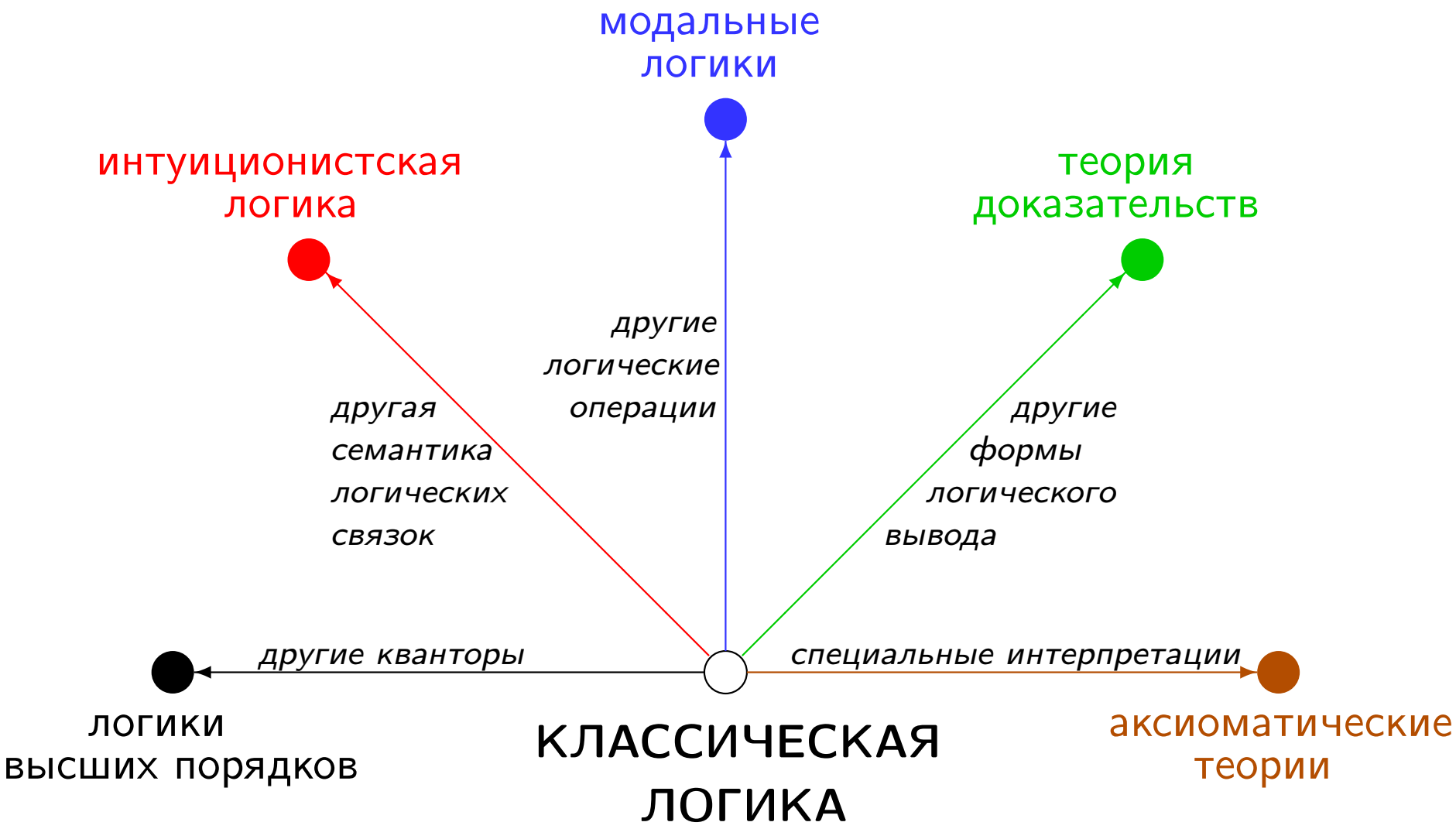
Основы математической логики и логического программирования

ЛЕКТОР: В.А. Захаров

Лекция 18.

Как устроена математика.
Исчисление предикатов первого порядка.
Аксиоматические теории.
Элементарная геометрия.
Теория множеств Цермело–Френкеля.
Арифметика Пеано.
Теорема Геделя о неполноте.


модальные
логики
интуиционистская
логика
теория
доказательств
другие
логические
операции
другая
семантика
логических
связок
другие
формы
логического
вывода
другие кванторы
специальные интерпретации
логики
высших порядков
КЛАССИЧЕСКАЯ
ЛОГИКА
аксиоматические
теории

Как устроена математика

Математика — это специфическая наука.

Она не относится к числу естественных наук (физика, ботаника, геология, и пр.), т. к. она не имеет дела ни с природными явлениями, ни с эмпирическими знаниями.

Она не относится к числу гуманитарных наук (философия, история, политология и пр. болтология), т. к она не занимается ни людской деятельностью, ни людскими воззрениями.

Она занимается созданием, развитием и изучением математических теорий — умозрительных конструкций, которые строятся по строгим объективным законам формальной логики .

Как устроена математика

Станислав Лем сравнивал математику с безумным портным, который шьет одежду для неведомых существ.
Портного не беспокоит, кому придется впору его одежда.
Он лишь хочет, чтобы платье было сшито прочно.

Как устроена математика

С чего начинается рассказ о каждом разделе математики?

- Вначале уславливаются о системе обозначений, определяют язык, на котором будут записывать математические утверждения (определяется синтаксис математического языка).
- Затем приходят к соглашению об основополагающих свойствах, законах, которым должны удовлетворять интересующие нас операции и отношения над воображаемыми объектами (формулируются аксиомы математической теории).
- Далее договариваются о том, какие средства обоснования истинности математических утверждений считаются допустимыми (определяется аппарат логического вывода).
- И после этого приступают к получению логически обоснованных утверждений сформулированной математической теории (вывод теорем).

Вот так строятся формальные аксиоматические теории .

Классическое исчисление предикатов

Как можно аксиоматизировать теорию общезначимых утверждений (формул)? Например, так:

АКСИОМЫ.

1. Ax1. $\varphi_1 \to (\varphi_2 \to \varphi_1)$,
2. Ax2. $(\varphi_1 \to (\varphi_2 \to \varphi_3)) \to ((\varphi_1 \to \varphi_2) \to (\varphi_1 \to \varphi_3))$,
3. Ax3. $(\varphi_1 \,\&\, \varphi_2) \to \varphi_1$,
4. Ax4. $(\varphi_1 \,\&\, \varphi_2) \to \varphi_2$,
5. Ax5. $\varphi_1 \to (\varphi_2 \to (\varphi_1 \,\&\, \varphi_2))$,
6. Ax6. $\varphi_1 \to (\varphi_1 \vee \varphi_2)$,
7. Ax7. $\varphi_2 \to (\varphi_1 \vee \varphi_2)$,
8. Ax8. $(\varphi_1 \to \varphi_0) \to ((\varphi_2 \to \varphi_0) \to ((\varphi_1 \vee \varphi_2) \to \varphi_0))$,
9. Ax9. $\varphi_1 \to (\neg\varphi_1 \to \varphi_0)$,
10. Ax10. $\varphi_1 \vee \neg\varphi_1$,

Классическое исчисление предикатов

АКСИОМЫ.

1. Ax11. $\forall X\ \varphi(X) \to \varphi(t)$,
2. Ax12. $\varphi(t) \to \exists X\ \varphi(X)$,
3. Ax13. $\forall X\ (\varphi_1 \to \varphi_2(X)) \to (\varphi_1 \to \forall X\ \varphi_2(X))$,
4. Ax14. $\forall X\ (\varphi_1(X) \to \varphi_2) \to (\exists X\ \varphi_1(X) \to \varphi_2)$.

ПРАВИЛА ВЫВОДА.

1. Правило отделения (modus ponens) $\dfrac{\varphi,\ \varphi \to \psi}{\psi}$,
2. Правило обобщения $\dfrac{\varphi}{\forall X\ \varphi}$

Классическое исчисление предикатов

ЛОГИЧЕСКИЙ ВЫВОД.

Пусть задано некоторое множество формул (гипотез) Γ.
Тогда логическим выводом из множества гипотез Γ называется конечная последовательность формул

$$\varphi_1, \varphi_2, \ldots, \varphi_n,$$

в которой каждая формула φ_i удовлетворяет одному из следующих условий:

1. либо φ_i является аксиомой,
2. либо φ_i является гипотезой, т. е. $\varphi_i \in \Gamma$,
3. либо φ_i получается из предшествующих формул этой последовательности по правилу отделения или по правилу обобщения.

В этом случае формула φ_n называется выводимой из множества Γ, и этот факт обозначается $\Gamma \vdash \varphi_n$

Формула φ называется теоремой, если $\varnothing \vdash \varphi$, и этот факт обозначается $\vdash \varphi$.

Классическое исчисление предикатов

Исчисление предикатов с равенством.

Введем специальный двухместный предикатный символ $=$ и добавим к аксиомам КИП следующие аксиомы равенства:

1. Ax15. $\forall X\ (X = X)$,
2. Ax16 $\forall X, Y\ (X = Y\ \rightarrow\ (\varphi(X, X)\ \rightarrow\ \varphi(X, Y)))$.

Полученную систему аксиом называют классическим исчислением предикатов с равенством $КИП_{=}$.

Алгебраическая система I называется нормальной интерпретацией , если для любой пары различных предметов d_1, d_2 из области интерпретации D_I верно соотношение

$$I\ \not\models\ d_1 = d_2\ .$$

Аксиоматические теории первого порядка

Элементарная аксиоматическая теория образуется из исчисления предикатов с равенством за счет

- ограничения сигнатуры языка логики предикатов фиксированным конечным набором констант, функциональных и предикатных символов, обозначающих базовые объекты, операции и отношения теории,
- добавления к множеству аксиом исчисления предикатов специальных (нелогических) аксиом, описывающих базовые принципы теории.

Таким образом образуются элементарная теория равенства, элементарная теория групп, элементарная теория полей, элементарная геометрия, элементарная арифметика, элементарная теория множеств, и др.

Формулы φ, логически выводимые из аксиом элементарной аксиоматической теории T, называются теоремами этой теории и обозначаются записью $T \vdash \varphi$.

Аксиоматические теории первого порядка

Элементарная аксиоматическая теория T называется

- непротиворечивой, если не все формулы являются теоремами теории T, т. е. существует такая формула φ, для которой $T \nvdash \varphi$;
- полной, если всякая формула или ее отрицание являются теоремами теории T, т. е. для любой формулы φ либо $T \vdash \varphi$, либо $T \vdash \neg\varphi$;
- категоричной, если любые **нормальные** две модели теории T изоморфны, т. е. для любой пары нормальных интерпретаций I_1, I_2 верно
$$I_1 \models T \text{ и } I_2 \models T \implies I_1 \cong I_2;$$
- разрешимой, если существует алгоритм, проверяющий, является ли произвольная формула теоремой теории T.

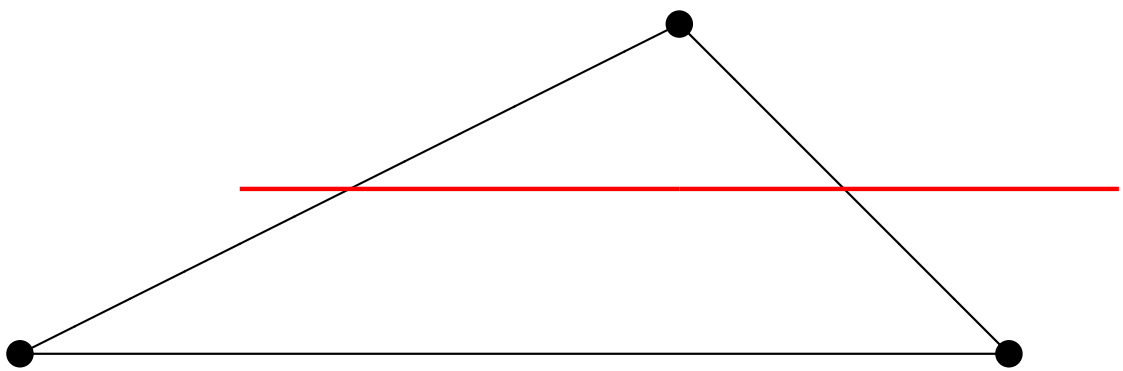
Аксиоматическое устройство геометрии

Впервые попытку аксиоматизировать геометрию предпринял Евклид (3 в. до н. э.). Геометрическая теория Евклида опиралась на 5 аксиом.

К сожалению, система геометрических аксиом из «Начал» Евклида неполна.

Вот пример истинного утверждения, которое нельзя вывести из аксиом и постулатов Евклида.

Если прямая пересекает одну из сторон треугольника в точке, отличной от вершины треугольника, то эта прямая также пересекает еще одну сторону треугольника.



Аксиоматическое устройство геометрии

Систематическое и основательное построение геометрической системы аксиом было осуществлено Д. Гильбертом (40 аксиом) в 1899 г. Более более краткую аксиоматику удалось построить А. Тарскому и его ученика (12 аксиом).

Аксиомы Тарского

Будем рассматривать геометрический мир, все объекты которого — точки .

На множестве точек есть всего лишь два базовых предиката:

$\mathbf{B(x, y, z)}$	точка y лежит между точками x и z на одной прямой
$\mathbf{D(x, y, z, u)}$	точка x отстоит от точки y на такое же расстояние, что и точка z от точки u

Аксиоматическое устройство геометрии

Аксиомы T1–T5

1). $\forall x, y, z\ (B(x, y, z) \rightarrow B(z, y, x))$
(аксиома симметричности предиката B)

2). $\forall x, y, z, u\ (B(x, y, u) \& B(y, z, u) \rightarrow B(x, y, z))$
(аксиома транзитивности предиката B)

3). $\forall x, y\ D(x, y, y, x)$
(аксиома симметричности равенства длин отрезков)

4). $\forall x, y, z\ (D(x, y, z, z) \rightarrow x = y)$
(аксиома нулевого отрезка)

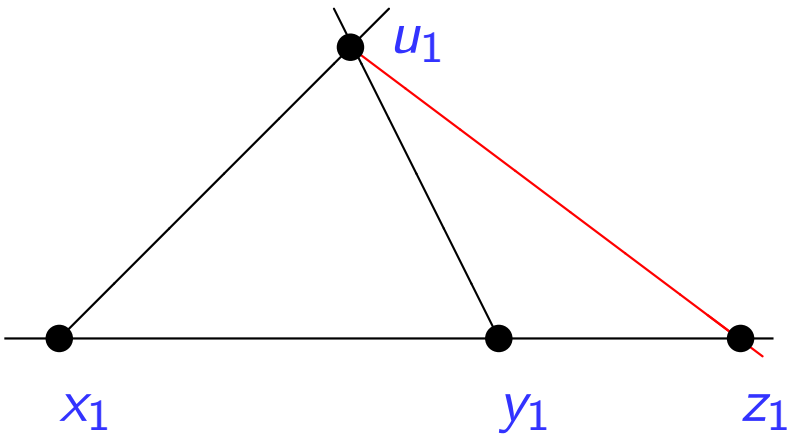
5). $\forall x_1, y_1, x_2, y_2, x_3, y_3$
$(D(x_1, y_1, x_2, y_2) \& D(x_2, y_2, x_3, y_3) \rightarrow D(x_1, y_1, x_3, y_3))$
(аксиома транзитивности равенства длин отрезков)

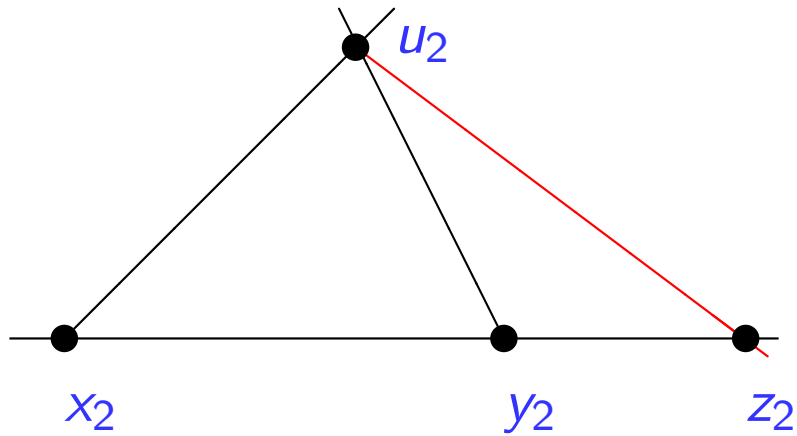
Аксиоматическое устройство геометрии

Аксиома T6

6). $\forall x_1, y_1, z_1, u_1, x_2, y_2, z_2, u_2$
$(x_1 \neq y_1 \& y_1 \neq z_1 \&$
$B(x_1, y_1, z_1) \& B(x_2, y_2, z_2) \&$
$D(x_1, y_1, x_2, y_2) \& D(y_1, z_1, y_2, z_2) \&$
$D(y_1, u_1, y_2, u_2) \& D(x_1, u_1, x_2, u_2) \rightarrow$
$\rightarrow D(z_1, u_1, z_2, u_2))$

(аксиома пяти отрезков)





Аксиоматическое устройство геометрии

Аксиомы Аксиомы T7–T10

7). $\forall x, y, z, u\ \exists v\ (B(x, y, z)\ \&\ D(y, z, u, v))$
(аксиома откладывания отрезка)

8). $\forall x, y,\ \exists z\ (B(x, z, y) \& D(x, z, z, y))$
(аксиома деления отрезка пополам)

9). $\exists x, y, z\ (\neg B(x, y, z)\ \&\ \neg B(x, z, y)\ \&\ \neg B(z, x, y))$
(аксиома существования неколлинеарных точек)

10). $\forall x, y, z\ (\neg B(x, y, z)\ \&\ \neg B(x, z, y)\ \&\ \neg B(z, x, y)\ \rightarrow$
$\rightarrow\ \exists v\ (D(v, x, v, y) \& D(v, x, v, z)))$
(аксиома центра описанной окружности)

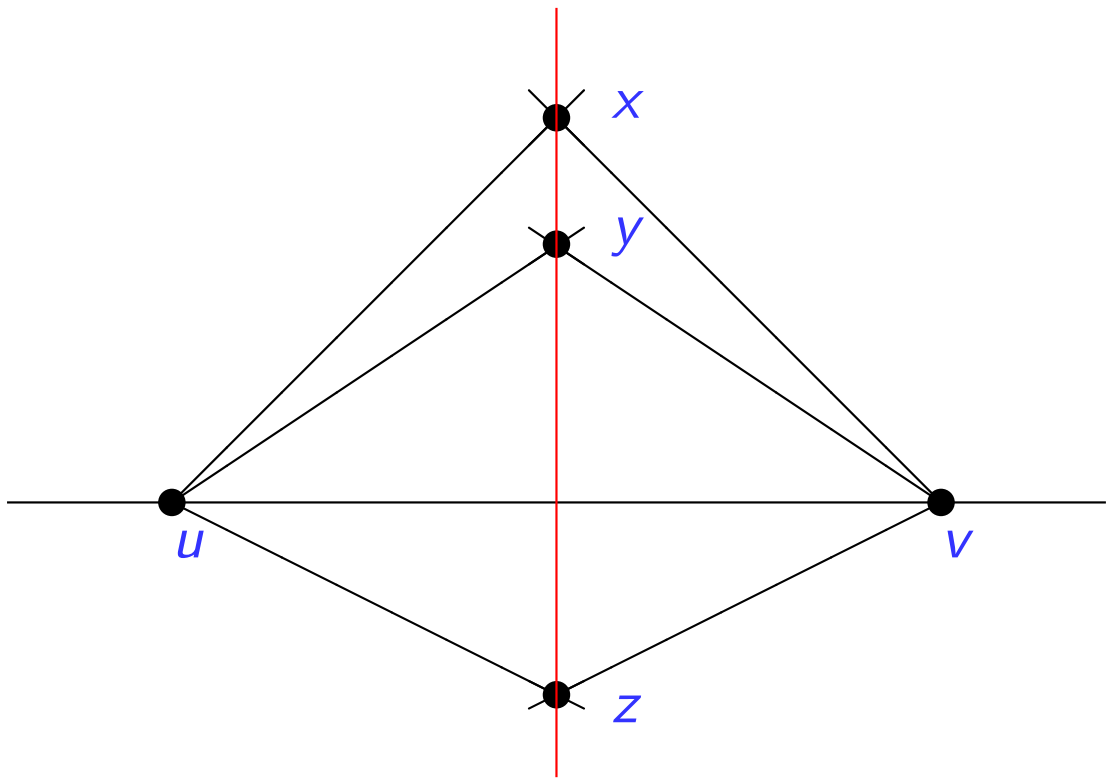
Аксиоматическое устройство геометрии

Аксиома T11

11). $\forall x, y, z, u, v$

$$(D(x,u,x,v)\&D(y,u,y,v)\&D(z,u,z,v) \rightarrow$$
$$\rightarrow (B(x,y,z) \vee B(y,z,x) \vee B(z,y,x)))$$

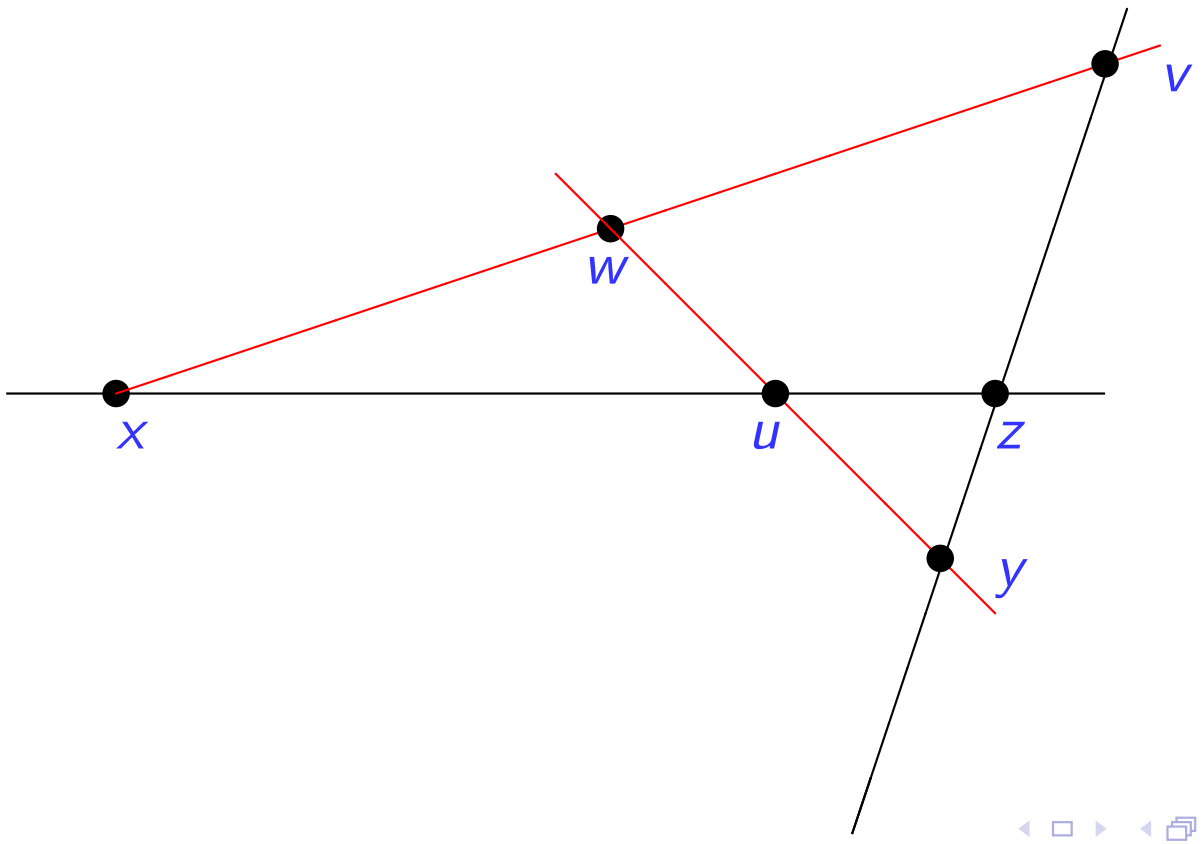
(аксиома перпендикуляра к середине отрезка)



Аксиоматическое устройство геометрии

Аксиома T12

12). $\forall x, y, z, u, v$
$(B(x, u, z) \& B(y, z, v) \rightarrow$
$\rightarrow \exists w\ (B(y, u, w) \& B(x, w, v)))$
(аксиома Паша)



Аксиоматическое устройство геометрии

Аксиома T13

13). $\forall x\ \exists y, z\ (\varphi(y)\&\psi(z)\ \rightarrow\ B(x,y,z))\ \rightarrow$
$\rightarrow\ \forall x'\ \exists y', z'\ (\varphi(y')\&\psi(z')\ \rightarrow\ B(y',x',z'))$
(схема аксиом непрерывности)

Аксиоматическое устройство геометрии

Основные свойства формальной геометрии Тарского

Теорема

Аксиоматическая теория T1–T13 (формальная геометрия Тарского)

- непротиворечива,
- полна,
- категорична,
- алгоритмически разрешима.

К сожалению для школьников, разрешающая процедура, способная доказывать любую геометрическую теорему, имеет невероятно большую вычислительную сложность.

Теория множеств

МНОЖЕСТВО — это основополагающее понятие современной математики. Понятие множества предложил во второй половине 19 в. немецкий математик Георг Кантор.

А что же такое множество?

Поскольку это основополагающее понятие, строгого определения дать нельзя. Это коллекция (семейство, совокупность, собрание) различных предметов (объектов, элементов).

Может ли математика спокойно развиваться, опираясь на столь зыбкое основание?

Теория множеств

Парадокс Рассела

Элементами множеств могут быть множества. Рассмотрим коллекцию всех множеств, каждое из которых не является своим собственным элементом: $A = \{x : x \notin x\}$.
У нас нет достаточных оснований не признавать эту совокупность множеств A множеством.

Но тогда мы должны уметь давать ответ на вопрос: содержит ли множество A в качестве элемента само множество A (т. е. верно ли что $A \in A$?)
Ответ обескураживающий:

- если $A \in A$, то по определению A верно $A \notin A$,
- а если $A \notin A$, то определению A верно $A \in A$.

Теория множеств

Значит, в наивной теории множеств существуют математические утверждения, которые нельзя признать ни истинными, ни ложными. На основе такой расплывчатой теории хорошей математики не построить.

Может быть стоило бы исключить эту странную коллекцию A из числа множеств?

Можно. Но тогда придется создать «кодекс теории множеств», в котором должно быть указано, какие именно конструкции признаются множествами, и какими свойствами они должны обладать.

Попытку создания такого «кодекса теории множеств» — аксиоматической теории множеств — предприняли в Эрнест Цермело в 1908 г.. Аксиоматику Цермело пополнили Абрахам Френкель, Торальф Сколем, Джон фон Нейман.

Теория множеств Цермело–Френкеля

Понятие множества и свойства множеств можно описать с использованием единственного предикатного символа $\in$, обозначающего отношение принадлежности одного множества в качестве элемента другого множества.

Представим себе математический мир, состоящий только из множеств. Этот мир может быть описан следующими аксиомами.

Теория множеств Цермело–Френкеля

1) $\forall x, y, u, v\ (x = y\ \&\ u = v)\ \rightarrow\ (x \in u\ \equiv\ y \in v)$
   (Аксиома равенства множеств)
2) $\forall x, y\ (\forall z\ (z \in x\ \equiv\ z \in y)\ \equiv\ x = y)$
   (Аксиома объемности)
3) $\forall x \forall u_1, \ldots, u_n\ \exists y\ \forall z\ (z \in y\ \equiv\ (z \in x\ \&\ \varphi(z, u_1, \ldots, u_n)))$
   (Схема аксиом выделения)

   здесь $\varphi(x, u_1, \ldots, u_n)$ — произвольная формула логики предикатов сигнатуры $\sigma = \langle \in \rangle$.

Теория множеств Цермело–Френкеля

Примеры применения аксиомы выделения

1. Существует единственное пересечение двух множество

Существование пересечения двух множеств следует из аксиомы выделения

$$\forall x_1, x_2 \; \exists y \; \forall z \; (z \in y \; \equiv \; (z \in x_1 \; \& \; z \in x_2)),$$

а единственность пересечения следует из аксиомы объемности

$$\forall x, y \; (\forall z \; (z \in x \; \equiv \; z \in y) \; \equiv \; x = y).$$

Теория множеств Цермело–Френкеля

Примеры применения аксиомы выделения

2. Существует единственное пустое множество

Существование пустого множества следует из аксимы выделения

$$\forall x\ \exists y \forall z (z \in y\ \equiv\ (z \in x\ \&\ z \neq z)),$$

а единственность пустого множества следует из аксиомы объемности

$$\forall x, y\ (\forall z\ (z \in x\ \equiv\ z \in y)\ \equiv\ x = y).$$

Но здесь есть один нюанс. А откуда берется множество X на основании которого определяется пустое множество?

Теория множеств Цермело–Френкеля

Примеры применения аксиомы выделения

2. Существует единственное пустое множество

Существование пустого множества следует из аксимы выделения

$$\forall X\ \exists y \forall z (z \in y\ \equiv\ (z \in X\ \&\ z \neq z)),$$

а единственность пустого множества следует из аксиомы объемности

$$\forall x, y\ (\forall z\ (z \in x\ \equiv\ z \in y)\ \equiv\ x = y).$$

Но здесь есть один нюанс. А откуда берется множество X на основании которого определяется пустое множество?

Теория множеств Цермело–Френкеля

Примеры применения аксиомы выделения

Поэтому приходится вводить специальную аксиому.

4). $\exists y\ \forall z\ \neg(z \in y)$
(Аксиома пустого множества)

Введем специальный символ $\varnothing$ для обозначения пустого множества, а запись $y = \varnothing$ будем рассматривать как сокращенное обозначение формулы

$$\forall z\ \neg(z \in y)\ .$$

Теория множеств Цермело–Френкеля

Примеры применения аксиомы выделения

3. Существует единственное объединение двух множеств

Казалось бы, объединение множеств легко ввести так же, как это было сделано для пересечения:

$$\forall x_1, x_2\ \exists y\ \forall z\ (z \in y\ \equiv\ (z \in x_1\ \vee\ z \in x_2))\ .$$

Но эта формула не подпадает под схему аксиом выделения

$$\forall x \forall u_1, \ldots, u_n\ \exists y\ \forall z\ (z \in y\ \equiv\ (z \in x\ \&\ \varphi(z, u_1, \ldots, u_n)))\ .$$

Можно было бы записать определение объединения так:

$$\forall X, x_1, x_2\ \exists y\ \forall z\ (z \in y\ \equiv\ (z \in X\ \&\ (z \neq x_1\ \vee\ z \in x_2)))\ .$$

Но совершенно непонятно, откуда взять подходящее множество X. Может быть, в качестве X взять $x_1 \cup x_2$? Но мы ведь еще не

Теория множеств Цермело–Френкеля

Примеры применения аксиомы выделения

3. Существует единственное объединение двух множеств. Поэтому приходится вводить две специальные аксиомы.

5). $\forall y, z\ \exists x\ \forall u\ (u \in x\ \equiv\ (u = y\ \vee\ u = z))$
(Аксиома пары)

Множество x, существование которого утверждает аксиома пары, традиционно обозначается $\{y, z\}$.

6). $\forall y\ \exists x\ \forall u\ (u \in x\ \equiv\ \exists z\ (z \in y\ \&\ u \in z))$
(Аксиома объединения)

Множество x, существование которого утверждает аксиома объединения, традиционно обозначается $\bigcup\limits_{z \in y} z$ или более коротко $\cup y$. Таким образом $x_1 \cup x_2$ — это $\cup\{x_1, x_2\}$.

Теория множеств Цермело–Френкеля

Примеры применения аксиомы выделения

4. А что делать, если нам нужно множество, состоящее из одного-единственного элемента?

Для этого достаточно выделения и аксиомы пары:
множество, состоящее из одного элемента u — это множество {u,u}.

5. А что делать, если нам нужны упорядоченные наборы элементов?

Для этого достаточно аксиомы выделения и аксиомы пары:
упорядоченная пара $\langle y, z \rangle$ — это множество $\{y, \{y, z\}\}$.

Далее аналогично можно определять упорядоченные наборы (кортежи), функции, инъективные отображения, биективные отображения, отношения включения, равномощности и т. д.

Теория множеств Цермело–Френкеля

Но таким образом из пустого множества $\varnothing$, — единственного множества, существование которого гарантируют аксиомы, — можно получить только конечные множества. А откуда возьмутся бесконечные множества?

7). $\exists x\ (\varnothing \in x\ \&\ \forall y\ (y \in x\ \rightarrow\ y \cup \{y\} \in x))$
(Аксиома бесконечности)

Фактически, аксиома бесконечности определяет множество натуральных чисел:

$$\Big\{ \underbrace{\varnothing}_{0},\ \underbrace{\{\varnothing\}}_{1},\ \underbrace{\{\varnothing, \{\varnothing\}\}}_{2},\ \underbrace{\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}}_{3},\ \dots \Big\}$$

Теория множеств Цермело–Френкеля

А откуда возьмутся несчетные множества?

8). $\forall y\ \exists x\ \forall z\ (z \in x\ \equiv\ \forall u\ (u \in z\ \rightarrow\ u \in y))$
(Аксиома степени)

Аксиома степени определяет множество всех подмножеств заданного множества (множество-степень, powerset). Значит, множества могут нарастать неограниченно «высоко».

Теория множеств Цермело–Френкеля

А являются ли множествами образы множеств относительно заданных функций, определяемых при помощи формул логики предикатов?

9). $\forall x\ \big(\forall y, z, u\ (y \in x\ \&\ \varphi(y, z)\ \&\ \varphi(y, u)\ \to z = u)\ \to$
$\to\ \exists v\ \forall w\ (w \in v\ \equiv\ \exists t\ (t \in x\ \&\ \varphi(t, w)))\big)$
(Схема аксиом замены)

Теория множеств Цермело–Френкеля

А насколько «глубоко» могут опускаться множества? Не могут ли у нас образовываться такие множества, которые входят в состав самих себя в качестве элементов?

10). $\forall x\ (x \neq \varnothing\ \rightarrow\ \exists y\ (y \in x\ \&\ x \cap y = \varnothing))$
(Аксиома фундирования (регулярности))

Эта аксиома играет роль предохранителя, оберегающего теорию множеств от парадоксов. Аксиома фундирования объявляет, что семейства множеств вида

$$\left\{X_1, X_2, X_3, \dots\right\},$$

у которых $X_2 \in X_1$, $X_3 \in X_2$, $\dots$, $X_{n+1} \in X_n$, $\cdots$ и т. д. множествами не являются .

Теория множеств Цермело–Френкеля

Примеры применения аксиомы фундирования

$ZF \vdash \forall u(u \notin u)$
Из аксиомы фундирования

$$\forall x\ (x \neq \varnothing\ \rightarrow\ \exists y\ (y \in x\ \&\ x \cap y = \varnothing))$$

следует (если в качестве x выбрать $\{u\}$)

$$ZF \vdash \exists y\ (y \in \{u\}\ \&\ u \cap y = \varnothing)\ .$$

Поскольку единственным элементом y в множестве $\{u\}$ является u, получаем

$$ZF \vdash \{u\} \cap u = \varnothing\ .$$

Следовательно, $ZF \vdash u \notin u$.

Теория множеств Цермело–Френкеля

Примеры применения аксиомы фундирования

Попробуйте самостоятельно убедиться, что из аксиом теории множеств Цермело–Френкеля следует невозможность существования «парадоксальных множеств»:

$$ZF \vdash \forall u, v\ (u \notin v\ \vee v \notin u)$$

$$ZF \vdash \neg\exists x\ \forall y\ (y \in x\ \equiv y \notin y)$$

Нужны ли еще какие-нибудь другие аксиомы?

Теория множеств Цермело–Френкеля

К сожалению, для решения некоторых задач приходится вводить дополнительные аксиомы.
Например, интуиция подсказывает, что любые два множества должны быть сравнимы по мощности. Два множества A и B называются равномощными ($A \sim B$), если существует биективная функция, отображающая одно множество на другое. Справедливо ли следующее утверждение?

Теорема трихотомии. Для любых двух множеств A и B верно одно из трех:

- либо $A \sim B$,
- либо $A \not\sim B$, но существует такое A', $A' \subset A$, что $A' \sim B$,
- либо $A \not\sim B$, но существует такое B', $B' \subset B$, что $A \sim B'$.

Эту теорему можно доказать, но лишь при том условии, если у нас есть хоть какой-нибудь способ, позволяющий выбрать из произвольного непустого множества хоть какой-нибудь элемент. Чтобы этот способ выбора стал легальным средством доказательства, нужно ввести специальную аксиому выбора.

Теория множеств Цермело–Френкеля

Аксиома выбора (CA)

Каково бы ни было множество попарно непересекающихся множеств $U = \{X_1, X_2, \dots\}$, существует множество Y, содержащее в точности по одному представителю из каждого множества $X_1, X_2, \dots$ семейства U.

Аксиома выбора используется при доказательстве очень большого числа теорем математики. С ее помощью можно доказать весьма неожиданные утверждения. К их числу относится

Теорема Цермело

Любое множество можно вполне упорядочить, т. е. определить на этом множестве такое отношение линейного порядка, при котором не существует бесконечно убывающих последовательностей элементов.

Теория множеств Цермело–Френкеля

А не привнесет ли аксиома выбора какое-нибудь противоречие в теорию ZF? Этот вопрос остается открытым и по сей день.

Есть в теории множеств и другие задачи, для решения которых недостаточно аксиом теории множеств ZF.

Континуум-гипотеза (CH)

Любое подмножество множества вещественных чисел либо является счетным, либо равномощно множеству вещественных чисел (является континуальным).

В 1939 г. К. Гедель доказал теорему:

Если теория множеств ZF+CA непротиворечива, то теория ZF+AC+CH также непротиворечива .

В 1963 г. П. Коэн доказал теорему:

Если теория множеств ZF+CA непротиворечива, то теория ZF+AC+$\neg$CH также непротиворечива .

Формальная арифметика

А можно ли полностью аксиоматизировать арифметику натуральных чисел?

В 1889 г. итальянский математик Д. Пеано предложил список аксиом, при помощи которых можно доказывать утверждения о свойствах натуральных чисел.

Арифметика Пеано (PA) образуется за счет добавления к ИПР сигнатуры $\langle 0, s, +, \times \rangle$ следующих аксиом.
Здесь $s(x)$ нужно рассматривать как одноместную операцию, реализующую функцию вычисления следующего натурального числа $x + 1$.

Формальная арифметика

1. $\forall x, y\ (s(x) = s(y)\ \rightarrow x = y)$;
2. $\forall x\ (s(x) \neq 0)$;
3. $\forall x\ \exists y(x \neq 0\ \rightarrow\ x = s(y))$;
4. $\forall x\ (x + 0 = x)$;
5. $\forall x, y\ (x + s(y) = s(x + y))$;
6. $\forall x\ (x \times 0 = 0)$;
7. $\forall x, y\ (x \times s(y) = x \times y + x)$;
8. $\varphi(0)\ \&\ \forall x\ (\varphi(x)\ \rightarrow\ \varphi(s(x)))\ \rightarrow\ \forall x\ \varphi(x)$.

Вопрос о непротиворечивости и полноте этой аксиоматической теории долгое время оставался центральной проблемой математики. В 1931 г. К. Гедель доказал теорему, которая дала совершенно неожиданный ответ на этот вопрос.

Формальная арифметика

Нумералы и арифметизуемые отношения

Нумералом $\bar{\mathbf{n}}$ натурального числа n называется терм

$$\underbrace{s(s(\ldots s(}_{n \text{ раз}} 0)\ldots))$$

Например, $\bar{\mathbf{4}}$ — это терм $s(s(s(s(0))))$.

Отношение $P^{(k)}$ на множестве натуральных чисел называется **арифметизуемым**, если существует такая формула $\varphi(x_1, x_2, \ldots, x_k)$, что для всякого набора натуральных чисел $(n_1, n_2, \ldots, n_k)$ верны соотношения

- $P^{(k)}(n_1, n_2, \ldots, n_k) = \mathit{true} \iff PA \vdash \varphi(\bar{\mathbf{n}}_1, \bar{\mathbf{n}}_2, \ldots, \bar{\mathbf{n}}_k)$,
- $P^{(k)}(n_1, n_2, \ldots, n_k) = \mathit{false} \iff PA \vdash \neg\varphi(\bar{\mathbf{n}}_1, \bar{\mathbf{n}}_2, \ldots, \bar{\mathbf{n}}_k)$.

Формальная арифметика

Нумералы и арифметизуемые отношения

Теорема Геделя–Тьюринга.
Отношение $P^{(k)}$ на множестве натуральных чисел арифметизуемо в том и только том случае, если существует такая машина Тьюринга M, которая для любого набора натуральных чисел $(n_1, n_2, \ldots, n_k)$ имеет завершающееся вычисление, преобразующее начальную конфигурацию

$$q_1 \underbrace{11\ldots1}_{n_1+1 \text{ раз}} 0 \underbrace{11\ldots1}_{n_2+1 \text{ раз}} 0\ldots0 \underbrace{11\ldots1}_{n_k+1 \text{ раз}}$$

- в заключительную конфигурацию $q_0 1$, если $P^{(k)}(n_1, n_2, \ldots, n_k) = \mathit{true}$,
- в заключительную конфигурацию $q_0 0$, если $P^{(k)}(n_1, n_2, \ldots, n_k) = \mathit{false}$.

Формальная арифметика

Нумерация Геделя

Закодируем натуральными числами (занумеруем) символы алфавита формальной арифметики, формулы и конечные последовательности формул.

$gn(0) = 3,\ gn(s) = 5,\ gn(+) = 7,\ gn(\times) = 9,\ gn(=) = 11,$

$gn(\neg) = 13,\ gn(\&) = 15,\ gn(\vee) = 17,\ gn(\rightarrow) = 19,$
$gn(\forall) = 21,\ gn(\exists) = 23,$

$gn(\ (\ ) = 25,\ gn(\ )\ ) = 27,$

$gn(x_1) = 29,\ gn(x_2) = 31,\ \ldots,\ gn(x_i) = 27 + 2i, \ldots.$

Геделев номер слова:
$gn(a_1 a_2 a_3 \ldots a_n) = 2^{gn(a_1)} 3^{gn(a_2)} 5^{gn(a_3)} \ldots p_n^{gn(a_n)}.$

Геделев номер последовательности слов:
$gn(\alpha_1 \alpha_2 \alpha_3 \ldots \alpha_m) = 2^{gn(\alpha_1)} 3^{gn(\alpha_2)} 5^{gn(\alpha_3} \ldots p_m^{gn(\alpha_m)}.$

Формальная арифметика

Примеры арифметизуемых отношений

Рассмотрим два отношения

1. $\mathrm{Form}^{(1)}$: $\mathrm{Form}(n) = \mathit{true} \iff n$ — геделев номер формулы арифметики Пеано.
2. $\mathrm{Proof}^{(2)}$: $\mathrm{Proof}(n, m) = \mathit{true} \iff n$ — геделев номер некоторой формулы φ арифметики Пеано, а m — геделев номер конечной последовательности формул, составляющей доказательство формулы φ.

Лемма

Отношения Form и Proof арифметизируемы.

Обозначим *Proof* арифметическую формулу, реализующую предикат Proof .

Формальная арифметика

Странные предикаты

Ну, если вы поверили, что предикат $\mathrm{Proof}^{(2)}$ арифметизуем, то совершенно очевидно, что арифметизуемым является и такой странный предикат $\mathrm{MetaProof}^{(2)}$:

$$\mathrm{MetaProof}(n, m) = \mathit{true}$$

$$\Updownarrow$$

n — геделев номер некоторой формулы арифметики Пеано, $\varphi(x)$, зависящей от одной переменной,
а m — геделев номер конечной последовательности формул, составляющей доказательство формулы $\varphi(\bar{\mathbf{n}})$.

Но если предикат $\mathrm{MetaProof}^{(2)}$ арифметизуем, то существует арифметическая формула $\mathcal{W}(x, y)$, выражающая отношение $\mathrm{MetaProof}$.

Формальная арифметика

Странные предикаты

Рассмотрим формулу $\varphi(x) = \neg\exists y\ \mathcal{W}(x, y)$ и ее геделев номер $n_0 = gn(\varphi(x))$.

Интересно, а что за высказывание выражает замкнутая формула $\varphi(\bar{\mathbf{n}}_{\mathbf{0}})$?

Это высказывание таково: Нельзя доказать формулу $\varphi(\bar{\mathbf{n}}_{\mathbf{0}})$, т. е. формула $\varphi(\bar{\mathbf{n}}_{\mathbf{0}})$ утверждает, что она недоказуема.

Таким образом, мы имеем дело со строго сформулированным аналогом «парадокса лжеца».

И если эта формула действительно не имеет доказательства в арифметике Пеано, то она выражает истинное суждение.

Теорема Геделя о неполноте PA

(облегченный вариант)

Если множество натуральных чисел с операциями сложения и умножения $(\mathcal{N}_0, +, \times)$ является моделью для аксиом PA, то PA неполна.

Доказательство.

1. Покажем, что $PA \nvdash \varphi(\bar{\mathbf{n}}_\mathbf{0})$.
Допустим противное $PA \vdash \varphi(\bar{\mathbf{n}}_\mathbf{0})$. Тогда формула $\varphi(\bar{\mathbf{n}}_\mathbf{0})$ имеет доказательство в PA: $\psi_1, \psi_2, \ldots, \psi_N = \varphi(\bar{\mathbf{n}}_\mathbf{0})$.

Пусть $m = gn(\psi_1, \psi_2, \ldots, \psi_N)$. Тогда $MetaProof(n_0, m) = true$.
Поэтому, учитывая арифметизуемость предиката $MetaProof$, получаем $PA \vdash \mathcal{W}(\bar{\mathbf{n}}_\mathbf{0}, \bar{\mathbf{m}})$. Но это означает, что $PA \vdash \exists y\ \mathcal{W}(\bar{\mathbf{n}}_\mathbf{0}, y)$ и, следовательно, $PA \vdash \neg\varphi(\bar{\mathbf{n}}_\mathbf{0})$.
Но это означает, что PA — противоречивая теория, вопреки условию теоремы (PA имеет модель).

Теорема Геделя о неполноте PA

(облегченный вариант)

Если множество натуральных чисел с операциями сложения и умножения $(\mathcal{N}_0, +, \times)$ является моделью для аксиом PA, то PA неполна.

Доказательство.

2. Покажем, что $PA \nvdash \neg\varphi(\bar{\mathbf{n}}_\mathbf{0})$.
Допустим противное $PA \vdash \neg\varphi(\bar{\mathbf{n}}_\mathbf{0})$, т. е. $PA \vdash \exists y\ \mathcal{W}(\bar{\mathbf{n}}_\mathbf{0}, y)$.
Тогда (почему?) существует такое натуральное число m, для которого верно $PA \vdash \mathcal{W}(\bar{\mathbf{n}}_\mathbf{0}, \bar{\mathbf{m}})$. Учитывая, что формула $\mathcal{W}$ выражает отношение *MetaProof* , приходим к выводу: m — это геделев номер доказательства формулы $\varphi(\bar{\mathbf{n}}_\mathbf{0})$ в PA. Значит, $PA \vdash \varphi(\bar{\mathbf{n}}_\mathbf{0})$.
Но это означает, что PA — противоречивая теория, вопреки условию теоремы (PA имеет модель).

Теорема Геделя о неполноте PA

(облегченный вариант)

Если множество натуральных чисел с операциями сложения и умножения $(\mathcal{N}_0, +, \times)$ является моделью для аксиом PA, то PA неполна.

Доказательство.

3. Итак,

$PA \nvdash \varphi(\bar{\mathbf{n}}_\mathbf{0})$

$PA \nvdash \neg\varphi(\bar{\mathbf{n}}_\mathbf{0})$.

Значит, $\varphi(\bar{\mathbf{n}}_\mathbf{0}) = \neg\exists y\ \mathcal{W}(\bar{\mathbf{n}}_\mathbf{0}, y)$ — это истинное арифметическое утверждение, которое нельзя ни доказать, ни опровергнуть в арифметике Пеано.
Значит, арифметика Пеано неполна. $\square$

Теорема Геделя о неполноте PA

(Основной вариант)

Пусть запись *Consist* обозначает арифметическую формулу

$$\neg\exists X \; Proof(\overline{gn(0 = s(0))}, X)$$

Если формальная арифметика PA непротиворечива, то

$$\begin{aligned} PA &\nvdash Consist \\ PA &\nvdash \neg Consist. \end{aligned}$$

Это означает, что аксиоматические теории (сколь бы выразительны они ни были) не позволяют построить доказательство их собственной непротиворечивости.

КОНЕЦ ЛЕКЦИИ 18