула $\forall x\ A(x)$ (первое правило Бернайса), а вот $A(x) \to \forall x\ A(x)$ вообще не общезначима.

Доказательство. (В сложную сторону) Индукция по построению вывода $\Gamma, A \vdash B$. Первые четыре варианта разбираются совершенно аналогично пропозициональному случаю.

- B аксиома исчисления предикатов. $B,\ B \to (A \to B),\ A \to B$.
- $B \in \Gamma$. То же самое.

[8] Приведём пример важности условия подстановочности. Пусть дана формула $\forall x[\exists y(x \neq y)] \to (\exists y(t \neq y))$. Попытка подставить вместо t терм y приведёт к конфузу.

- $B = A$. $\vdash A \to A$.
- Пусть B получена по правилу MP. $B = B_2\ \Gamma, A \to B_1\ \Gamma, A \vdash B_1 \to B_2$. Тогда добавляем в вывод:

  $\Gamma \vdash A \to B_1, \Gamma \vdash A \to (B_1 \to B_2), (A \to (B_1 \to B_2)) \to ((A \to B_1) \to (A \to B_2)), MP, MP, \Gamma \vdash A \to B_2$.
- Существенный случай: пусть применялось правило Бернайса: например, из предположения индукции $A \to (\varphi \to \psi)$ нужно получить $A \to (\varphi \to \forall x\, \psi(x))$, где x не параметр формулы ψ. Здесь можно перейти, например, от $A \to (\varphi \to \psi)$ к $(A \wedge \varphi) \to \psi$ и уже здесь применить правило Бернайса (поскольку A замкнута и заведомо не может иметь параметр x); из полученной $(A \wedge \varphi) \to \forall x\, \psi$ осталось симметрично вернуть A влево.

  Аналогично рассматривается и второе правило Бернайса, только теперь $A \to (\varphi \to \psi)$ нужно по пропозициональным тавтологиям переписать как $\varphi \to (A \to \psi)$, навесить квантор существования слева и протащить A обратно.

Определение 36 *Теория T* — это множество замкнутых формул. T *непротиворечива,* если из неё нельзя вывести противоречие, то есть $\nexists A\ T \vdash A, \neg A$.

Теорема 25 [Теорема о полноте в форме существования модели; Гёдель, 1929] Всякая непротиворечивая теория имеет модель, т.е. если $T \nvdash \bot$, то найдется модель M_σ, такая что $M_\sigma \models T$.

Идея рассуждения такова: в качестве искомой модели рассмотреть совокупность всех замкнутых термов в некотором расширении нашей сигнатуры. Тогда термы интерпретируются сами собой (если M — множество замкнутых термов, то функциональному символу f^n можно сопоставить отображение из M^n в M, которое переводит набор термов $t_1, \ldots, t_n$ в терм $f^n(t_1, \ldots, t_n)$), но если термов "слишком мало", неясно даже, как интерпретировать предикаты, не говоря уже о возможности навешивать квантор с сохранением истинности. Для реализации нашей программы язык теории и саму теорию необходимо расширять, что мы и далее сделаем, следуя Хенкину[9] (1947).

Конец лекции № 12

Начало лекции № 13

Определение 37 T — теория со *свойством Хенкина,* если для любой выводимой в T *экзистенциальной* формулы, то есть формулы вида $\exists x \varphi(x)$, существует такая константа $c \in \mathrm{Const}_\Sigma$, что $T \vdash \varphi(c)$.

[9]Хенкин, Леон Альберт (1921 – 2006) — американский логик XX века, профессор Калифорнийского университета.

Определение 38 Теорию T назовем *полной,* если T непротиворечива и для любой замкнутой формулы $\varphi \in \mathcal{M}_T$ имеем $T \vdash \varphi$ или $T \vdash \neg\varphi$.

Упражнение 11 $Th(M_\sigma) = \{A \mid M_\sigma \models A\}$ является полной теорией; её принято называть *элементарной теорией модели* M_σ.

Следующая лемма обосновывает значение введённых понятий.

Утверждение 25 [1, о существовании модели] Если T — полная теория со свойством Хенкина, то у неё существует модель $\mathcal{M} \models T$.

Доказательство. Пусть M — множество всех замкнутых термов Σ. Для каждого функционального символа f^n положим

$$f^n_M(t_1, \ldots, t_n) \overset{def}{\rightleftharpoons} f^n(t_1, \ldots, t_n),$$

а значение предиката $P_M(t_1, \ldots, t_n)$, соответствующего символу P^n, свяжем с теорией T:

$$P_M(t_1, \ldots, t_n) \overset{def}{\rightleftharpoons} \begin{cases} 1 & \text{если } T \vdash P(t_1, \ldots, t_n) \\ 0 & \text{если } T \vdash \neg P(t_1, \ldots, t_n) \end{cases}$$

Докажем, что истинность любой формулы логики предикатов в предложенной M тогда в точности эквивалентна её выводимости в рамках теории T. Индукция по глубине формулы A.

Случай 1: A атомарная формула. Утверждение следует из определения истинности предиката в построенной модели.

Случай 2: A получена с помощью логической связки. Рассуждаем по аналогии с пропозициональным случаем. Утверждение, что $T \vdash \neg A$ эквивалентно $T \nvdash A$ формализует полноту и непротиворечивость T, свойства конъюнкции, дизъюнкции и импликации устанавливаем разбором случаев или же ссылкой на выводимость частных случаев всех тавтологий логики высказываний.

Случай 3: A имеет вид $\exists x\, \varphi(x)$. Пусть A выводима. Это значит, что (используем свойство Хенкина) существует такая константа (то есть замкнутый терм теории T) c, что $\varphi(c)$ выводима. По предположению индукции, $\varphi(c)$ истинна; итак, в самом деле существует такой терм, что φ обращается в истину, то есть $\exists x\, \varphi(x)$, и $M \models A$.

Обратно: пусть A истинна в M. Это означает по её смыслу, что есть некий терм $t \in M$, обращающий в истину формулу φ. По предположению индукции, тогда $\varphi(t)$ выводима; но формула $\varphi(t) \to \exists x \varphi(x)$ является одной из аксиом. Следовательно $T \vdash A$.

Итак, ближайшая наша цель — так расширить теорию T (и обогатить её язык константами), чтобы она обрела два свойства: полноты и Хенкина, не утратив при этом своей непротиворечивости. Начнём с полноты, она обеспечивается аналогично логике высказываний.

Утверждение 26 [2, Линденбаума] Всякая непротиворечивая теория T в сигнатуре Σ имеет в Σ полное расширение.

Доказательство. Вместо повторения рассуждений из пропозиционального случая с последовательным добавлением в теорию либо формулы φ, либо $\neg\varphi$, которое отлично работает в случае счётной сигнатуры, но перестаёт нас удовлетворять при увеличении её мощности, когда формул становится слишком много. Поэтому взамен мы неконструктивно сошлёмся на лемму 8: рассмотрим множество всех непротиворечивых теорий, содержащих T и упорядоченных по включению. Если $\{T_i \mid i \in I\}$ — цепь, то объединение всех T_i является её верхней гранью. Теперь фиксируем максимальный элемент и замечаем, что его противоречивость достигалась бы конечным числом аксиом и поэтому выявилась бы уже на конечном шаге построения.

Теперь научимся расширять теорию, добиваясь свойства Хенкина. Очевидно следующее утверждение:

Утверждение 27 [3, о свежей константе] Пусть T — теория в Σ, и $c \notin \Sigma$. Тогда, если $T \vdash \varphi(c)$ в сигнатуре $\Sigma \cup \{c\}$, то $T \vdash \varphi(a)$, где a — прежде не использовавшаяся в выводе $\varphi(c)$ свободная переменная.

Доказательство. В выводе $\varphi(c)$ всюду заменим c на свежую переменную a. Полученная последовательность будет выводом в T, поскольку аксиомы T не содержат c.

Отсюда следует, что при добавлении в сигнатуру новой константы новых теорем в старой сигнатуре не появляется: если φ не содержит константы c, то $T \vdash \varphi$ в $\Sigma \cup \{c\}$ влечёт $T \vdash \varphi$ и в Σ. Это свойство расширения называется *консервативностью*.

Следствие 12 Пусть T — непротиворечивая теория, в которой выводится формула $\exists x\, \varphi(x)$, и

$$T' \overset{def}{\leftrightharpoons} T \cup \{\varphi(c)\},$$

где c — свежая константа. Тогда T' также непротиворечива.

Доказательство. От противного: пусть T' противоречиво, то есть на самом деле из T выводится отрицание $\varphi(c)$: существует конечный поднабор посылок $\gamma \subseteq T$, что $T \vdash \bigwedge \gamma \to \neg\varphi(c)$. Но формулы из γ не содержат c. Следовательно по лемме 27 $T \vdash \gamma \to \neg\varphi(x)$, где x — свежая переменная, не входящая в φ. Согласно закону контрапозиции, отсюда получаем $T \vdash \varphi \to \neg \bigwedge \gamma$, а правило Бернайса дает $T \vdash \exists x\, \varphi(x) \to \neg \bigwedge \gamma$. Но, согласно условию, $\exists x\, \varphi(x)$ выводилось из T, то есть $T \vdash \neg \bigwedge \gamma$, и T противоречиво. Противоречие.

Естественно, это рассуждение можно обобщить на любое число констант.

Утверждение 28 [4] Пусть T — непротиворечивая теория, и

$$T' \stackrel{def}{\leftrightharpoons} T \cup \{\varphi_\alpha(c_\alpha) \mid \alpha \in I\},$$

где множество I индексирует все формулы вида $\exists v_\alpha\, \varphi_\alpha(v_\alpha)$, выводимые в T, а $\Sigma' = \Sigma \cup \{c_\alpha \mid \alpha \in I\}$ — расширение сигнатуры Σ попарно различными константами. Тогда T' — непротиворечива.

Доказательство. В самом деле, если бы T' была противоречива, то вывод противоречия использовал бы конечное число новых аксиом, и достаточно для каждой из них повторить рассуждения, доказывающие предыдущее следствие.

Заметим, что лемма 26 обеспечивает расширение, которое полно, но ничего не говорит о свойстве Хенкина. Напротив, лемма 28 приближает нас к свойству Хенкина (но не гарантирует его: про формулы вида $\exists x\, \varphi(x)$, содержащие вновь добавленные константы, нам ничего не известно), но никак не гарантирует полноты. Скомбинируем оба расчсуждения.

Утверждение 29 [5, основная] Всякая непротиворечивая теория T в сигнатуре Σ имеет непротиворечивое расширение S в языке Σ', обогащённом константами, обладающее одновременно полнотой и свойством Хенкина.

Доказательство. Счётное число раз поочерёдно применим описанные процедуры пополнения и добавления констант. В пределе получим объединение, обладающее обоими свойствами одновременно. В самом деле: непротиворечивость следует из компактности (вывод противоречия использует конечное число новых аксиом и поэтому появляется на конечном шаге). Из конечности длины формулы следует, что в ней лишь конечное число новых констант, поэтому на конечном шаге очередное пополнение добавит либо её, либо её отрицание в теорию. Наконец, свойство Хенкина также следует из конечности формулы: когда все новые константы нашей формулы появятся в сигнатуре, следующее добавление констант обеспечит искомую c.

Доказательство теоремы Гёделя. Пусть T — непротиворечивая теория.Расширим её до надтеории P в языке Σ', обладающей одновременно и непротиворечивостью, и полнотой, и свойством Хенкина (Лемма 29). Но тогда, по лемме 25, у теории P существует модель, являющаяся моделью и для подтеории T. Теорема Гёделя доказана.

Теорема 26 [Гёделя, о полноте, стандартная формулировка] $T \models \varphi \Rightarrow T \vdash \varphi$, то есть если для любой модели $\mathcal{M}$ из $\mathcal{M} \models T$ следует $\mathcal{M} \models \varphi$, то $T \vdash \varphi$.

Доказательство. В самом деле: пусть, напротив, $T \nvdash \varphi$. Тогда теория $T \cup \{\neg\varphi\}$ непротиворечива. Но тогда найдется модель $\mathcal{M}$, такая что $\mathcal{M} \models T$ и $\mathcal{M} \models \neg\varphi$, что означает $T \not\models \varphi$.

В частности, в пустой теории (т.е. в исчислении предикатов) имеем ожидаемое $\models \varphi \Rightarrow \vdash \varphi$.

Выпишем теперь классические следствия теоремы Гёделя.

Теорема 27 [Гёделя-Мальцева, о компактности] T имеет модель тогда и только тогда, когда её любая конечная подтеория T_0 имеет модель.

Доказательство. Очевидно: по теореме Геделя T имеет модель в том и только том случае, когда T непротиворечива. Непротиворечивость T равносильна непротиворечивости всех ее конечных подтеорий (т.к. вывод использует конечное число аксиом), и непротиворечивость всех конечных подтеорий в силу теоремы Геделя расносильна тому, что каждая из них имеет модель.

Упражнение 12 Рассмотрим модель $\omega = (\mathbb{N}; +; \cdot; 0; =)$ и ее теорию $Th(\omega) = \{A \in L_{arith} \mid \omega \models A\}$. Назовём *нестандартной моделью арифметики* модель $M \ncong \omega$ $M \models Th(\omega)$.

Докажем, что нестандартные модели арифметики существуют.

Рассмотрим язык $L_{arith}(c)$, где c — константа. Рассмотрим теорию

$$T \overset{def}{\leftrightharpoons} Th(\mathbb{N}) \cup \{c \neq 0,\, c \neq 1, \ldots\}.$$

Тогда, если $\mathcal{M} \models T$ и $c_{\mathcal{M}}$ — интерпретация c в $\mathcal{M}$, то $c \notin \{0, 1, 2, \ldots\}$, и следовательно $\mathcal{M}$ — нестандартная модель арифметики. Осталось доказать, что такая модель существует. По теореме 27, для выполнимости T достаточно показать выполнимость каждой конечной подтеории $T_0 \subset T$. Подтеория T_0 содержит лишь конечное число формул вида $c \neq n_1, \ldots, c \neq n_k$. Ее модель — это $(\mathbb{N}; c \overset{def}{\leftrightharpoons} m)$, где, например, $m > \max\{n_1 \ldots n_k\}$).

Теорема 28 [Лёвенгейма-Скулема, слабый вариант] Любая непротиворечивая теория первого порядка в счётном языке имеет счётную модель.

Доказательство. Наблюдение за мощностью модели в доказательстве теоремы Гёделя.

Конец лекции № 13

Начало лекции № 14 12 февраля 2015 г.19 февраля 2015 г.

Теории с равенством

Часто мы рассматриваем языки с двуместным предикатным символом “равенства” $=$; вообще говоря, никаких обременений на значение этого предиката нет, но мы выделяем модели, в которых ему назначено естественное значение.

Определение 39 *Нормальная модель* — это модель $\mathcal{M}$ сигнатуры с равенством $=$, где $=_{\mathcal{M}}$ интерпретируется как совпадение элементов модели, $\{< x, x >| \, x \in \mathcal{M}\}$.

Такое обременение, естественно, нагружает нормальную теорию дополнительными аксиомами.

Аксиома 1.9 (Равенства для сигнатуры Σ) *1. $=$ есть отношение эквивалентности:*

$\forall x \, (x = x)$, $\forall x, y, x \, (x = y \wedge y = z \to x = z)$, $\forall x, y \, (x = y \to y = x)$.

2. Для каждого $f \in \Sigma$,

$\forall \vec{x} \ \forall \vec{y} \ \ (x_1 = y_1 \wedge \ldots \wedge x_n = y_n \ \to \ f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n))$.

3. Для каждого $P \in \Sigma$,

$\forall \vec{x} \ \forall \vec{y} \ \ (x_1 = y_1 \wedge \ldots \wedge x_n = y_n \ \to \ (P(x_1, \ldots, x_n) \leftrightarrow P(y_1, \ldots, y_n)))$.

Определение 40 *Теория с равенством* — это теория, содержащая все аксиомы равенства для символа $=$ в своей сигнатуре Σ.

Теорема 29 [О полноте и корректности]

1. Пусть $\mathcal{M}$ — нормальная модель. Тогда $Th(M) = \{A \mid \mathcal{M} \models A\}$ — (непротиворечивая) теория с равенством.

2. Пусть T — непротиворечивая теория с равенством. Тогда найдется нормальная модель $\mathcal{M}$, такая что $\mathcal{M} \models T$.

Доказательство.

1. Очевидно.

2. По теореме о полноте, найдется модель $\mathcal{M}_0$, такая что $\mathcal{M}_0 \models T$. На $\mathcal{M}_0$ определим отношение эквивалентности:

$$x \sim y \ \overset{def}{\leftrightharpoons} \ \mathcal{M}_0 \models x = y.$$

Положим $\mathcal{M}$ — факторструктура $\mathcal{M}_0$ по отношению $\sim$, т.е. $\mathcal{M} \overset{def}{\leftrightharpoons} \mathcal{M}_0/\sim$. Это нормальная модель. Положим для функциональных символов $f_{\mathcal{M}}([x_1], \ldots, [x_n]) \overset{def}{\leftrightharpoons} [f_{\mathcal{M}_0}(x_1, \ldots, x_n)]$, и для предикатных символов $P_{\mathcal{M}}([x_1], \ldots, [x_n]) \overset{def}{\leftrightharpoons} [P_{\mathcal{M}_0}(x_1, \ldots, x_n)]$. Осталось рутинно (индукцией по построению формулы) проверить, что для любых формулы A и $\vec{x} \in \mathcal{M}_0$ выполняется $\mathcal{M}_0 \models A(\vec{x}) \ \Leftrightarrow \ \mathcal{M} \models A([x_1], \ldots, [x_n])$.

Замечание 9 Можно записать аксиомы компактнее:

T — теория с равенством, если и только если в ней выводится аксиома 1 и для всех $\vec{x}, \vec{y}$, $T \vdash (x_1 = y_1 \wedge \ldots \wedge x_n = y_n \ \to \ (A(x_1, \ldots, x_n) \ \leftrightarrow \ A(y_1, \ldots, y_n)))$.

Начиная с этого места, мы временно ограничимся в рассмотрении исключительно теориями с равенством. Аксиомы равенства мы всегда будем молчаливо подразумевать, не выписывая.

Теоремы Лёвенгейма-Скулема

Напомним:

Определение 41 *Теория данной модели* $\mathcal{M}$*:* $Th(\mathcal{M}) \stackrel{def}{\leftrightharpoons} \{A \mid \mathcal{M} \models A\}$.

Элементарно эквивалентные модели $\mathcal{M}_1$ *и* $\mathcal{M}_2$*:* $\mathcal{M}_1 \equiv \mathcal{M}_2 \stackrel{def}{\leftrightharpoons} Th(\mathcal{M}_1) = Th(\mathcal{M}_2)$.

Элементарная подмодель: $\mathcal{M}_1 \prec \mathcal{M}_2 \stackrel{def}{\leftrightharpoons} \mathcal{M}_1 \subset \mathcal{M}_2$, и для любой $A(\vec{x})$, $\forall\ \vec{a} \in \mathcal{M}_1$ $(\mathcal{M}_1 \models A[\vec{a}] \Leftrightarrow \mathcal{M}_2 \models A[\vec{a}])$. В частности, элементарная подмодель элементарно эквивалентна исходной модели.

Упражнение 13 Натуральный ряд является элементарной подмоделью любой нестандартной модели арифметики: $\mathbb{N} \prec \mathcal{M} : \forall n \in \mathbb{N}\, (\mathbb{N} \models A[n] \Leftrightarrow \mathcal{M} \models A[n])$.

Теорема 30 Любая бесконечная модель $\mathcal{M}$ имеет собственное элементарное расширение $\mathcal{M}'$, т.е. $\mathcal{M} \prec \mathcal{M}'$.

Доказательство. Добавим к языку ещё одну константу c и запишем следующую теорию $Th(\mathcal{M}, \{c_\alpha \mid \alpha \in \mathcal{M}\}) \cup C$, где $C \stackrel{def}{\leftrightharpoons} \{c \neq c_\alpha \mid a \in \mathcal{M}\}$. Тогда любая конечная подтеория, а, значит, и вся теория, имеет модель. Эта модель будет собственным элементарным расширением $\mathcal{M}$.

Теорема 31 [Лёвенгейма-Скулема-Мальцева, о повышении мощности] Любая бесконечная модель $\mathcal{M}$ имеет элементарные расширения любой мощности δ, большей мощности $|\mathcal{M}|$.

Доказательство. Заведём константы $\{c_\alpha \mid \alpha \in \mathcal{M}\}$ для всех элементов исходной модели; введём дополнительно новые константы $\{d_\beta \mid \beta \in I\}$, чтобы получить желаемую мощность. Рассмотрим теорию T, полученную из $Th(\mathcal{M})$ добавлением серии аксиом, постулирующих попарное различие всех новых констант. Далее используем теорему о компактности: всякая конечная подтеория T имеет модель (можно доопределить в $\mathcal{M}$ значения новых констант, т.к. в подтеорию их входит конечное число), следовательно, T также имеет модель, причем нормальную. Все новые константы имеют в этой модели различные значения, следовательно, мощность этой модели не меньше δ.

Теорема 32 [Лёвенгейма-Скулема, о понижении мощности] Любая модель $\mathcal{M}$ имеет элементарно эквивалентную подмодель $\mathcal{N} \prec \mathcal{M}$ такую, что $|\mathcal{N}| \leqslant \max(\aleph_0, |\Sigma|)$.

Доказательство. Будем, начав с произвольной счетной подмодели $\mathcal{N}_0 \subset \mathcal{M}$, строить последовательность элементарных расширений внутри $\mathcal{M}$: $\mathcal{N}_0 \subset \mathcal{N}_1 \subset \mathcal{N}_2 \subset \ldots$ Для каждого $k = 0,\ 1,\ \ldots$ определим $\mathcal{N}_{k+1}$ следующим образом: для каждой формулы $A[v, \vec{u}]$ и произвольных $\vec{y} \in \mathcal{N}_k$, в случае если $\mathcal{M} \models \exists x\, A[x, \vec{y}]$; выбираем a из $\mathcal{M}$, такое что $\mathcal{M} \models\ A[a, \vec{y}]$, и добавим к $\mathcal{N}_k$. Положим

$$\mathcal{N} \overset{def}{=\!=} \bigcup_{k<\omega} \mathcal{N}_k.$$

Покажем, что построенная подмодель — искомая.

Утверждение 30 Для любой формулы A и любых $\vec{x} \in \mathcal{N}$ имеем ($\mathcal{M} \models \exists y\, A(y, \vec{x}) \Leftrightarrow \exists y \in \mathcal{N}\ \mathcal{M} \models A(y, \vec{x})$).

Доказательство. $\Leftarrow$ очевидно. Для доказательства $\Rightarrow$ заметим, что $\vec{x} \in \mathcal{N}_k$ для некоторого k, следовательно если $\mathcal{M} \models \exists y\, A(y, \vec{x})$, то по определению $\mathcal{N}_{k+1}$ найдется $y \in \mathcal{N}_{k+1}$, такой что $\mathcal{M} \models A(y, \vec{x})$.

Утверждение 31 $\mathcal{N}$ есть подмодель $\mathcal{M}$.

Доказательство. Если $x_1, \ldots, x_n \in \mathcal{N}$, то для некоторого k имеем $x_1, \ldots, x_n \in \mathcal{N}_k$. Тогда $f(x_1, \ldots, x_n) \in \mathcal{N}_{k+1} \subset \mathcal{N}$, поскольку для $x_1, \ldots, x_n \in \mathcal{N}_k$ можно рассмотреть формулу $\exists y\ y = f(x_1, \ldots, x_n)$. Эта формула истинна в $\mathcal{M}$, следовательно $\exists y \in \mathcal{N}_{k+1}$, такой что $\mathcal{M} \models y = f(\vec{x})$.

Утверждение 32 Для всякой формулы $A[\vec{x}]$ и элементов $\vec{x} \in \mathcal{N}$ имеем

$$\mathcal{N} \models A[\vec{x}] \ \Leftrightarrow\ \mathcal{M} \models A[\vec{x}].$$

Доказательство. Для атомарных формул утверждение следует из того, что $\mathcal{N}$ — подмодель $\mathcal{M}$ (см. предыдущую лемму). Случай логических связок очевиден. Если $A = \exists y B[\vec{x}, y]$, воспользуемся леммой 30.

Конец лекции № 14

Начало лекции № 15 19 февраля 2015 г.5 марта 2015 г.

Элиминация кванторов. Разрешимость

> Once one has eliminated the impossible, whatever remains, however improbable, must also be eliminated.
>
> Justin Richards

Пусть Σ — сигнатура, A — её структура. Иногда удаётся доказать факт следующего вида: "если φ — формула сигнатуры Σ, то существует бескванторная формула φ' (этой же сигнатуры), такая что $A \models \varphi \leftrightarrow \varphi'$". Тогда такую алгебраическую структуру называют *допускающей элиминацию кванторов.* Рассмотрим примеры подобных структур и докажем для них это свойство.

Упражнение 14 Рассмотрим структуру $(\mathbb{Z}, =, 0, S)$. Здесь S — функция следования, т.е., прибавление единицы. В этой структуре можно выразить крайне мало: $SSS\ldots S(u) = SSS\ldots S(v)$, где u, v — 0 или переменная. Докажем, что любая формула φ эквивалентна формуле такого вида. Приведём φ к предварённой нормальной форме $Q_1x_1Q_2x_2\ldots Q_nx_n\ \varphi')$, где Q_i — кванторы, формула φ' — бескванторная. Используя представление $\forall x\ \varphi' \Leftrightarrow \neg\exists x\ \neg\varphi'$, можем считать, что все кванторы — существования, и вести индукцию по кванторной глубине формулы.

Утверждение 33 $\exists x\varphi'$ в $(\mathbb{Z}, =, 0, S)$ эквивалентна некоторой бескванторной формуле.

Доказательство. Вынося ненужное за квантор и приводя к ДНФ, будем считать, что формула φ имеет следующий вид:

$$\exists x\ \tau(x, x_1\ldots x_n)$$
$$\text{где } \tau \text{ имеет вид } t_1 = t_2 \wedge t_3 = t_4 \wedge \ldots \wedge \neg t_n = t_{n+1}),$$

и каждое из равенств содержит x хотя бы с одной стороны. Далее, если какое-то равенство термов содержит x с обеих сторон, $SS\ldots S(x) = SSS\ldots S(x)$, то оно либо тождественно ложно, либо тождественно истинно. В зависимости от этого и от того, входит ли это равенство в конъюнкцию под отрицанием или нет, этот множитель можно исключить из конъюнкции, либо вся конъюнкция ложна. Аналогично, если равенство (отрицание равенства) термов не содержит x с обеих сторон и не содержит других переменных, то это просто равенство двух натуральных чисел, которое также либо истинно, либо ложно.

Итак, мы можем считать, что в каждом равенстве x присутствует с одной стороны, но не с другой. Если все равенства в τ входят с отрицанием, то $\exists x\tau$ истинна в нашей структуре независимо от значений остальных входящих в нее переменных. Пусть τ содержит без отрицания хотя бы одно равенство, $\ldots S(x) = SSS\ldots S(v)$, где v — другая переменная или 0, то есть $x = s$ где s_i — либо число, либо выражение $u + c$, где u — переменная (для простоты мы разрешим прибавлять целые константы вместо натуральных; это не меняет класса выводимых формул, зато оставляет слева одинокий x). Рассмотрим формулу $\varphi' = \tau[x/s]$, полученную из τ подстановкой s вместо всех вхождений x. Очевидно, φ и φ' эквивалентны в нашей структуре. $\varphi' \vee \varphi''$ — бескванторная формула, эквивалентная исходной.

Упражнение 15 Теория $(\mathbb{Q}, <, =)$, или $\mathbb{R}$. Выберем произвольную формулу φ, вынесем наружу кванторы и устраняем их по одному изнутри. Вновь мы можем считать, что последний из кванторов — существования, и нужно разобраться только с утверждением: $\exists x\, \varphi'$, где φ' — бескванторная формула. Атомарные формулы имеют вид: $u < v$ или $u = v$. Приведем φ' к ДНФ, удалим отрицания атомарных формул путём замены $\neg(u < v)$ на $(u = v \vee v < u)$, и $\neg(u = v)$ на $(u < v \vee v < u)$. Снова приведем полученную формулу к ДНФ (она уже не будет содержать отрицаний атомарных формул) и пронесем квантор существования через дизъюнкцию. Нам остается элиминировать квантор существования в формуле вида $\exists x\, (u_1 < v_1 \wedge u_2 < v_2 \wedge \ldots \wedge u_n < v_n \wedge u_{n+1} = v_{n+1} \ldots)$. Равенства вида $u = s$ можно вычеркнуть из конъюнкции, при наличии неравенства вида $u < u$ вся конъюнкция ложна. Если присутствует равенство вида $x = v$, то подставим везде v вместо x и уберем квантор существования по x. Если такого равенства нет, то равенств нет вообще (т.к. равенства, не содержащие x, можно вынести из-под квантора. Если в оставшихся неравенствах x всегда справа (или слева), то такой x всегда существует, и формула тождественно истинна. Иначе выражение $\exists x\, (u_1 < x \wedge \ldots \wedge u_n < x \wedge x < v_1 \wedge \ldots \wedge x < v_m)$эквивалентна (в силу плотности порядка) формула $\bigwedge\limits_{i,j} u_i < v_j$, а это бескванторная формула.

Заметим, что в обоих случаях мы установили факт элиминируемости кванторов конструктивно, а поскольку любая замкнутая формула без кванторов либо истинна, либо ложна, то мы одновременно построили алгоритм проверки истинности произвольной замкнутой формулы в теории: “записать эквивалентную бескванторную, в которой будут только константы, подставить их и вычислить, истинно это или ложно.” Такое свойство теорий называется *разрешимостью.*

Более изощрённым является следующий результат о разрешимости.

Теорема 33 [Тарского-Зайденберга[10]] Пусть $A = (\mathbb{R}, =, <, 0, 1, +, \cdot)$. Тогда всякая формула φ равносильна в A некоторой бескванторной формулой.

Доказательство. Общая схема доказательства аналогична предыдущим примерам: приведем формулу к предварённой форме, и устраняем кванторы по одному; достаточно рассмотреть квантор существования. Итак, рассматриваем формулу вида $\exists x\, \varphi$, где φ — бескванторная формула. Приведем φ к дизъюнктивной нормальной форме, избавимся в ней от отрицаний атомарных формул аналогично предыдущему примеру, снова приведем к дизъюнктивной форме и квантор существования распределим через дизъюнкцию. После этого под квантором стоит конъюнкция выражений вида

[10]Тарский, Альфред (1901 – 1983) — польско-американский математик, логик. Создатель аксиоматизации евклидовой геометрии и разработчик метода элиминации кванторов. Зайденберг, Абрахам (1916 – 1988) — американский математик.

$t_1 = t_2$ и $t_1 < t_2$, где $t_1, t_2 \in \mathbb{N}[x, x_1 \dots x_n]$, т.е. являются многочленами многих переменных с натуральными коэффициентами. Перенося всё для простоты налево и вычитая, получаем вид: $t = 0$, $t < 0$ или $t > 0$, где уже $t \in \mathbb{Z}[x, x_1 \dots x_n]$.

Докажем основную лемму.

Утверждение 34 Рассмотрим формулу вида $\exists x\ \varphi'$, где φ' — конъюнкция формул вида $t = 0$, $t < 0$, $t > 0$, где $t \in \mathbb{Z}[x, x_1 \dots x_n]$. Тогда она эквивалентна некоторой бесквантворной формуле ψ от переменных $x_1 \dots x_n$.

Доказательство. Запишем каждый многочлен t в виде многочлена из $\mathbb{Z}[x_1 \dots x_n][x]$, т.е. многочлена переменной x, коэффициенты которого — многочлены переменных $x_1, \dots, x_n$. Пусть формула имеет вид $\exists x\,(t_1(x) = 0 \wedge t_2(x) = 0 \wedge \dots \wedge t_m(x) < 0)$. Если бы коэффициенты всех многочленов были числами, то мы могли бы записать следующую таблицу всех корней многочленов и их знаков: $2k+1$ её столбцов (k — общее количество всех корней всех многочленов семейства, за вычетом повторяющихся) соответствуют этим корням и промежуткам между ними, включая бесконечные лучи слева и справа, m строк соответствуют самим многочленам, а их знаки в этих точках и на промежутках обозначены в клетках таблицы знаками $+, -0$. Важно, что числовые значения корней в заголовках столбцов не записаны: описывается лишь "топологическое" взаиморасположение графиков. Истинность формулы означает наличие в таблице столбца определенного вида.

Такие таблицы будем называть *диаграммами многочленов*. Мы докажем, что при нескоторых правилах расширения диаграмм диаграмма для многочленов степени 0 однозначно восстановит её для исходного набора.

Приведем список правил, по которым можно добавлять в таблицу многочлены (если получаются уже имеющиеся, повторять не надо):

1. добавить старший член любого из многочленов первой и более степени;
2. добавить производную любого многочлена по x;
3. добавить многочлен, полученный из некоторого многочлена в таблице отбросыванием старшего члена (по x);
4. добавить модифицированный остаток от деления P на Q, где P и Q — многочлены из диаграммы и $a = deg(P)$ больше чем $b = deg(Q)$; модифицированный остаток от деления P на Q получается, если разделить на Q многочлен P, домноженный на старший член Q в степени $a - b + 1$. В этом случае результат деления будет иметь в качестве коэффициентов многочлены от $x_1, \dots, x_n$ с целыми коэффициентами.

Расширяем таблицу исходную таблицу описанными выше способами; за конечное число шагов, добавляя многочлены степени, не превосходящей исходных, мы дойдём до набора многочленов, замкнутого относительно предложенных операций. Обозначим этот набор через F. Через F_0 обозначим все находящиеся в нём многочлены степени 0 по x. Наша цель очевидна: пусть дана диаграмма только для F_0 (исключительно распределение знаков и нулей, константа во всю длину строки). Докажем, что тогда всю таблицу (при данных $x_1, \ldots, x_n$) можно заполнить снизу вверх.

Будем добавлять назад многочлены по одному, упорядочив по возрастанию степеней. Пусть мы "возвращаем" многочлен $P(x, x_1 \ldots x_n)$, причём все многочлены меньших степеней уже добавлены. Старший коэффициент этого многочлена a у нас уже записан (даже есть в F_0); его знак в диаграмме указан.

Если в диаграмме указано, что что $a = 0$. Но тогда многочлен P при данных значениях $x_1, \ldots, x_n$ совпал с многочленом меньшей степени, добавленным по правилу 3. Найдем этот многочлен и продублируем его строчку в строке для P.

Пусть теперь в диаграмме указано, что $a > 0$. Сначала восстановить, какие знаки имеет наш многочлен в уже имеющихся в диаграмме точках (не на промежутках). Выберем какую-то точку a из диаграммы. Она имеется в диаграмме, поскольку некоторый многочлен Q (расположенный ниже в таблице, и следовательно уже возвращенный) уже обращается в 0 при $x = a$. Для определённости считаем, что старший коэффициент Q ненулевой; более того, этот коэффициент c уже есть в F_0, и его знак указан в диаграмме для F_0. Далее, в списке есть и появившийся по пункту 4 модифицированный остаток от деления P на Q, и он записан ниже, чем P, то есть уже разобран по предположению индукции. Но поскольку Q в этой точке нулевой, то $c^k P = 0 + R$, и мы, зная знак для P и знак c, легко вычисляем знак для P.

Пусть теперь знаки во всех имеющихся корнях уже вписаны. Пусть в двух подряд корнях стоит один знак; тогда, раз между ними не появилось корня у производной многочлена P (производная находится ниже в таблице, следовательно, уже возвращена в диаграмму, и столбцы для ее корней уже добавлены), то в нуль P на этом интервале дополнительно не обращается. Если же в двух подряд точках P имеет разный знак, то корень P между ними есть (по теореме Больцано-Коши), и ровно один из тех же соображений. Тогда добавляем между этими корнями новый столбик и вписываем туда нуль в строке для многочлена P. Осталось понять, что происходит перед первым корнем и после последнего. Из соображений наличия корней производной многочлена P, если знак P в крайней точке справа и знак старшего коэффициента P совпадают, то новых корней нет; иначе он один. С левого конца аналогично, но с учётом ещё и степени P.

Берём многочлены нашей формулы, доводим его до замкнутого множества, выписываем все возможные диаграммы для F_0, каждую из них восстанавливаем до диа-

граммы для F и, если распределение знаков и нулей совпало с требуемым в формуле, дописываем этот вариант в дизъюнкцию. Получается формула от $x_1, \ldots, x_n$, не содержащая переменной x и равносильная исходной.

Конец лекции № 15

Начало лекции № 16 5 марта 2015 г.12 марта 2015 г.

Вещественные поля. 17 проблема Гильберта.

Определение 42 *Упорядоченное поле* — это пара $(F, <)$, где F — поле, $<$ — линейный порядок на его элементах, такой, что $x < y$ влечёт $x + z < y + z$, а $x, y > 0 \to x \cdot y > 0$.

В частности, поля $\mathbb{Q}$ и $\mathbb{R}$ упорядочены, а задать такой порядок на $\mathbb{C}$ невозможно. Установим необходимые и достаточные условия, при которых поле можно упорядочить.

Утверждение 35 В упорядоченном поле:

1. $\forall x \neq 0\ (x^2 > 0)$.
2. $1 > 0$.
3. Упорядоченное поле всегда имеет характеристику 0.
4. $-1 \neq {a_1}^2 + \ldots + {a_n}^2$.

Доказательство. Первый пункт: если $x > 0$, то $x \cdot x > 0$. Если же $x < 0$, то $-x > 0$, и опять же $x \cdot x = (-x)(-x) > 0$. Второй следует из первого, так как $1 = 1^2 > 0$. Поскольку $1 > 0$, имеем $1 + 1 > 0 + 1 = 1 > 0$, и по индукции $\underbrace{1 + \ldots + 1}_{n} > 0$ для всякого натурального n, что даёт нам характеристику 0. Если $a > 0$, то $-a < 0$; в частности, $-1 < 0$, а сумма квадратов — больше.

Определение 43 Назовём поле $\mathcal{F}$ *вещественным* (согласно Артину[11]), если $\forall n \forall a_1 \ldots a_n \in \mathcal{F}\ (-1 \neq {a_1}^2 + \ldots + {a_n}^2)$.

Мы убедились, что вещественными являются все упорядоченные поля. Но оказывается, что и обратное верно: на любом формально вещественном поле можно задать линейный порядок, согласованный со структурой поля.

Конец лекции № 16

Начало лекции № 17 12 марта 2015 г.19 марта 2015 г.

[11] Артин, Эмиль (1898 – 1962) — австрийский алгебраист, создатель теории вещественных полей. Автор решения 17 проблемы Гильберта.

Теорема 34 Если $\mathcal{F}$ — вещественное поле, то $\mathcal{F}$ можно упорядочить, то есть задать отношение линейного порядка $<$ над $\mathcal{F}$ такое, что $x < y \to x + z < y + z$, и $x > 0 \wedge y > 0 \to x \cdot y > 0$; более того, для любого a такого, что $-a \notin \Sigma\mathcal{F}^2$, можно сделать это так, что $a > 0$.

Доказательство.

Докажем серию лемм о свойствах таких полей и их алгебраических расширений.

Утверждение 36 [1] Пусть $\mathcal{F}$ — вещественное поле, $a \in \mathcal{F}$, $a \neq 0$. Тогда невозможно, чтобы одновременно выполнялось

$$\begin{cases} a \in \Sigma\mathcal{F}^2, \\ -a \in \Sigma\mathcal{F}^2. \end{cases}$$

Доказательство. Если a и b — суммы квадратов, то $\frac{a}{b} = \frac{a}{b^2} \cdot b$ является суммой квадратов. Следовательно, если бы a и $-a$ являлись суммами квадратов одновременно, то их частное $\frac{a}{-a} = -1 \in \Sigma\mathcal{F}^2$, и поле $\mathcal{F}$ не вещественно.

Утверждение 37 [2] Если $\mathcal{F}$ — вещественно, $-a \notin \Sigma\mathcal{F}^2$, то $\mathcal{F}(\sqrt{a})$ — вещественно.

Доказательство. Достаточно рассмотреть существенный случай, когда $\sqrt{a} \notin \mathcal{F}$. Согласно определению, $\mathcal{F}(\sqrt{a}) = \{u + v\sqrt{a} \mid u, v \in \mathcal{F}\}$. От противного: пусть $\mathcal{F}(\sqrt{a})$ не вещественно. Тогда существуют такие $b_i, c_i \in \mathcal{F}$, что

$$-1 = \sum (b_i + c_i\sqrt{a})^2 = \sum (b_i^2 + 2b_i c_i\sqrt{a} + c_i^2 a).$$

Однако $-1 = -1 \cdot 1 + 0 \cdot \sqrt{a}$, поэтому слагаемые с корнем зануляются, и в действительности

$$-1 = \sum b_i^2 + a \sum c_i^2.$$

Отсюда выражается

$$-a = \frac{1 + \sum b_i^2}{\sum c_i^2} = \frac{(\sum b_i^2) \cdot (\sum c_i^2) + (\sum c_i^2)}{(\sum c_i^2)^2},$$

откуда $-a$ выражается в виде суммы квадратов. Противоречие.

Следствие 13 Если $\mathcal{F}$ — вещественно, то либо $\mathcal{F}(\sqrt{a})$, либо $\mathcal{F}(\sqrt{a})$ — вещественно.

Утверждение 38 [3] Пусть $\mathcal{F}$ — вещественно замкнуто, то есть никакое его алгебраическое расширение не является более вещественным. Положим $a \geq 0 \overset{\text{def}}{\iff} a \in \mathcal{F}^2$; $x \geq y \overset{\text{def}}{\iff} x - y \geq 0$. Тогда $(\mathcal{F}, \leq)$ — упорядоченное поле.

Доказательство. Антисимметричность порядка вытекает из леммы 1. Транзитивность: если $x \geq y \geq z$, то $x - y = a^2, y - z = b^2$. Тогда $x - z = a^2 + b^2 \in \Sigma\mathcal{F}^2$. По лемме 2, мы можем взять из неё корень, и $\mathcal{F}(\sqrt{a^2+b^2})$ — тоже вещественно. Но у поля $\mathcal{F}$ нет собственных вещественных алгебраических расширений! Значит, $\sqrt{a^2+b^2} \in \mathcal{F}$, что влечёт $a^2 + b^2 \in \mathcal{F}^2$, то есть $x - z \in \mathcal{F}^2$, и $x \geq z$. Линейность: для любого $a \in \mathcal{F}$, либо $a \in \mathcal{F}^2$, либо $-a \in \mathcal{F}^2$: в самом деле, если бы они оба не принадлежали $\mathcal{F}^2$, то среди двух полей $\mathcal{F}(\sqrt{a})$ и $\mathcal{F}(\sqrt{-a})$ есть собственное вещественное расширение. Согласованность со структурой: если $x < y$, то $(x + z) - (y + z) \in \mathcal{F}^2$, откуда $y + z > x + z$.

Утверждение 39 [4] Если $\mathcal{F}$ — вещественное поле, то существует $\mathcal{F}' \supseteq \mathcal{F}$, и $\mathcal{F}'$ — вещественно замкнуто.

Доказательство. Рассмотрим все вещественные поля, содержащие $\mathcal{F}$, фактор которых по $\mathcal{F}$ — алгебраический, с отношением включения. Любая цепь имеет верхнюю грань: это объединение всех её элементов. По лемме Цорна, существует максимальный элемент $\mathcal{F}'$. Он будет алгебраически замкнутым, иначе нарушилась бы максимальность. Значит, он — искомый.

Пусть $\mathcal{F}$ — вещественное поле, $-a \notin \Sigma\mathcal{F}^2$. Применим лемму 37: $\mathcal{F}(\sqrt{a})$ — тоже вещественно. По лемме 39, существует $\mathcal{F}' \supseteq \mathcal{F}(\sqrt{a})$, и $\mathcal{F}'$ — уже вещественно замкнуто. Теперь, применяя лемму 38, строим на $\mathcal{F}'$ такой порядок, что $a > 0$. Рассмотрим сужение $<|_{\mathcal{F}}$ — это искомое упорядочение.

Теорема 35 [17 проблема Гильберта] Пусть f — рациональная функция над $\mathcal{F}$ — вещественно замкнутым, $\forall\ \vec{a}\ f(\vec{a}) \geq 0$. Тогда существуют $f_1 \dots f_n$ — такие рациональные функции над $\mathcal{F}$, что $f = \sum\limits_{i=1}^{n} f_i^2$.

Доказательство. Пусть f не является суммой квадратов. Тогда у поля рациональных функций $\mathcal{F}(X)$ существует упорядочение, причём f можно сделать при нём отрицательным. Вещественно замкнём поле $\mathcal{F}(X)$ до $\mathcal{R}$, сохраняя порядок. Тогда $\mathcal{R} \models \exists\vec{v}\,(f(\vec{v}) < 0)$, поскольку $f < 0$ в $\mathcal{R}$. Но тогда и $\mathcal{F} \models \exists\vec{v}\,(f(\vec{v}) < 0)$, что противоречит неотрицательности f. 17 проблема Гильберта полностью решена.

Для более глубокого знакомства с вещественными полями рекомендуем обратиться к изданию [?] или к "Алгебре" С. Ленга.

Категоричные теории

Определение 44 Пусть α — бесконечный кардинал, T — теория первого порядка в сигнатуре Σ. Пусть T имеет модель мощности α. Будем говорить, что T — *α-категорична* (или *категорична в мощности* α), если $\forall\mathcal{M}_1, \mathcal{M}_2\ (\mathcal{M}_1 \models T \wedge \mathcal{M}_2 \models T \wedge |\mathcal{M}_1| = |\mathcal{M}_2| = \alpha \rightarrow \mathcal{M}_1 \sim \mathcal{M}_2)$.

Упражнение 16

- Теория равенства $T_=$ (с $\Sigma = \{=\}$) категорична в каждой мощности.

- Пусть теория описывает отношение эквивалентности, разделяющее все элементы на два класса, причём они бесконечны. Она категорична в счётной мощности, но ни в какой большей.

- Теория DLO плотного линейного порядка без первого и последнего элементов: симметричность, транзитивность, линейность, плотность, отсутствие наименьшего и наибольшего элементов. Общеизвестный факт гласит:

  Утверждение 40 DLO категорична в счётной мощности (но ни в какой большей).

- Обратно, пусть $\Sigma = \{0, +\}$ — язык аддитивных групп. Будем говорить, что G — абелева группа с делением без кручения, если $\forall y \exists x\ (x + \ldots + x = y)$, но $\forall x\ (x \neq 0 \to x + \ldots + x \neq 0)$ для любого числа n слагаемых в записи. Пусть T — теория таких абелевых групп. Тогда $\mathcal{T}$ не категорична в счётной мощности, а во всех остальных — категорична.

  В самом деле, условимся об очевидном обозначении $n \cdot a$, где $n \in \mathbb{N}$. Тогда $forall n\ G \models \forall a \exists! b (nb = a)$. Существование частного — это аксиома. Единственность: если $a = nb = nb'$, то $0 = n(b - b')$, что противоречит отсутствию кручения. В силу этого введём обозначения: $b = \frac{1}{n} \cdot a$. Аналогично, обретает смысл запись $\frac{m}{n} a$, то есть наша группа есть векторное пространство над $\mathbb{Q}$. Но векторные пространства имеют очень простой изоморфизм: по размерности. Тогда счётная группа может иметь любую конечную или счётную размерность, что даёт некатегоричность, а вот у более чем счётного векторного пространства размерность совпадает с мощностью, и с точностью до изоморфизма оно единственно.

- (без доказательства) Пусть ACF_p — теория алгебраически замкнутых полей характеристики p. Тогда эта теория категорична для каждого несчётного кардинала. При этом каждая из этих теорий имеет даже конечную модель ($\mathbb{Z}_p$).

- Доказанный нами факт о существовании нестандартной модели арифметики доказывает счётную некатегоричность арифметики Пеано. Истинностная арифметика (множество всех замкнутых формул, верных в стандартной модели) — аналогично.

Теорема 36 [Воота/Vaught] Пусть теория $\mathcal{T}$ в сигнатуре Σ имеет какую-то модель, но не имеет конечных моделей; пусть, кроме того, $\mathcal{T}$ — α-категорична для некоторого

$\alpha \geq |\Sigma|$. Тогда $\mathcal{T}$ — полна, то есть $\forall \varphi \in St$ выполнено либо (Σ) $\mathcal{T} \models \varphi$, либо $\mathcal{T} \models \neg\varphi$[12].

Доказательство. От противного: предположим, что $\mathcal{T}$ неполна. Зафиксируем формулу φ, невыводимую вместе с отрицанием. Тогда обе теории, получаемые из $\mathcal{T}$ добавлениями φ и $\neg\varphi$ непротиворечивы: у них существуют модели, и их без ограничения мощности можно выбрать мощности α. Тогда они — модели $\mathcal{T}$, которые заведомо неизоморфны. Противоречие.

Условие отсутствия конечных моделей существенно: рассмотрим теорию групп, в которых каждый элемент имеет порядок 2. У неё есть конечная (группа из двух элементов) и бесконечные. Запишем формулу $\exists x, y, z\,(x \neq y \wedge y \neq z \wedge x \neq z)$. Тогда ни её, ни её отрицание нельзя вывести из теории.

Конец лекции № 17

Начало лекции № 18 19 марта 2015 г.9 апреля 2015 г.

[12]Значит, и теории из примеров 4 и 5 — полны. Обратное неверно: рассмотрите истинностную арифметику или пример 3.

Теоремы Геделя о неполноте

Вычислимые функции, разрешимые и перечислимые множества

Определение 45 $f\colon \mathbb{N}^k \to \mathbb{N}^s$ *вычислима,* если существует машина Тьюринга, на любом входе $\langle n_1, \ldots, n_k \rangle$ вычисляющая $m = f(n_1 \ldots n_k)$. Функция f может быть частичной, если $\mathrm{Dom}(f) \subsetneq \mathbb{N}^k$; тогда на остальных входах машина Тьюринга зацикливается.

Определение 46 Подмножество $P \subseteq \mathbb{N}^k$ *перечислимо,* если существует вычислимая функция f, что область её определения равна P.

Можно доказать, что это эквивалентно существованию такой вычислимой f, чтобы P стало её областью значений, и даже такой тотальной (то есть всюду заданной) вычислимой f с фиксированной областью значений (но в последнем случае нужно специально оговориться, что ещё бывает $P = \emptyset$, не являющееся областью значений никакой тотальной функции).

Связь определений обеспечивает замечательная *теорема о графике:* Функция f вычислима $\Leftrightarrow$ график $f = \{< x, y >|\ f(x) = y\}$ перечислим.

Определение 47 Множество P *разрешимо,* если вычислима его характеристическая функция, то есть есть алгоритм, способный проверить произвольный вход[13] на принадлежность P. Простейшая *теорема Поста* гласит, что P разрешима, если и только если P и $\mathbb{N}^k \setminus P$ одновременно перечислимы.

Оказывается, что разрешимые множества — это Δ_1, а перечислимые совпадают с Σ_1 (это мотивация для обозначения множеств из Π_1 как *коперечислимых*). Чтобы быть готовыми к доказательству нашей теоремы, введём одно понятие, следуя Гёделю.

Примитивно рекурсивные функции

Определение 48 *Примитивно рекурсивные функции* $f\colon \mathbb{N}^k \to \mathbb{N}$ определяется по индукции. Начальные функции: $z(x) \equiv 0$, $S(x) = x + 1$, $I^n_k(x_1 \ldots x_n) = x_k$. Операции для построения новых:

- Композиция: если $f, g_1 \ldots g_k$ — примитивно рекурсивные, то $h(\vec{x}) \overset{def}{\leftrightharpoons} f(g_1(\vec{x}) \ldots g_n(\vec{x}))$ такова.
- Примитивная рекурсия: если g, h — примитивно рекурсивные, то строим по следующим правилам.

$$\begin{cases} f(0, \vec{x}) & = & g(\vec{x}), \\ f(n+1, \vec{x}) & = & h(f(n, \vec{x}), n, \vec{x}). \end{cases}$$

[13] Из $\mathbb{N}^k$.

Приведём примеры примитивно рекурсивных функций, которые понадобятся нам в дальнейшем.

Упражнение 17 1. $f(x,y) = x + y$. В самом деле,

$$\begin{cases} f(0,y) & = & y, \\ f(x+1,y) & = & S(f(x,y)). \end{cases}$$

2. $f(x,y) = x \cdot y$. Действительно,

$$\begin{cases} x \cdot 0 & = & 0 \\ x \cdot (y+1) & = & x \cdot y + x. \end{cases}$$

Почему мы можем вести рекурсию по любому аргументу функции? Дело вот в чём: если f — п. р., то $g(x,y) = f(y,x)$ тоже, ибо $g(x,y) = f(I_2^2(x,y), I_1^2(x,y))$

3.

$$pd(x) = \begin{cases} x-1 & \text{если} \quad x > 0, \\ 0 & \text{если} \quad x = 0. \end{cases} \quad \text{Действительно,} \quad \begin{cases} pd(0) & = & 0, \\ pd(x+1) & = & I_2^3(pd(x), x, x). \end{cases}$$

4. Функция “предыдущее число”

$$sgn(x) = \begin{cases} 1 & \text{если} \quad x > 0, \\ 0 & \text{если} \quad x = 0. \end{cases} \quad \text{Действительно,} \quad \begin{cases} sg(0) & = & 0, \\ sg(x+1) & = & I_2^3(pd(x), x, x). \end{cases}$$

5. $x - y$ определяется схемой

$$\begin{cases} x - 0 = x \\ x - (y+1) = pd(x-y) \end{cases}$$

6. $$\begin{array}{lcl} \min(x,y) & = & y \cdot sg(x-y) + x \cdot sg(y-x), \\ \max(x,y) & = & x \cdot sg(x-y) + y \cdot sg(y-x), \end{array}$$

7. $$case(x,y,z) = \begin{cases} x, & \text{если} \quad z = 0 \\ y, & \text{если} \quad z > 0 \end{cases} = x \cdot (1 - sg(z)) + y \cdot sg(z).$$

Конец лекции № 18

Начало лекции № 19 9 апреля 2015 г.16 апреля 2015 г.

Остаток $rm(x,y)$ и частное $qt(x,y)$ от деления x на y — примитивно-рекурсивные функции:

$$\begin{cases} rm(0,y) & = & 0 \\ rm(x+1,y) & = & S(rm(x,y)) \cdot sg(|y - S(rm(x,y))|) \end{cases}$$

$$\begin{cases} qt(0,y) & = & 0 \\ qt(x+1,y) & = & qt(x,y) + (1 - sg(\|y - S(rm(x,y))\|)) \end{cases}$$

Пусть $f(\vec{x},y)$ — данная функция. Будем рассматривать функции $\sum\limits_{y<z(y\leq z)} f(\vec{x},y)$ и $\prod y < z(y \leq z) f(\vec{x},y)$.

Утверждение 41 Если функция $f(\vec{x},y)$ примитивно-рекурсивна, то и функции $\sum\limits_{y<z(y\leq z)} f(\vec{x},y)$ и $\prod y < z(y \leq z) f(\vec{x},y)$ примитивно-рекурсивны.

Доказательство. Положим:

$$\begin{cases} h_f(\vec{x},0) & = & 0 \\ h_f(\vec{x},y+1) & = & h_f(\vec{x},y) + f(\vec{x},y) \end{cases}$$

Определение 49 Скажем, что отношение $R \subseteq \mathbb{N}^k$ примитивно-рекурсивно, если примитивно-рекурсивна его характеристическая функция

$$\chi_R(\vec{x}) = \begin{cases} 0, & \text{если } R(\vec{x}) \\ 1, & \text{иначе} \end{cases}$$

Упражнение 18 Следующие отношение примитивно-рекурсивны: $=, <, \leq$, "x делится на y", "x простое".

Определение 50 Пусть $R \subseteq \mathbb{N}^{k+1}$. *Ограниченные кванторы* задают следующие отношения:

$\exists u < v\ R(\vec{x},u)$; $\forall u < v\ R(\vec{x},u)$.

Утверждение 42 Если R примитивно рекурсивно, то $\exists u < y\ R$, $\forall u < y\ R$ также примитивно-рекурсивны.

Доказательство. В самом деле:

$\chi_{\exists u<y\ R}(\vec{x},u) = \prod\limits_{u<y} \chi_R(\vec{x},u)$,

$\chi_{\forall u<y\ R}(\vec{x},u) = sg \sum\limits_{u<y} \chi_R(\vec{x},u)$.

Определение 51 *Ограниченный μ-оператор:*

$$f(\vec{x},z) = \mu y < z . R(\vec{x},y) = \begin{cases} \text{наименьшее } y \text{ такое, что } y < z \text{ и } R(\vec{x},y), \text{если он существует,} \\ z, \text{ иначе.} \end{cases}$$

Утверждение 43 Если R примитивно рекурсивно, то $\mu\ y < z.\ R(\vec{x},y)$ примитивно рекурсивно.

Доказательство. Действительно: $\mu\ y < z.\ R(\vec{x},y) = 1 + \sum\limits_{y<z} \prod\limits_{u\leq y} (1 - \chi_R(\vec{x},u)$.

Упражнение 19 Обозначим через p_x простое число с номером x (по возрастанию). Это примитивно-рекурсивная функция от x. Действительно:

$$p_0 = 2, \qquad p_{x+1} = \mu\, y < (p_x)! + 1.\ (Prime(y) \wedge p_x < y).$$

Опишем кодирование последовательностей натуральных чисел натуральными числами, при котором естественные операции над последовательностями окажутся примитивно рекурсивными. А именно, последовательность $a_0, \ldots, a_n$ будем кодировать числом $p_0^{a_0} \cdot p_1^{a_1+1} \cdot \ldots \cdot p_n^{a_n+1}$. Обозначим код последовательности $a_0, \ldots, a_n$ через $\lceil a_0, \ldots, a_n \rceil$.

Утверждение 44 Следующие функции примитивно-рекурсивны:

1. $f(x, i) = (x)_i$ — показатель степени при p_i в разложении x на простые множители
2. $lh(x)$ — число различных простых делителей x
3. приписывание последовательностей

   $\lceil a_0, \ldots, a_n \rceil * \lceil b_0, \ldots, b_m \rceil = \lceil a_0, \ldots, a_n, b_0, \ldots, b_m \rceil$
4. предикат $seq(x)$ "x — код последовательности"

Доказательство. Предъявим выражение для этих функций через известные нам примитивно-рекурсивные функции.

- $(x)_i = \mu\, y < x.\ (p_i^y \mid x \wedge \neg(p_i^{y+1} \mid x))$;
- $lh(x) = \sum\limits_{y \le x} \chi_R(x, y)$, где $R = \{\langle x, y\rangle \mid Prime(y) \wedge (y \mid x) \wedge x \neq 0\}$;
- $x * y = x \cdot \prod j < lh(y)(P_{lh(x)+j})^{(y)_j}$.
- $seq(x) = \forall i < lh(x)(p_i \mid x)$

Утверждение 45 Пусть для $i, j = 1, \ldots, n$ функции g_i и отношения $\cup R_i = \mathbb{N}^k$ примитивно-рекурсивны, причем $R_i \cap R_j = 0\ (i \neq j)$ и $\bigcup_i R_i = \mathbb{N}^k$. Тогда примитивно-рекурсивна следующая функция разбора случаев:

$$f(\vec{x}) = \begin{cases} g_1(\vec{x}), & \text{если} \quad R_1(\vec{x}), \\ g_2(\vec{x}), & \text{если} \quad R_2(\vec{x}), \\ \ldots & \\ g_n(\vec{x}), & \text{если} \quad R_n(\vec{x}). \end{cases}$$

Доказательство. $f(\vec{x}) = g_1(\vec{x}) \cdot \chi_{R_1}(\vec{x}) + \ldots + g_n(\vec{x}) \cdot \chi_{R_n}(\vec{x})$.

Определение 52 Совместная рекурсия: пусть g_1, g_2, h_1, h_2 — примитивно рекурсивные функции. Для $i = 1, 2$ положим $f_i(\vec{x}, 0) = g_i(\vec{x})$,

$f_i(\vec{x}, y+1) = h_i(\vec{x}, y, f_1(\vec{x}, y), f_2(\vec{x}, y))$. Тогда f_i примитивно-рекурсивны.

Доказательство. Определим рекурсией функцию

$$g(\vec{x}, y) = \lceil f_1(\vec{x}, 0), f_2(\vec{x}, 0) \rceil$$

следующим образом:

$$\begin{array}{rcl} g(\vec{x}, 0) & = & \lceil g_1(\vec{x}), g_2(\vec{x}) \rceil \\ g(\vec{x}, y+1) & = & \lceil h_1(\vec{x}, y, (g(\vec{x}, y))_1, (g(\vec{x}, y))_2), h_2(\vec{x}, y, (g(\vec{x}, y))_1, (g(\vec{x}, y))_2) \rceil \end{array}$$

После этого заметим, что

$$f_i(\vec{x}, y) = (g(\vec{x}, y))_i.$$

Следующая формула задает (примитивно-рекурсивную) нумерацию пар чисел:

$pair(x, y) = sg(x - y)(x^2 + 2y + 1) + sg(y - x)(y^2 + 2x)$.

Порядок будет таким: $(0,0); (0,1), (1,0), (1,1); (0,2), (2,0), (1,2), (2,1), (2,2); \ldots$

Обратные к ней функции левого и правого члена пары также примитивно-рекурсивны: действительно, $left(0) = right(0) = 0$, а также

$$left(n+1) = \begin{cases} right(n), & \text{если} \quad left(n) < right(n), \\ right(n) + 1, & \text{если} \quad left(n) > right(n), \\ 0, & \text{если} \quad left(n) = right(n) \end{cases}$$

$$right(n+1) = \begin{cases} left(n), & \text{если} \quad left(n) \neq right(n), \\ left(n) + 1, & \text{если} \quad left(n) = right(n). \end{cases}$$

Пользуемся леммами о разборе случаев и двойной рекурсии.

Определение 53 *Возвратная рекурсия:* $f_\sharp(\vec{x}, y) = \prod u < y (p_u)^{f(\vec{x}, u)}$.

(При этом $f(\vec{x}, y) = (f_\sharp(\vec{x}, y+1))_{y+1}$.)

Утверждение 46 Если h примитивно рекурсивна, то $f(\vec{x}, y) \overset{def}{\leftrightarrows} h(\vec{x}, y, f_\sharp(\vec{x}, y))$ — тоже.

Доказательство. Функции f и $f_\sharp$ нужно определять совместной рекурсией:

$$\begin{array}{rcl} f(\vec{x}, 0) & = & h(\vec{x}, 0, 1) \\ f_\sharp(\vec{x}, 0) & = & 1 \\ f(\vec{x}, y+1) & = & h(\vec{x}, y, f_\sharp(\vec{x}, y)) \\ f_\sharp(\vec{x}, y+1) & = & f_\sharp(\vec{x}, y) * f(\vec{x}, y) \end{array}$$

Идея возвратной рекурсии — задавать значение функции в точке, исходя не только из одного предыдущего, но и из всех предшествовавших значений. Например, таковы последовательность Фибоначчи ($a_0 = 1$, $a_1 = 1$, $a_n = a_{n-1} + a_{n-2} (n \geq 2)$) и большинство синтаксических определений. Например, для определения терма

1. $Tm(t) = 1$, если $Var(t) \vee Const(t)$;

2. Если $t = f(t_1, \ldots, t_n) \wedge Fn(f^n) \wedge \forall i \in 1 \ldots n\ (Tm(t_i) = 1)$, то $Tm(t) = 1$;

3. $Tm(t) = 0$, иначе.

Рекурсивные функции

Определение 54 *Рекурсивные функции* получаются при замыкании класса примитивно-рекурсивных фукнций относительно (неограниченного) μ–оператора:

$$f(\vec{x}) = \mu y.(g(\vec{x}, y) = 0)$$

Мы считаем, что $f(\vec{x}) = y$, если $g(\vec{x}, y) = 0$ и для каждого $z < y$ значение $g(\vec{x}, y)$ определено и $g(\vec{x}, y) \neq 0$, и $f(\vec{x})$ не определена иначе.

Следующая функция рекурсивна, но не примитивно-рекурсивна.

Упражнение 20 *Функция Аккермана:*

$$\begin{cases} Ack(0, x) & = & x + 2, \\ Ack(n + 1, 0) & = & Ack(n, 0), \\ Ack(n + 1, m + 1) & = & Ack(n, Ack(n + 1, m)) \end{cases}$$

Тогда $Ack(1, 0) = 2,\ Ack(1, m + 1) = Ack(1, m) + 2,\ Ack(2, 0) = 2,\ Ack(2, m + 1) = 2(Ack(2, m)) + 2$, что влечёт $Ack(2, m) \geq 2^m$. Можно доказать, что k-тая ветвь функции Аккермана растёт быстрее любой примитивно рекурсивной функции, в которой не более k вложенных рекурсий (теорема несложна, но вычислительно неприятна). В частности, диагонализированная $Ack(n, n)$ является не-примитивно рекурсивной функцией одной переменной.

1.4 Рекурсивные функции (в широком смысле)

Теорема 37 [Клини, об униформизации] Существуют такие примитивно рекурсивная функция U и примитивно рекурсивный предикат T, что для любой (частичной) вычислимой функции $f(\vec{x})$ можно подобрать число $e \in \mathbb{N}$, что $\forall\ \vec{x}\ \ f(\vec{a}) \equiv U(\mu y.\, T(e, \vec{x}, y))$.

Теорема 38 Функция рекурсивна тогда и только тогда, когда она вычислима по Тьюрингу.

Доказательство.

Конец лекции № 19

Начало лекции № 20 16 апреля 2015 г.23 апреля 2015 г.

Формальная арифметика. Арифметическая иерархия. Σ_1–определимость.

Рассмотрим арифметику $PA(+,\cdot,0,S,=,\leq)$, где $x \leq y \leftrightarrow \exists z\, x+z=y$. Будем изучать, какте именно подмножества натурального ряда являются определимыми. Далее, введём обозначения:

$\forall x \leq t\, \varphi(x) \overset{\text{def}}{\Longleftrightarrow} \forall x\, (x \leq t \to \varphi(x))$,

$\exists x \leq t\, \varphi(x) \overset{\text{def}}{\Longleftrightarrow} \exists x\, (x \leq t\, \wedge\, \varphi(x))$,

где x не входит в t.

Определение 55 *Ограниченные формулы* (класс Δ_0) — это формулы, все вхождения кванторов в которые ограничены.

Утверждение 47 Если $\varphi(\vec{x}) \in \Delta_0$, то существует алгоритм, который по значениям параметров формулы $\vec{n}$ проверяет $\mathbb{N} \models \varphi(\vec{n})$.

Доказательство. При фиксированных значениях параметров можно вычислить значения термов, входящих в формулу, после этого ограниченные кванторы можно заменить конечными конъюнкциями и дизъюнкциями.

Определение 56 *Классы* Σ_n *и* Π_n. $\Sigma_0 = \Pi_0 = \Delta_0$.

$\Sigma_{n+1} \overset{\text{def}}{\Longleftrightarrow} \{\exists x\, \varphi(\vec{x}, \vec{y}) \mid \varphi \in \Pi_n\}$,

$\Pi_{n+1} \overset{\text{def}}{\Longleftrightarrow} \{\forall x\, \varphi(\vec{x}, \vec{y}) \mid \varphi \in \Sigma_n\}$

Определим классификацию арифметических предикатов (т.е. предикатов, выразимых в стандартной модели арифметики): скажем, что предикат $P \subseteq \mathbb{N}^k$ лежит в $\Sigma_n(\Pi_n)$, если P определим $\Sigma_n(\Pi_n)$-формулой. Далее, предикат P принадлежит классу Δ_n, если он одновременно принадлежит Σ_n и Π_n.

Утверждение 48

- Классы Σ_n и Π_n–отношений замкнуты относительно ограниченных кванторов.
- Класс Σ_n замкнут относительно квантора существования, а Π_n относительно квантора всеобщности.
- Классы Σ_n и Π_n замкнуты относительно объединения, пересечения и дополнения.

Доказательство. 1. Основываемся на следующих эквиалентностях:

$$\begin{aligned}
\exists x < a \exists y \varphi &\sim \exists y \exists x < a \varphi \\
\forall x < a \exists y \varphi(a,x,y) &\sim \exists z \forall x < a \exists u < z (\varphi(a,x,y/u) \wedge u = (z)_x) \\
\forall x < a \forall y \varphi &\sim \forall y \forall x < a \varphi \\
\exists x < a \forall y \varphi &\sim \forall y \forall x < a \varphi
\end{aligned}$$

2. Для доказательства используем следующие эквивалентности:

$$\begin{aligned}\forall x\forall y\varphi(x,y) &\sim \forall z\exists x<z\exists y<z(x=left(z)\wedge y=right(z)\wedge\varphi(x,y))\\ \exists x\exists y\varphi(x,y) &\sim \exists z\exists x<z\exists y<z(x=left(z)\wedge y=right(z)\wedge\varphi(x,y))\end{aligned}$$

3. Для доказательства выносим кванторы через конъюнкцию и дизъюнкцию.

Утверждение 49 Любая арифметическая формула эквивалентна некоторой Σ_n-формуле.

Доказательство. По теореме о предварённой нормальной форме. Затем, по предыдущей лемме, блоки одноименных кванторов можно заменить одним квантором. Вообще говоря, ни представление, ни n не единственны (но среди подходящих n можно выделить минимальный).

Основная теорема этого раздела:

Теорема 39 [Об эквивалентности Σ_1-определимости и перечислимости] Предикат $P\subseteq\mathbb{N}^k$ является Σ_1-определимым в том и только в том случае, когда P перечислим.

Доказательство. Перечислимость Σ_1 предикатов следует из того, что класс примитивно-рекурсивных отношений замкнут относительно булевых связок и ограниченных кванторов.

Докажем обратное. Для этого достаточно показать, что график любой рекурсивной функции Σ_1-определим. Доказательство индукцией по рекурсивной схеме: для каждой рекурсивной функции $f(x_1,\ldots,x_n)$ найдется Σ_1 формула $F(x_1,\ldots,x_n,y)$, такая что для любых натуральных $k_1,\ldots,k_n.m$

$$f(k_1,\ldots,k_n)=m \iff \omega\models F(k_1,\ldots,k_n,m).$$

Построим сначала формулы для базовых функций.

- $Z(x)=0$; $F(x,y)\overset{def}{\leftrightharpoons} x=x\wedge y=0$;
- $S(x)=x+1$; $F(x,y)\overset{def}{\leftrightharpoons} y=S(x)$;
- $I^k_n(x_1,\ldots,x_n)=x_k$; $F^k_n(x_1,\ldots,x_n,y)\overset{def}{\leftrightharpoons}(\bigwedge_{i=1}^n(x_i=x_i))\wedge y=x_k$.

Пусть теперь функция f получена композицией из функций $h(y_1,\ldots,y_k)$ и $g_i(x_1,\ldots,x_n)$, то есть $f(x_1,\ldots,x_n)=h(g_1(x_1,\ldots,x_n),\ldots,g_k(x_1,\ldots,x_n))$. По предположению индукции, графики функций h и g_i определяются Σ_1-формулами $H(y_1,\ldots,y_k,y)$ и $G_i(x_1,\ldots,x_n,z_i)$ Положим

$$F(x_1,\ldots,x_n,y)\overset{def}{\leftrightharpoons}\exists z_1\ldots\exists z_k\ \left(H(z_1,\ldots,z_k,y)\wedge\left(\bigwedge_{i=1}^k G_i(x_1,\ldots,x_n,z_i)\right)\right)$$

Очевидно, что эта формула определяет график функции f и она Σ_1, поскольку класс Σ_1-формул замкнут относительно кванторов существования и булевых операций.

Пусть теперь f получена из функции g с помощью μ-оператора, то есть $f(x_1,\ldots,x_n) = \mu y.(g(x_1,\ldots,x_n,y)=0)$, причем функция g — всюду определенная. По предположению индукции найдется Σ_1-формула $G(x_1,\ldots,x_n,y,z)$, определяющая график функции g. Положим

$$F(x_1,\ldots,x_n,y) \overset{def}{\rightleftharpoons} G(x_1,\ldots,x_n,y,0) \wedge \forall z < y \neg G(x_1,\ldots,x_n,z,0).$$

Очевидно, что эта формула определяет график функции f, и она задает Σ_1-отношение, поскольку класс Σ_1-отношений замкнут относительно булевых связок и ограниченных кванторов.

Пусть, наконец, функция f будет получена из g и h рекурсией, то есть

$$\begin{cases} f(x_1,\ldots,x_n,0) &= g(x_1,\ldots,x_n) \\ f(x_1,\ldots,x_n,y+1) &= h(x_1,\ldots,x_n,y,f(x_1,\ldots,x_n,y)) \end{cases}$$

Согласно предположению индукции, графики функций g и h определяются формулами $G(x_1,\ldots,x_n,u)$ и $H(x_1,\ldots,x_n,y,z,v)$. Тогда, в полуформальной записи, формула $F(x_1,\ldots,x_n,y,w)$ должна означать следующее:

$$\begin{aligned} \exists s \,(\quad & \mathrm{length}(s) = y+1 \wedge G(x_1,\ldots,x_n,(s)_0) \wedge (s)_y = w \wedge \\ & \wedge \forall i < y H(x_1,\ldots,x_n,i,(s)_i,(s)_{i+1})) \end{aligned}$$

Кодирование синтаксиса

Опишем кодирование синтаксиса языка первого порядка натуральными числами. Цель — сделать это таким образом, чтобы естественные предикаты “быть кодом терма”, “быть кодом формулы”, “быть кодом аксиомы”, и наконец, “x — код вывода формулы с кодом y” были примитивно-рекурсивными. Каждому слову φ будем сопоставлять его геделев номер — число $\ulcorner\varphi\urcorner$.

Конец лекции № 20

Начало лекции № 21 23 апреля 2015 г.30 апреля 2015 г.

Пусть Σ — не более чем счётная сигнатура, содержащая функциональные символы $\{f_i^n\}$, предикатные символы $\{R_i^n\}$, переменные $v_0, v_1, \ldots$ Например, положим $=$ как R_0^2, 0 как f_0^0, S есть f_0^1 и так далее. Наша цель — приписать гёделевы номера объектам языка, чтобы разным объектам соответствовали разные натуральные числа, а смысл слова мог бы определяться примитивно-рекурсивным образом. Обозначив гёделев номер объекта A как $\ulcorner A\urcorner$, распределим номера, скажем, так:

$$
\begin{array}{ll}
\ulcorner v_i \urcorner & \overset{def}{\leftrightharpoons} \langle 1, i\rangle \\
\ulcorner f_i^n \urcorner & \overset{def}{\leftrightharpoons} \langle 2, \langle n, i\rangle\rangle \\
\ulcorner R_i^n \urcorner & \overset{def}{\leftrightharpoons} \langle 3, \langle n, i\rangle\rangle \\
\ulcorner \neg \urcorner & \overset{def}{\leftrightharpoons} \langle 4, 0\rangle \\
\ulcorner \to \urcorner & \overset{def}{\leftrightharpoons} \langle 4, 1\rangle \\
\ulcorner \forall \urcorner & \overset{def}{\leftrightharpoons} \langle 4, 2\rangle
\end{array}
$$

$\ulcorner s \urcorner > 4$ для любого символа s

В частности, $\ulcorner (A \to B) \urcorner = \langle \ulcorner \to \urcorner, \ulcorner A \urcorner, \ulcorner B \urcorner\rangle$, $\ulcorner \neg A \urcorner = \langle \ulcorner \neg \urcorner, \ulcorner A \urcorner\rangle$, $\ulcorner \forall v_i A \urcorner = \langle \ulcorner \forall \urcorner, \ulcorner v_i \urcorner, \ulcorner A \urcorner\rangle$. Довольно понятно, как разбирать выражение по его коду и понимать, чем оно является. Оказывается, это примитивно рекурсивные процедуры!

Упражнение 21 Например, рассмотрим характеристическую функцию $Tm(x)$ и выпишем явно функцию проверки "x есть гёделев номер терма":

1. Вернуть 1, если $\exists i \leq x\ x = \langle 1, i\rangle$
2. Вернуть 1, если $Seq(x) \wedge \exists n \leq x\ lh(x) = n + 1 \wedge \exists i \leq x\ (x)_0 = \langle 2, \langle n, i\rangle\rangle \wedge \forall j < n : Tm((x)_{j+1}) = 0$,
3. Вернуть 0, иначе.

То, что смысл верен, ясно: мы проверяем, что либо x — номер переменной, либо кодирует последовательность из функционального символа и термов. Эта функция примитивно–рекурсивна в силу лемм о возвратной рекурсии и разборе случаев.

Покажем, что отношение "x — код атомарной формулы " ($AtFm(x)$) также примитивно-рекурсивно: это бывает, если $Seq(x) \wedge \exists n, i \leq x((x)_0 = \langle 3, \langle n, i\rangle\rangle \wedge lh(x) = n + 1 \wedge \forall j < n\ Tm((x)_{j+1}) = 0)$.

Определение 57 *"x есть гёделев номер формулы": $Fm(x)$.*

1. Вернуть 1, если $AtFm(x) = 0$,
2. Вернуть 1, если $Seq(x) \wedge lh(x) = 2 \wedge (x)_0 = \ulcorner \neg \urcorner \wedge Fm((x)_1) = 0$,
3. Вернуть 1, если $Seq(x) \wedge lh(x) = 3 \wedge (x)_0 = \ulcorner \to \urcorner (x)_1, (x)_2 \in Fm$[14],
4. Вернуть 1, если $Seq(x) \wedge lh(x) = 3 \wedge (x)_0 = \ulcorner \forall \urcorner \wedge \exists i \leq x\ (x)_1 = \langle 1, i\rangle \wedge (x)_2 \in Fm$,
5. Вернуть 0, иначе.

[14]Договоримся писать вместо $Fm(x) \wedge Fm(y)$ символ "$x, y \in Fm$," и аналогичные.

Определение 58 *Нумерал* $\underline{n}$ натурального числа n — это терм вида $\underbrace{S(S\ldots S}_{n}(0))$ n раз. Положим $nm(x) \overset{def}{\leftrightharpoons} \ulcorner \underline{x} \urcorner$; она рекурсивно определяется как:

$$\begin{cases} nm(0) & = & \ulcorner 0 \urcorner, \\ nm(n+1) & = & \langle \ulcorner S \urcorner, nm(n) \rangle. \end{cases}$$

$Num(x) \overset{def}{\leftrightharpoons} \exists n \leq x\, x = nm(n)$.

Переходим к самому технически тонкому моменту всей конструкции.

Определение 59 *Подстановка:* $Sub(x, i, y)$ "результат подстановки в x выражения y вместо свободных вхождений переменной v_i". То есть, если $x = \ulcorner \varphi \urcorner$, то выполняется $Sub(\ulcorner \varphi \urcorner, i, \ulcorner t \urcorner) = \ulcorner \varphi[v_i/t] \urcorner$.

1. $Sub(\ulcorner v_i \urcorner, i, y) = y$,
2. $Sub(\ulcorner v_j \urcorner, i, y) = \ulcorner v_j \urcorner$, если $j \neq i$,
3. $Sub(\ulcorner f^n_j(t_1, \ldots, t_n) \urcorner, i, y) = \langle \ulcorner f^n_j \urcorner, Sub(\ulcorner t_1 \urcorner, i, y), \ldots, Sub(\ulcorner t_n \urcorner, i, y) \rangle$,
4. $Sub(\ulcorner R^n_j(t_1, \ldots, t_n) \urcorner, i, y) = \langle \ulcorner R^n_j \urcorner, Sub(\ulcorner t_1 \urcorner, i, y), \ldots, Sub(\ulcorner t_n \urcorner, i, y) \rangle$,
5. $Sub(\ulcorner \neg \varphi \urcorner, i, y) = \langle \ulcorner \neg \urcorner, Sub(\ulcorner \varphi \urcorner, i, y) \rangle$,
6. $Sub(\ulcorner \to \varphi \urcorner, i, y) = \langle \ulcorner \to \urcorner, Sub(\ulcorner \varphi \urcorner, i, y) \rangle$,
7. $Sub(\ulcorner \forall v_j \varphi \urcorner, i, y) = \begin{cases} \ulcorner \forall v_i \varphi \urcorner, & \text{если } i = j, \\ \langle \ulcorner \forall \urcorner, \ulcorner v_j \urcorner, Sub(\ulcorner \varphi \urcorner, i, y) \rangle, & \text{если } i \neq j, \end{cases}$
8. 0 (например), иначе.

Теперь мы научились проверять свободность вхождения: это неизменность при подстановке.

Определение 60 $Free(x, y) \overset{def}{\leftrightharpoons}$ "x есть гёделев номер переменной, имеющей свободное вхождение в выражение с номером y":

$\exists i \leq x\, (x = \ulcorner v_i \urcorner = \langle 1, i \rangle \wedge Sub(y, i, \ulcorner 0 \urcorner) \neq y)$.

$Tm(t) \wedge Free(x, t)$ "переменная x входит в t".

Упражнение 1.2 *Возвратной рекурсией по построению у выпишите аналогичным образом определение* $SubFm(x, y)$ *"x есть код подформулы формулы с кодом y".*

Определение 61 Следующее определение не полностью формально, т.к. мы отождествляем логические связки с примитивно рекурсивными функциями, вычисляющими их номера.

$Sbnt(t,i,\varphi)$ "t подстановочен в φ вместо свободного вхождения переменной v_i":

$Sbnt(t,i,\varphi) = 0 \leftrightarrow Tm(t) \wedge Var(v_i) \wedge Fm(\varphi) \wedge \{$ одно из нижеперечисленного:$\}$

1. $AtFm(\varphi)$;

2. $\exists \varphi_1, \varphi_2 < \varphi\ \varphi = (\varphi_1 \wedge \varphi_2) \wedge Sbnt(t,i,\varphi_1) = 0 \wedge Sbnt(t,i,\varphi_2) = 0$;

3. $\exists \varphi_1 < \varphi\ \varphi = (\neg\varphi_1) \wedge Sbnt(t,i,\varphi_1) = 0$;

4. $\exists \psi < \varphi\ \varphi = P(x,v_i) \wedge (j = i \vee (Sbnt(t,i,\psi) \wedge \neg(v_j \in Var(t) \wedge Free(v_i,\psi))))$.

$LogAx(x) = \bigvee\limits_{i=1}^{k} Ax_i(x)$,

где, например, $Ax_1(x) = \exists a,b \le x\ (a,b \in Fm \wedge x = \langle \ulcorner\rightarrow\urcorner, a, \langle \ulcorner\rightarrow\urcorner, b, a\rangle\rangle)$

...

$Ax_{10}(x) = \exists y \le x \exists i \le x\ x = \ulcorner\forall v_i \varphi \ \rightarrow\ \varphi[t/v_i]\urcorner$, где t подстановочно вместо v_i в $\varphi, \wedge Tm(t) \wedge Fm(y) \wedge x = \langle \ulcorner\rightarrow\urcorner, \langle \ulcorner\forall\urcorner, \ulcorner v_i \urcorner, y\rangle, Sub(y,i,t)\rangle$.

Имеет смысл также определить выведение через modus ponens:

$MP(x,y,z) \overset{def}{\leftrightarrows} (y = \langle \ulcorner\rightarrow\urcorner, x, z\rangle \wedge x,y,z \in Fm)$,

представимость формулы в виде квантора всеобщности от другой:

$Gen(x,i,y) \overset{def}{\leftrightarrows} (y = \langle \ulcorner\forall\urcorner, \ulcorner v_i \urcorner, x\rangle)$;

теперь мы можем установить *"y есть вывод x в логике предикатов":*

$Prf_{PC}(x,y) = Seq(y) \wedge \forall i < lh(y) : Fm((y)_i) \wedge \forall i < lh(y)\ (LogAx((y)_i) \vee \exists j,k < i\ MP((y)_j,(y)_k,(y)_i) \vee \exists p < y \exists j < i\ Gen((y)_j),p,(y)_i)$.

Конец лекции № 21

Начало лекции № 22 30 апреля 2015 г.14 мая 2015 г.

Подведём итоги, чего именно мы добились.

- Описали примитивно–рекурсивные функции.
- Описали кодирование натуральными числами синтаксиса арифметики.
- Доказали примитивную рекурсивность некоторых функций и предикатов, связанных с синтаксисом арифметики, в частности, предиката выводимости из гипотез $Prf_{PC}(y,x)$

Определение 62 Пусть T — теория в арифметическом языке. Отношение $P(\vec{x}) \subseteq \mathbb{N}^k$ *разрешимо* в T, если существует формула $\varphi(\vec{x})$, что $\forall\ \vec{n}$

$$\begin{aligned} P(\vec{n}) &\Rightarrow T \vdash \varphi(\underline{\vec{n}}) \\ \neg P(\vec{n}) &\Rightarrow T \vdash \neg\varphi(\underline{\vec{n}}). \end{aligned}$$

Определение 63 Функция $f(\vec{x})$ *представима* в T, если существует $\varphi(\vec{x}, y)$ такая, что:

$$f(\vec{n}) = m \Rightarrow T \vdash \varphi(\vec{\underline{n}}, \underline{m}) \text{ и}$$
$$T \vdash \forall y(\varphi(\vec{\underline{n}}, y) \rightarrow\ y = \underline{m}).$$

Но наиболее естественным и идейным (не техническим) является такое понятие:

Определение 64 Функция *доказуемо рекурсивна* в T, если $\exists\varphi(\vec{x}, y) \in \Sigma_1$:

$$f(\vec{n}) = m \Leftrightarrow \mathbb{N} \models \varphi(\vec{\underline{n}}, \underline{m}) \text{ и}$$
$$T \vdash \forall\ \vec{x}\ \ \exists! y\ \varphi(\vec{x}, y).$$

Теорема 40 1. Любая ПРФ Σ_1-определима в $\mathbb{N}$;

2. Любая ПРФ доказуема рекурсивно в PA (и даже в $I\Sigma_1$);

3. В конечно аксиоматизируемой *арифметике Робинсона* Q, являющейся PA без схемы индукции, но с добавленной аксиомой $\forall y(y \neq 0 \rightarrow \exists x\, y = S(x))$ разрешимы все ПР (и даже рекурсивные) отношения и представимы все ПРФ.

Для доказательства этих фактов нам понадобится другое яркое достижение Гёделя — иной вариант кодирования последовательностей.

Утверждение 50 Существует такая (тотальная) Σ_1-определимая функция $\beta(x, y, z)$, что

$$\forall\langle k_0 \dots k_n\rangle\ \exists a, b:\ \forall i \leq n\ \beta(a, b, i) = k_i.$$

Её легко указать: $\beta(x, y, z)$ — это остаток от деления $(z+1)\cdot y + 1$ на x. Её представляет следующая простая арифметическая формула:

$\beta(x, y, z) = u \overset{def}{\leftrightharpoons} \exists q\ ((z+1)\cdot y + 1 = qx + u \wedge u < x)$.

Поверим без доказательства: $I\Sigma_1 \vdash \forall x, y, z\ \exists! u\ \beta(x, y, z) = u$.

Положим $m = max(n, k_0 \dots k_n)$, $c = m!$ Выпишем последовательность $u_0 \dots u_n$, где $u_i \overset{def}{\leftrightharpoons} c(i+1) + 1$.

Утверждение 51 НОД$(u_i, u_j) = 1$, если $i \neq j$.

Доказательство. В самом деле: пусть $p \mid u_i, p \mid u_j$. Тогда $p \mid (u_i - u_j) = c(i-j)$. Не может быть, чтобы $p \mid c$, ибо в этом случае $p \mid u_i$ и $p \mid (u_i - 1)$, что невозможно; значит, $p \mid (i-j)$. Но $o < i - j \leq n \leq m$, откуда $(i-j) \mid m! = c$. Итак, опять $p \mid c$, и противоречие. Значит, эти числа взаимно просты.

Теперь в игру вступает

Теорема 41 [Китайская теорема об остатках] $\forall k_0 \dots k_n \exists b < u_0 \dots u_n$, что $\forall i \leq n\, b \equiv k_i \pmod{u_i}$.

$k_i < u_i$, поэтому k_i есть остаток от деления b на u_i, мы получаем $\beta(b,c,i) = rm(b,u_i) = k_i$.

Докажем первый пункт теоремы. ***Доказательство.***

1. $I_k^n, S, Z(x) \equiv 0$. $S(x) = y$ $x = x \wedge y = 0$ $I_k^n = y \leftrightarrow y = x_k$.

2. Композиция: $f(g(x)) = y$.

$g(x) = y, f(u) = v \quad \varphi(x,y), \psi(u,v) \in \Sigma_1 \quad \exists z(g(x) = z \wedge f(z) = y)$.

3. Примитивная рекурсия:

$$\begin{cases} f(0,a) & = & g(a), \\ f(n+1,a) & = & h(f(n,a),n,a) \end{cases}$$

$f(n,a) = y$ равносильно тому, что $\exists b,c\, \beta(b,c,0) = g(a) \wedge \forall i < n\, \beta(b,c,i+1) = h(\beta(b,c,i),i,a) \wedge \beta(b,c,n) = y$ что в свою очередь равносильно $\Leftrightarrow \exists b,c,u,v,w : \beta(b,c,0) = u = g(0) \wedge \forall i < n\, \beta(b,c,i) = v \wedge h(v,i,a) = w \wedge \beta(b,c,i+1) = w \wedge \beta(b,c,n) = y$.

Для приведения к Σ_1-виду осталось стереть неограниченные кванторы, сославшись на общий принцип (Σ_1-ограниченности): $\forall i < n \exists w\, \varphi(i,w) \leftrightarrow \exists z \forall i < n \exists w \leq z\, \varphi(i,w)$.

Конец лекции № 22

Начало лекции № 23 14 мая 2015 г.21 мая 2015 г.

Утверждение 52 1. Всякая Δ_0-формула разрешима в арифметике Робинсона Q;

2. Всякая вычислимая формула представима в Q;

3. Q Σ_1-полна.

Доказательство.

1. Индукцией по построению A. Рассмотрим сначала $t_1(\vec{x}) = t_2(\vec{x})$.

Индукцией по построению терма t докажем, что $t(\vec{m}) = n$ влечёт $\vdash_Q t(\underline{\vec{m}}) = \underline{n}$, а $t(\vec{m}) \neq n$ влечёт $\vdash_Q t(\underline{\vec{m}}) \neq \underline{n}$. Для этого индукцией по n достаточно доказать, что в PA выводятся формулы

$$\overline{m} + \overline{n} = \overline{m+n}, \qquad \overline{m} \cdot \overline{n} = \overline{m \cdot n}$$

Для булевых связок разрешимость в Q легко проносится через формулу: $\models A \wedge B \Rightarrow \models A \bigwedge \models B \Rightarrow \vdash_Q A \bigwedge \vdash_Q B \Rightarrow \vdash_Q A \wedge B$ и т. д.

Интерес представляет случай с квантором: $\not\models \forall x \leq tA(x) \Rightarrow n \leq t \bigwedge \not\models A(\underline{n}) \Rightarrow \vdash_Q \underline{n} \leq t, \vdash_Q \neg A(\underline{n}) \Rightarrow \vdash_Q \neg \forall x \leq tA(x)$. Обратно, пусть $\models \forall x \leq tA(x)$. Тогда $t = n$, $\models \forall x \leq nA(x) \Rightarrow A(0) \wedge \ldots \wedge A(\underline{n}) \Rightarrow A(0) \wedge \ldots \wedge A(\underline{n})$. Почему отсюда следует желанное $\forall x \leq \underline{n} A(x)$? Это происходит из того факта, что в Q выводится $\forall x (x \leq \underline{n} \leftrightarrow (x = 0 \vee \ldots \vee x = n))$. Индукцией по n : обоснуем, что $x \leq 0 \Leftrightarrow x = 0$, $x \leq S\underline{n} \Leftrightarrow x \leq \underline{n} \vee x = S\underline{n}$. Теперь

вспоминаем, что отношение «меньше или равно» мы задаём как $x \leq y \Leftrightarrow \exists z\, x + z = y$. Пусть $x + z = 0$; тогда либо $z = 0$ (и $x = 0$), либо $z = Su$ (и $x + z = S(x + u) \neq 0$) и т. д.

3. Это следует из пункта 1: пусть $A \in \Sigma_1$; $\models A \Rightarrow \vdash_Q A$. $\models \exists\ \vec{x}\ A(\vec{x})$ $(A \in \Delta_0)$; $\models (\vec{\underline{n}}) \Rightarrow \vdash_Q A(\vec{\underline{n}})$, $\vdash_{PC} A(\vec{\underline{n}}) \to \exists\ \vec{x}\ A(\vec{x})$.

Теоремы Геделя о неполноте

Теорема 42 Существует замкнутая формула φ (истинная в стандартной модели арифметики), такая что PA $\nvdash \varphi$

Для доказательства нам потребуется следующая важная лемма.

Утверждение 53 [О неподвижной точке] Пусть $\psi(x_i)$ — формула с единственной свободной переменной x_i. Найдется замкнутая арифметическая формула φ, такая что

$$\text{PA} \vdash \varphi \leftrightarrow \psi(\ulcorner \varphi \urcorner).$$

Доказательство. Рассмотрим формулу

$$\theta(x_i) \overset{def}{\leftrightharpoons} \psi(sub(x_i, i, x_i))$$

Пусть

$$n \overset{def}{\leftrightharpoons} \ulcorner \theta \urcorner.$$

Положим

$$\varphi \overset{def}{\leftrightharpoons} \theta(\overline{m}).$$

Тогда

$$\text{PA} \ \vdash \ \varphi \equiv \theta(\overline{m}) \equiv \psi(sub(\overline{m}, i, \overline{m}))$$

$$\text{PA} \ \vdash \ sub(\overline{m}, i, \overline{m}) = \ulcorner \theta(\overline{m}) \urcorner = \ulcorner \varphi \urcorner$$

Therefore

$$\text{PA} \ \vdash \ \varphi \equiv \psi(sub(\overline{m}, i, \overline{m})) \equiv \psi(\ulcorner \varphi \urcorner)$$

Доказательство. Докажем I теорему Геделя о неполноте. Рассмотрим формулу $\neg Prf(x, y)$, выражающую предикат "x является геделевым номером вывода формулы с неделевым номером y", положим $Pr(y) \overset{def}{\leftrightharpoons} \exists x Prf(x, y)$. Эта формула называется *формулой доказуемости для арифметики Пеано.* Согласно доказанному раньше, для всякой замкнутой формулы φ

$$\text{PA} \vdash \varphi \Leftrightarrow \text{PA} \vdash Pr(\ulcorner \varphi \urcorner).$$

По лемме о неподвижной точке, найдется замкнутая формула φ, такая что

$$\text{PA} \vdash \varphi \leftrightarrow \neg Pr(\lceil \varphi \rceil).$$

Тогда если $\text{PA} \vdash \varphi$, то по условию на неподвижную точку $\text{PA} \vdash \neg Pr(\lceil \varphi \rceil)$, следовательно в силу непротиворечивости арифметики $\text{PA} \nvdash Pr(\lceil \varphi \rceil)$, откуда $\text{PA} \nvdash \varphi$. Противоречие.

Пусть теперь $\text{PA} \vdash \neg\varphi$. Тогда по условию на неподвижную точку $\text{PA} \vdash Pr(\lceil \varphi \rceil)$, следовательно согласно свойству формулы доказуемости $\text{PA} \vdash \varphi$. Противоречие.

Формулой непротиворечивости для арифметики Пеано называется

$$Consis \overset{def}{\leftrightharpoons} \neg Pr(\lceil 0 = 1 \rceil)$$

Теорема 43 [II теорема Геделя о неполноте] $\text{PA} \nvdash Consis$.

Для доказательства этой теоремы нужно доказать, что предикат доказуемости удовлетворяет следующим условиям (Гильберт, Бернайс, Гедель, Леб).

Теорема 44 Для любых замкнутых формул φ и ψ выполняются следующие факты:

$$\begin{aligned} \text{PA} \vdash \varphi \quad &\Rightarrow \quad \text{PA} \vdash Pr(\lceil \varphi \rceil) \\ \text{PA} \quad &\vdash \quad Pr(\lceil \varphi \to \psi \rceil) \to Pr(\lceil \varphi \rceil) \to Pr(\lceil \psi \rceil) \\ \text{PA} \quad &\vdash \quad Pr(\lceil \varphi \rceil) \to Pr(\lceil Pr(\lceil \varphi \rceil) \rceil). \end{aligned}$$

Доказательство. Для того чтобы доказать второе утверждение, нужно в арифметике Пеано вывести следующую формулу (со свободными переменными x и y):

$$\text{PA} \vdash Prf(x, \lceil \varphi \to \psi \rceil) \to (Prf(y, \lceil \varphi \rceil) \to Prf(x * y * \lceil \psi \rceil, \lceil \psi \rceil)).$$

Третье утверждение - частный случай доказуемой Σ_1 полноты арифметики Пеано. А именно, для всякой замкнутой формулы $\sigma \in \Sigma_1$ верно следующее:

$$\text{PA} \vdash \sigma \to Pr(\lceil \sigma \rceil).$$

Доказательство. Докажем II теорему Геделя, используя условия Гильберта–Бернайса. Для этого мы докажем, что неподвижная точна из I теоремы Геделя о неполноте эквивалентна формуле непротиворечивости.

Итак, пусть $\text{PA} \vdash \varphi \leftrightarrow Pr(\lceil \varphi \rceil)$. Обозначим $\bot \overset{def}{\leftrightharpoons} 0 = 1$ и $\Box\psi \overset{def}{\leftrightharpoons} Pr(\lceil \psi \rceil)$. Тогда следующие формулы выводимы в арфметике:

1.	$\bot \to \varphi$	тавтология
2.	$\Box(\bot \to \varphi)$	из 1 и ГБ(1)
3.	$\Box(\bot \to \varphi) \to (\Box\bot \to \Box\varphi)$	ГБ(2)
4.	$\Box\bot \to \Box\varphi$	modus ponens, 2 и 3
5.	$\neg\Box\varphi \to \neg\Box\bot$	из 4
6.	$\varphi \to \neg\Box\varphi$	условие на неподвижную точку
7.	$\varphi \to \neg\Box\bot$	из 5 и 6

т.е. PA $\vdash \varphi \to \mathit{Consis}$.

С другой стороны,

1.	$\varphi \to \neg\Box\varphi$	условие на неподвижную точку
2.	$\Box(\varphi \to \neg\Box\varphi)$	из 1 и ГБ(1)
3.	$\Box(\varphi \to \neg\Box\varphi) \to (\Box\varphi \to \Box\neg\Box\varphi)$	ГБ(2)
4.	$\Box\varphi \to \Box\neg\Box\varphi$	modus ponens, 2, 3
5.	$\Box\varphi \to \Box\Box\varphi$	ГБ(3)
6.	$\Box\varphi \to \Box\neg\Box\varphi \wedge \Box\Box\varphi$	из 4 и 5
7.	$\Box\neg\Box\varphi \wedge \Box\Box\varphi \to \Box(\Box\varphi \wedge \neg\Box\varphi)$	из 6
8.	$\Box\varphi \wedge \neg\Box\varphi \to \bot$	тавтология
9.	$\Box(\Box\varphi \wedge \neg\Box\varphi) \to \Box\bot$	из 8, ГБ(1) и ГБ(2)
10.	$\Box\varphi \to \Box\bot$	из 7 и 9
11.	$\neg\Box\bot \to \neg\Box\varphi$	из 7 и 9
12.	$\neg\Box\varphi \to \varphi$	из уравнения на неподвижную точку
13.	$\neg\Box\bot \to \varphi$	из 11 и 12

т.е. PA $\vdash \mathit{Consis} \to \varphi$. Следовательно, PA $\vdash \mathit{Consis} \leftrightarrow \varphi$, и в силу I теоремы Геделя о неполноте PA $\nvdash \mathit{Consis}$.

Теорема 45 [теорема Леба] Если PA $\vdash \mathit{Pr}(\ulcorner\varphi\urcorner) \to \varphi$, то PA $\vdash \varphi$.

Доказательство. Рассмотрим неподвижную точку

$$\text{PA} \vdash \psi \leftrightarrow (\mathit{Pr}(\ulcorner\psi\urcorner) \to \varphi).$$

Выводим в PA:

1.	$\psi \to (\Box\psi \to \varphi)$	уравнение на неподвижную точку
2.	$\Box(\psi \to (\Box\psi \to \varphi))$	из 1 и ГБ(1)
3.	$\Box(\psi \to (\Box\psi \to \varphi)) \to (\Box\psi \to \Box(\Box\psi \to \varphi))$	ГБ(2)
4.	$\Box\psi \to \Box(\Box\psi \to \varphi)$	из 2 и 3
5.	$\Box(\Box\psi \to \varphi) \to (\Box\Box\psi \to \Box\varphi)$	ГБ(2)
6.	$\Box\psi \to (\Box\Box\psi \to \Box\varphi)$	из 4 и 5
7.	$(\Box\psi \to \Box\Box\psi) \to (\Box\psi \to \Box\varphi)$	пропозициональная логика, 6
8.	$\Box\psi \to \Box\Box\psi$	ГБ(3)
9.	$\Box\psi \to \Box\varphi$	7 и 8
10.	$\Box\varphi \to \varphi$	по условию
11.	$\Box\psi \to \varphi$	9 и 10
12.	$(\Box\psi \to \varphi) \to \psi$	10 и 11
13.	ψ	11 и 12
14.	$\Box\psi$	13
15.	φ	11 и 14

Теорема 46 [Теорема Тарского] Одноместный предикат *"x есть геделев номер формулы, истинной в стандартной модели арифметики"*, не является арифметическим, т.е. не существует формула $T(x)$, такая что для всех замкнутых формул φ

$$\omega \models \varphi \quad \Leftrightarrow \quad \omega \models T(\ulcorner \varphi \urcorner).$$

Доказательство. От противного, предположим, что такая формула $T(x)$ существует, и рассмотрим неподвижную точку формулы $\neg T(x)$

$$\mathrm{PA} \vdash \varphi \leftrightarrow \neg T(\ulcorner \varphi \urcorner).$$

Тогда если $\omega \models \varphi$, то в силу условия на неподвижную точку $\omega \models \neg T(\ulcorner \varphi \urcorner)$, и значит $\omega \not\models T(\ulcorner \varphi \urcorner)$. По условию на $T(x)$ получим $\omega \not\models \varphi$, противоречие.

Если же $\omega \not\models \varphi$, то в силу условия на неподвижную точку $\omega \models T(\ulcorner \varphi \urcorner)$. По условию на $T(x)$ получим $\omega \models \varphi$, противоречие.

Следовательно, формула φ не может быть ни истинной, ни ложной в ω, противоречие.

Теорема 47 Арифметика Пеано неразрешима.

Доказательство. От противного: если арифметика разрешима, то найдется Σ_1-формула $P(x)$, такая что для любой замкнутой фомрулы φ

$$\begin{array}{lll} \text{если} & \mathrm{PA} \vdash \varphi, & \text{то} \quad \mathrm{PA} \vdash P(\ulcorner \varphi \urcorner) \\ \text{если} & \mathrm{PA} \nvdash \varphi, & \text{то} \quad \mathrm{PA} \vdash \neg P(\ulcorner \neg \varphi \urcorner) \end{array}$$

Рассмотрим неподвижную точку формулы $\neg Px$

$$\mathrm{PA} \vdash \varphi \leftrightarrow \neg P(\varphi).$$

Тогда если $\mathrm{PA} \vdash \varphi$, то $\mathrm{PA} \vdash \neg P(\varphi)$ из условия на неподвижную точку и $\mathrm{PA} \vdash P(\varphi)$ в силу свойств формулы P, противоречие. Если же $\mathrm{PA} \nvdash \varphi$, то $\mathrm{PA} \vdash \neg P(\varphi)$ в силу свойств формулы P, следовательно $\mathrm{PA} \vdash \varphi$ из условия на неподвижную точку, противоречие.

На самом деле, с помощью той же самой конструкции можно доказать результат о неразрешимости для меньшей теории, а именно, для арифметики Робинсона Q. В отличие от арифметики Пеано, Q является конечно аксиоматизируемой, следовательно из неразрешимости Q получиае следующий факт.

Теорема 48 Исчисление предикатов в сигнатуре арифметики неразрешимо.

Доказательство. Запишем аксиомы Q, заменив функциональные буквы на предикатные. Их конечное число. Пусть A — конъюнкция этих аксиом. Для каждой арифметической формулы φ через φ' обозначим результат замены функциональных символов в этой формуле на предикатные. Тогда верно следующее:

$$Q \vdash \varphi \Leftrightarrow \mathrm{PC} \vdash A' \to \varphi'.$$

Следовательно, распознавание выводимости в теории Q сводится к задаче распознавания выводимости в PC, и значит выводимость в PC неразрешима, поскольку выводимость в Q неразрешима.

Конец лекции № 23

---

21 мая 2015 г.

Список литературы